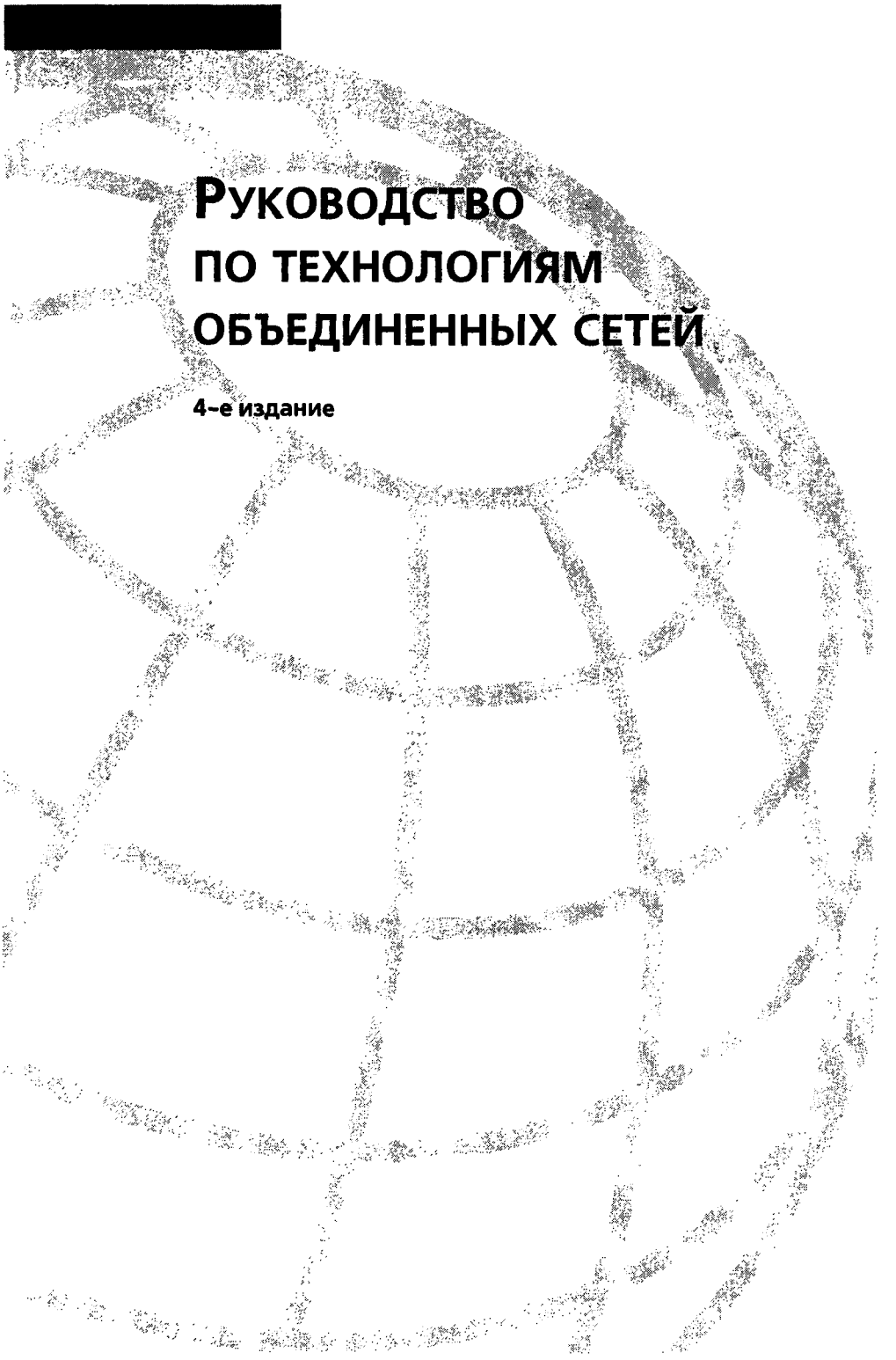
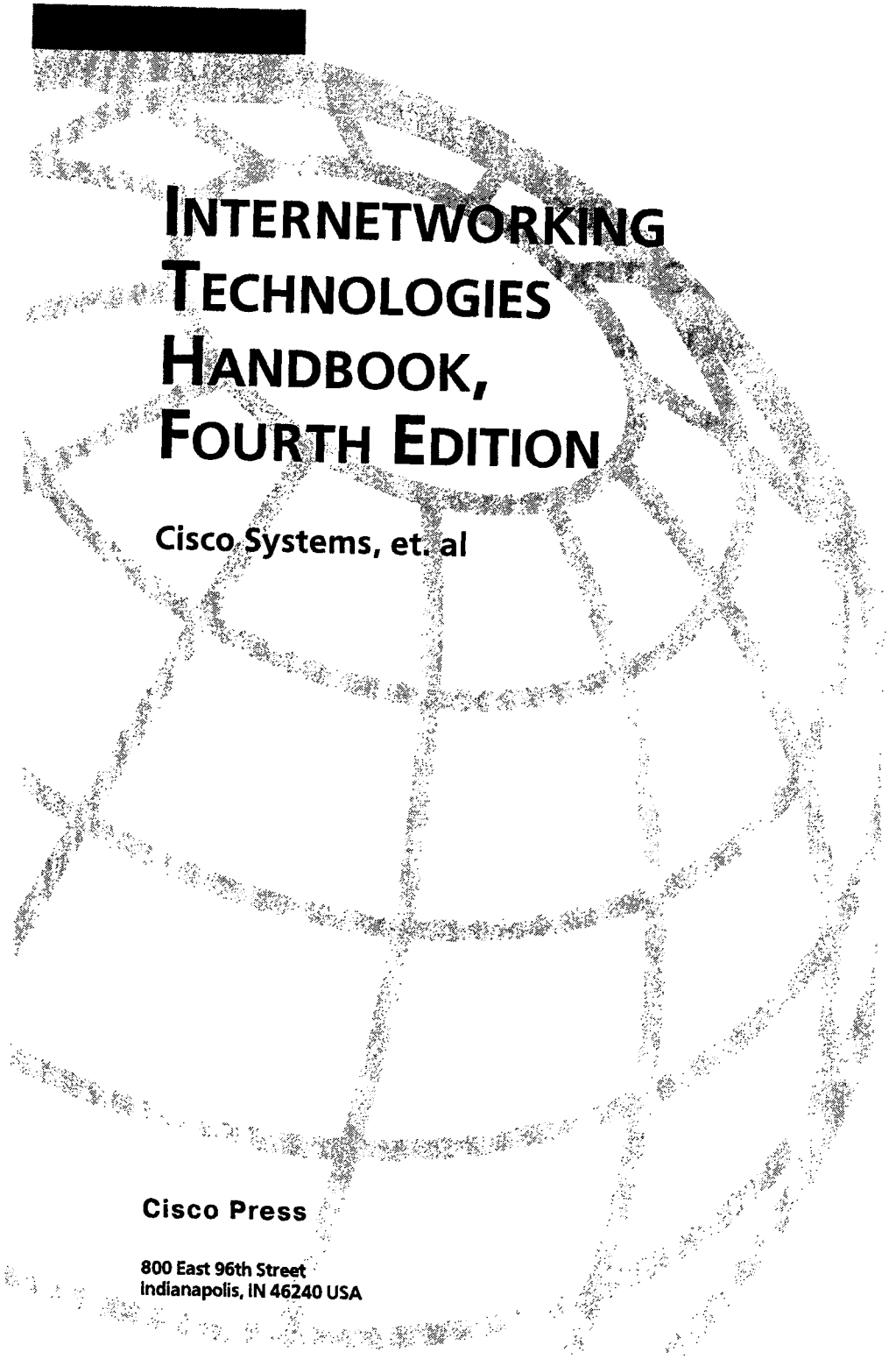


Руководство по технологиям объединенных сетей

4-е издание



INTERNETWORKING TECHNOLOGIES HANDBOOK, FOURTH EDITION

Cisco Systems, et. al

Cisco Press

800 East 96th Street
Indianapolis, IN 46240 USA

Руководство по технологиям объединенных сетей

4-е издание

Cisco Systems, Inc.

Москва • Санкт-Петербург • Киев
2005

ББК 32.973.26-018.2.75
Р84
УДК 681.3.07

Издательский дом "Вильямс"

Зав. редакцией *С.Н. Тригуб*

Перевод с английского и редакция *А.Н. Крикуна*

По общим вопросам обращайтесь в Издательский дом "Вильямс" по адресу:
info@williamspublishing.com, http://www.williamspublishing.com
115419, Москва, а/я 783, 03150, Киев, а/я 152.

Cisco Systems, Inc.

Р84 Руководство по технологиям объединенных сетей, 4-е издание. : Пер. с англ. — М. : Издательский дом "Вильямс", 2005. — 1040 с. : ил. – Парал. тит. англ.

ISBN 5-8459-0787-X (рус.)

Книга представляет собой обширный справочник, содержащий описаиие практически всех используемых в настоящее время сетевых протоколов и технологий. В книге рассмотрен широкий спектр вопросов межсетевого взаимодействия, включая протоколы локальных сетей, технологии распределенных сетей, мостовые и коммутируемые соединения, а также управление сетями. В ней также описаиы разрабатываемые в настоящее время протоколы и сетевые технологии. Приведена информация о последних разработках корпорации Cisco в сфере обеспечения безопасности сетей, их масштабируемости и повышения скорости передачи, а также о сетях хранения данных и об оптических сетях.

Киига предназначена для специалистов по сетевым технологиям.

ББК 32.973.26-018.2.75

Киига подготовлена прн участнн Региональной сетевой академии Cisco, http://www.academy.ciscopress.ru.

ISBN 5-8459-0787-X (рус.)
ISBN 1-58705-119-2 (англ.)

Оглавление

Часть I. Основы теории объединенных сетей **45**

Глава 1. Основные понятия теории объединенных сетей 47
Глава 2. Основы протоколов локальных сетей 73
Глава 3. Основные технологии распределенных сетей 81
Глава 4. Начальные сведения о программном обеспечении IOS Cisco 91
Глава 5. Основы мостовых и коммутируемых соединений 103
Глава 6. Основы маршрутизации 111
Глава 7. Основные принципы управления сетями 123

Часть II. Технологии локальных сетей **129**

Глава 8. Технологии Ethernet 131
Глава 9. Интерфейс FDDI 171

Часть III. Технологии распределенных сетей **183**

Глава 10. Протокол Frame Relay 185
Глава 11. Интерфейс HSSI 199
Глава 12. Технология ISDN 203
Глава 13. Протокол PPP 211
Глава 14. Служба SMDS 217
Глава 15. Коммутируемые соединения 229
Глава 16. Протокол SDLC и его производные 245
Глава 17. Протокол X.25 253
Глава 18. Виртуальные частные сети 263

Часть IV. Технологии мультисервисного доступа **279**

Глава 19. Интегрированная передача голосовых и обычных данных 281
Глава 20. Беспроводные технологии 317
Глава 21. Цифровые абонентские каналы 361
Глава 22. Технологии кабельного доступа 375
Глава 23. Введение в технологии оптических сетей 395

Глава 24. Технология передачи голосовых данных по протоколу IP (Voice over IP — VoiceIP) 415
Глава 25. Протоколы динамической транспортировки пакетов и эффективного использования полосы пропускания 455
Глава 26. Протокол расширяемой аутентификации (Extensible Authentication Protocol — EAP) 467

Часть V. Мосты и переключатели 477

Глава 27. Прозрачные мостовые соединения 479
Глава 28. Мостовое соединение разнородных сетей 487
Глава 29. Мостовая маршрутизация от источника 495
Глава 30. Коммутируемые локальные сети и сети VLAN 501
Глава 31. Коммутация в режиме ATM 509
Глава 32. Коммутация MPLS 537
Глава 33. Технология DLSw 553

Часть VI. Сетевые протоколы 567

Глава 34. Протоколы взаимодействия открытых систем 569
Глава 35. Протоколы Internet 579
Глава 36. Протокол IPv6 597
Глава 37. Протоколы NetWare 605
Глава 38. Протоколы AppleTalk 613
Глава 39. Протоколы сетевой архитектуры IBM 637
Глава 40. Протоколы DECnet 651

Часть VII. Протоколы маршрутизации 663

Глава 41. Протокол BGP 665
Глава 42. Протокол EIGRP 677
Глава 43. Маршрутизация в системной сетевой архитектуре IBM 685
Глава 44. Протокол IGRP 697
Глава 45. Многоадресатная рассылка 703
Глава 46. Протокол NSLP 721
Глава 47. Протокол OSPF 731
Глава 48. Протоколы маршрутизации OSI 739
Глава 49. Протокол RIP 757
Глава 50. Протокол RSVP 763
Глава 51. Протокол SMRP 777

Часть VIII. Управление сетями **789**
Глава 52. Технологии защиты сетей 791
Глава 53. Сетевые каталоги 807
Глава 54. Технологии сетевого кэширования 833
Глава 55. Сети для хранения информации 851
Глава 56. Управление сетями IBM 879
Глава 57. Удаленный мониторинг 887
Глава 58. Протокол SNMP 891
Глава 59. Качество обслуживания 909

Часть IX. Приложения **947**
Приложение А. Ответы на контрольные вопросы 949
Приложение Б. Традиционные технологии 995

Предметный указатель 1013

Содержание

Цели авторов 35
Изменения в четвертом издании 35
Для кого предназначена эта книга 36
Структура книги 36
Благодарности участникам настоящего издания 37
Участники третьего издания 40
Авторы первого издания 40
Используемые в книге пиктограммы 40
Обозначения, используемые в командах 41
От издательства 43

Часть I. Основы теории объединенных сетей 45

Глава 1. Основные понятия теории объединенных сетей 47

Что такое объединенная сеть? 47
- История объединенных сетей 47
- Проблемы создания объединенных сетей 48

Эталонная модель взаимодействия открытых систем 49
- Характеристики уровней эталонной модели OSI 50
- Протоколы 51
- Модель OSI и обмен данными между компьютерными системами 52
- Физический уровень модели OSI 55
- Канальный уровень эталонной модели OSI 55
- Сетевой уровень эталонной модели OSI 56
- Транспортный уровень эталонной модели OSI 57
- Сеансовый уровень модели OSI 57
- Уровень представления эталонной модели OSI 57
- Уровень приложений модели OSI 58

Информационные форматы 58
Иерархия сетей по стандарту ISO 60
Сетевые службы, ориентированные на соединение, и службы, не требующие подтверждения соединения 60
Адресация в объединенных сетях 62
- Адреса канального уровня 62
- MAC-адреса 63
- Преобразование адресов 64
- Адреса сетевого уровня 65
- Иерархическое и линейное пространства адресов 66
- Назначение адресов 66
- Адреса и имена устройств 67

Основы управления потоком 67
Основы контроля ошибок 68
Основы мультиплексирования 68
Разработчики стандартов 69
Резюме 70
Контрольные вопросы 71
Дополнительные источники 71

Глава 2. Основы протоколов локальных сетей 73

Что такое локальная сеть? 73
Протоколы локальных сетей и эталонная модель OSI 74
Методы доступа к среде передачи в локальных сетях 74
Методы передачи данных в локальных сетях 76
Топологии локальных сетей 76
Устройства локальных сетей 78
Дополнительные источники 79
Контрольные вопросы 79

Глава 3. Основные технологии распределенных сетей 81

Что такое распределенная сеть? 81
Соединения типа "точка-точка" 81
Коммутация каналов 82
Коммутация пакетов 83
Виртуальные каналы в распределенной сети 84
Службы удаленного доступа к распределенным сетям 85
Устройства, применяемые в распределенных сетях 85
Коммутатор распределенной сети 85
Сервер доступа 85
Модем 86
Модули CSU/DSU 86
Терминальный адаптер сети ISDN 87
Контрольные вопросы 88
Дополнительные источники 88

Глава 4. Начальные сведения о программном обеспечении IOS Cisco 91

Системная структура 91
Интерфейс командной строки IOS Cisco (CLI) 93
Отладка и загрузка 97
Перезагрузка и обновление программного обеспечения 99
Резюме 101
Контрольные вопросы 101
Дополнительные источники 101

Глава 5. Основы мостовых и коммутируемых соединений 103

Что такое мосты и коммутаторы? 103
Обзор устройств канального уровня 104
Типы мостов 105

Типы коммутаторов 107
Коммутаторы ATM 107
Коммутаторы локальных сетей 107
Контрольные вопросы 108
Дополнительные источники 109

Глава 6. Основы маршрутизации 111

Что такое маршрутизация? 111
Компоненты маршрутизации 111
Определение маршрута 112
Коммутация 113
Алгоритмы маршрутизации 114
Цели, которые ставятся при разработке алгоритмов маршрутизации 114
Типы алгоритмов маршрутизации 116
Сетевые протоколы 119
Контрольные вопросы 120

Глава 7. Основные принципы управления сетями 123

Введение 123
Что понимается под управлением сетью? 123
Историческая справка 123
Архитектура системы управления сетью 124
Модель управления сетью ISO 124
Управление производительностью 124
Управление конфигурацией 125
Управление учетными записями 126
Управление отказоустойчивостью 126
Управление безопасностью 127
Контрольные вопросы 127

Часть II. Технологии локальных сетей 129

Глава 8. Технологии Ethernet 131

Введение 131
Краткая история сетей Ethernet 131
Элементы сетей Ethernet 132
Топологии и структуры сетей Ethernet 132
Связь стандарта IEEE 802.3 и эталонной модели OSI 133
MAC-подуровень Ethernet 135
Основной формат фрейма Ethernet 136
Передача фрейма 137
Получение фреймов 141
Использование дескрипторов виртуальных сетей VLAN 142
Физические уровни Ethernet 143
Кодирование передаваемого сигнала 143
Взаимосвязь между физическим уровнем 802.3 и эталонной моделью OSI 145
Спецификация Ethernet 10BaseT (скорость передачи 10 Мбит/с) 147

Спецификация Fast Ethernet (скорость передачи 100 Мбит/с) 148
Спецификация Gigabit Ethernet — 1000 Мбит/с 153
Требования к пересечениям сетевых кабелей 157
Системные требования 158
Выбор компонентов и категории среды передачи для неэкранированной витой пары 159
Автосогласование — дополнительный метод автоматической настройки режимов работы канала 159
Возможная альтернатива высокоскоростных каналов в модернизированных сетях CSMA/CD — сетевые коммутаторы 161
Многоскоростные сетевые адаптеры 162
Выбор компонентов и среды передачи для сети 1000BaseX 162
Многоскоростные сети Ethernet 164
Объединение каналов и создание высокоскоростных сетевых магистралей 166
Управление сетью 167
Переход на высокоскоростные сети 167
Резюме 167
Контрольные вопросы 168

Глава 9. Интерфейс FDDI 171

Введение 171
Стандарты 171
Среда передачи интерфейса FDDI 172
Спецификации интерфейса FDDI 173
Типы подключения станций в протоколе FDDI 174
Отказоустойчивость FDDI 175
Двойное кольцо 175
Оптический обходной переключатель 177
Двойное подключение 178
Формат фрейма FDDI 178
Поля фрейма FDDI 179
Интерфейс CDDI 180
Резюме 181
Контрольные вопросы 181

Часть III. Технологии распределенных сетей 183

Глава 10. Протокол Frame Relay 185

Введение 185
Стандартизация Frame Relay 186
Устройства сетей протокола Frame Relay 186
Виртуальные каналы протокола Frame Relay 187
Коммутируемые виртуальные каналы 188
Постоянные виртуальные каналы 188
Идентификатор канального соединения 189
Механизмы управления переполнением 189
Бит допустимости отбрасывания во фреймах Frame Relay 190

Контроль ошибок в сетях Frame Relay 190
Интерфейс локального управления Frame Relay 190
Сетевые реализации протокола Frame Relay 191
Общедоступные сети 191
Частные сети 192
Форматы фреймов Frame Relay 192
Стандартный фрейм протокола Frame Relay 193
Формат LMI-фрейма 194
Резюме 195
Контрольные вопросы 196

Глава 11. Интерфейс HSSI 199

Введение 199
Основы интерфейса HSSI 199
Функционирование интерфейса HSSI 200
Контроль образования маршрутных петель 200
Резюме 201
Контрольные вопросы 201

Глава 12. Технология ISDN 203

Устройства ISDN 203
Службы ISDN 205
Служба BRI-интерфейса в сети ISDN 205
Служба PRI-интерфейса ISDN 205
Спецификации ISDN 205
1-й уровень (физический) 205
2-й уровень (канальный) 206
3-й уровень 207
Резюме 209
Контрольные вопросы 209

Глава 13. Протокол PPP 211

Введение 211
Компоненты протокола PPP 211
Основные принципы работы протокола PPP 212
Требования, определяемые физическим уровнем 212
Канальный уровень протокола PPP 212
Протокол управления каналом (LCP) стека протоколов PPP 213
Резюме 214
Контрольные вопросы 215

Глава 14. Служба SMDS 217

Введение 217
Сетевые компоненты службы SMDS 217
Протокол интерфейса SMDS 218
Уровни SIP 218
Шина DQDB 220

Классы доступа SMDS 221
Основы адресации SMDS 221
Стандарт SMDS: формат модуля PDU 3-го уровня интерфейса SIP 222
Стандарт SMDS: формат модуля PDU 2-го уровня интерфейса SIP 223
Резюме 225
Контрольные вопросы 225

Глава 15. Коммутируемые соединения 229

Введение 229
Краткая история коммутируемых соединений 229
Технология коммутируемых соединений 231
Общедоступная телефонная сеть 231
Базовый интерфейс ISDN 232
Линии T1/E1 232
Интерфейс первичной скорости передачи 233
Канально-ассоциированная сигнальная система 233
Модемы 234
Протокол PPP 236
Дополнительные замечания 238
Протокол аутентификации, авторизации и учета (AAA) 238
Методы реализации коммутируемых соединений 239
Что такое номеронабиратель? 239
Представляющие интерес данные 240
Преимущества и недостатки коммутируемых соединений 240
Резюме 241
Контрольные вопросы 242
Дополнительные источники 243

Глава 16. Протокол SDLC и его производные 245

Введение 245
Типы каналов и топологии SDLC 245
Формат фрейма протокола SDLC 246
Производные протоколы 247
Протокол HDLC 248
Протокол LAPB 249
Протокол IEEE 802.2 249
Протокол ограниченного управления логическим каналом (QLLC) 250
Резюме 250
Контрольные вопросы 251

Глава 17. Протокол X.25 253

Введение 253
Устройства протокола X.25 и его функционирование 253
Сборщик/разборщик пакетов 254
Создание сеанса X.25 255
Виртуальные каналы X.25 255
Набор протоколов X.25 256
Протокол PLP 256

Протокол LAPB 257
Протокол X.21bis 258
Формат фрейма протокола LAPB 258
Формат адреса X.121 259
Резюме 260
Контрольные вопросы 260

Глава 18. Виртуальные частные сети 263

Определение сетей VPN 263
VPN-приложения 264
Технология IPSec 264
Заголовок аутентификации 266
Нагрузка безопасности 267
Транспортный и туннельный режимы IPSec 268
Параметры безопасности (Security Association — SA) 269
Протокол обмена ключами в Internet (Internet Key Exchange — IKE) 269
Протокол создания туннелей на 2-м уровне (Layer 2 Tunneling Protocol — L2TP) 270
Топологии реализации 271
Соединения протокола L2TP, защищенные посредством IPSec 273
VPN-сети в MPLS-сетях 273
VPN-сети BGP/MPLS 274
VPN-сети 2-го уровня на базе коммутации MPLS 276
Резюме 277
Контрольные вопросы 277
Дополнительные источники 277

Часть IV. Технологии мультисервисного доступа 279

Глава 19. Интегрированная передача голосовых и обычных данных 281

Введение 281
Стандарты 281
Технология 282
Производительность сети 282
Экономическая эффективность 283
Совершенствование приложений 283
Современные технологии передачи голосовых данных 285
Сети для передачи голосовых данных 286
Основы телефонии 286
Передача голоса по сетям ATM 288
Сигнализация в сетях VoATM 289
Адресация в сетях VoATM 290
Маршрутизация VoATM 291
Задержки в VoATM 291
Передача голоса по сетям Frame Relay 292
Сигнализация VoFR 292
Адресация VoFR 292
Передача голоса по протоколу IP 293

Обзор голосовых кодеков 293
Ограничения при разработке сетей VoIP 296
Качество обслуживания для VoIP 301
Обзор стандарта H.323 302
Поток вызовов H.323 и взаимодействие протоколов 304
Кратко о протоколе MGCP 304
Основные понятия MGCP 305
Преимущества MGCP 306
Терминология протокола MGCP 306
Основы SIP 308
Сообщения SIP 309
Адресация SIP 310
Поток вызова SIP 310
Протокол управления работой пользователя 310
Сравнение альтернатив передачи сигналов VoIP 311
Развитие систем интегрированной передачи голоса и данных 312
Будущие приложения для телефонии 313
Стимулы создания приложений пакетной телефонии 314
Резюме 315
Контрольные вопросы 315
Дополнительные источники 315

Глава 20. Беспроводные технологии 317

Введение 317
Основы беспроводной связи 317
Основы радиосвязи 317
Компоненты беспроводной системы связи 318
Электромагнитный спектр 320
Теория передачи сигналов в диапазоне радиочастот RF 322
Беспроводная связь вне пределов видимости: уменьшение влияния наложения сигналов в высокоскоростных линиях 331
Наложение сигналов 331
Каналы микроволновой связи 333
Наложение сигналов в системах без прямой видимости 333
Методы модулирования и кодирования сигналов с использованием QAM 334
Улучшенные технологии сигнализации для уменьшения наложения сигналов 335
Квадратурно-амплитудная модуляция с обратной связью 336
Широкополосная модуляция 337
Системы FHSS 339
Системы FDM 339
Системы OFDM 339
Системы VOFDM 340
Элементы единой сети 341
Абонентские сети 341
Сети доступа 341
Базовые сети 342
Управление сетью 342
Развертывание 343
Беспроводные локальные сети WLAN 343

Обзор WLAN 343
WLAN-архитектура 345
Службы распределения 346
Резюме 348
Контрольные вопросы 350
Дополнительные источники 350
Акты и постановления 352
WLL 352
LMDS/MMDS 353
Беспроводные системы 353
Спутниковая связь 353
Модуляция 354
Интерфейсы 354
Глоссарий 354

Глава 21. Цифровые абонентские каналы 361

Введение 361
Технология ADSL 361
Возможности технологии ADSL 362
Технология ADSL 364
Управляющие сигналы и модуляция 366
CAP- и DMT-модулирование ADSL 366
Стандарты и объединения ADSL 368
Другие технологии DSL 368
SDSL 368
HDSL 369
HDSL-2 369
G.SHDSL 370
Цифровой абонентский канал ISDN 370
VDSL 371
Резюме 371
Контрольные вопросы 372
Дополнительные источники 372

Глава 22. Технологии кабельного доступа 375

Введение 375
Эволюция от однонаправленного вещания к двусторонним гибридным коаксиально-волоконным сетям 376
Характеристики и ограничения HFC-сетей 377
Стандарты, сигнальные протоколы и приложения DOCSIS 380
Внедрение систем DOCSIS и их возможности 386
Перспективные приложения DOCSIS 390
Резюме 391
Контрольные вопросы 392
Дополнительные источники 392
Книги 392
Адреса URL 392
Периодические издания 393

Глава 23. Введение в технологии оптических сетей 395
Что такое оптическая сеть? 395
Мультиплексирование по частотам и мультиплексирование с уплотнением по частотам 396
Оптический кабель к домашнему офису пользователя (Fiber to the Home — FTTH) 396
Полностью оптические сети 396
Пассивные оптические сети 397
Домашние и коммерческие PON-сети 397
Модули оптических сетей и терминалы оптических сетей 398
Пассивные оптические сети Ethernet 398
Сети доступа городского масштаба (сети Metro) 398
Прозрачные оптические сети 399
Транспортные сети 399
Сети передачи данных на большие расстояния 399
Сети передачи на дальние расстояния 400
Сети передачи на сверхдальние расстояния 401
Оптические сети Gigabit Ethernet и 10 Gigabit Ethernet 401
Обобщенная многопротокольная коммутация по метке 402
Маршрутизаторы с коммутацией по метке 402
Протокол управления каналом 404
Интерфейс "пользователь–сеть" 405
G.ASON 405
Управляющая плоскость 406
Объединенная контрольная плоскость 407
Конфигурация сети наложения 408
Одноранговая модель 408
Полная одноранговая модель 408
Модель фильтрованной пары и усовершенствованная модель 408
Интерфейс сети пользователя оптической управляющей плоскости 409
Оптический интерфейс "сеть–сеть" оптической управляющей плоскости 410
Обеспечение безопасности и восстановление работы сети в сетях следующего поколения 410
Резюме 411
Контрольные вопросы 412
Дополнительные источники 412

Глава 24. Технология передачи голосовых данных по протоколу IP (Voice over IP — VoiceIP) 415
Сетевые устройства протокола H.323 417
Терминалы H.323 417
Драйверы шлюзов протокола H.323 418
Каталоговые драйверы шлюзов протокола H.323 419
Шлюзы протокола H.323 419
Многоточечный управляющий модуль (Multipoint Control Unit — MCU) 420
Стек протоколов H.323 420
Спецификация H.323 421

Спецификация H.225 422
Протокол H.245 427
Протокол H.450 431
Аудиокодеки 432
Протокол H.225 RAS 434
Протокол инициализации сеанса (Session Initiation Protocol — SIP) 440
Сообщения протокола SIP 440
Протокол описания сеанса 443
Сетевые устройства протокола SIP 444
Обмен сообщениями при установке вызова в протоколе SIP 446
Соединение сети VoIP с сетью SS7 448
Резюме 449
Контрольные вопросы 451
Дополнительные источники 451
H.323 451
SIP 451
Соединения SS7 для голосовых шлюзов 451
Глоссарий 452

Глава 25. Протоколы динамической транспортировки пакетов и эффективного использования полосы пропускания 455

Структура протокола DPT 455
Оптимизация использования полосы пропускания в протоколе SRP 456
Приоритеты пакетов в протоколе SRP 458
Алгоритм установки справедливой очередности протокола SRP 458
Эластичность протокола DPT 459
Анализ топологии 460
Форматы пакетов протоколов DPT/SRP 461
Общий формат заголовка протокола SRP версии 2 461
Пакет данных протокола SRP 462
Управляющий пакет протокола SRP 463
Поддержка многоадресатной рассылки 464
Резюме 464
Контрольные вопросы 465
Дополнительные источники 465
Глоссарий 465

Глава 26. Протокол расширяемой аутентификации (Extensible Authentication Protocol — EAP) 467

Протокол EAP 468
Использование службы RADIUS для аутентификации EAP 470
Типичное обсуждение аутентификации 471
Поддержка инфраструктуры PKI с помощью протокола EAP 471
Безопасность протокола EAP на транспортном уровне (EAP-Transport Layer Security — EAP-TLS) 472
Защищенный протокол EAP (Protected EAP—PEAP) 472
Реализации протокола EAP 473

Резюме 474
Контрольные вопросы 474
Дополнительные источники 474

Часть V. Мосты и переключатели 477

Глава 27. Прозрачные мостовые соединения 479

Функционирование прозрачного мостового соединения 479
Мостовые петли 480
Алгоритм связующего дерева 480
Формат фреймов 483
Контрольные вопросы 484
Дополнительные источники 485

Глава 28. Мостовое соединение разнородных сетей 487

Введение 487
Проблемы трансляции 487
Мостовое соединение с трансляцией 489
Прозрачная мостовая маршрутизация от источника 492
Контрольные вопросы 492
Дополнительные источники 493

Глава 29. Мостовая маршрутизация от источника 495

Введение 495
SRB-алгоритм 495
Формат фрейма 497
Поле управления маршрутом 497
Поле описания маршрута 498
Контрольные вопросы 498
Дополнительные источники 499

Глава 30. Коммутируемые локальные сети и сети VLAN 501

История коммутаторов 501
Функционирование коммутатора LAN 502
Сети VLAN 502
Режимы портов коммутаторов 503
Передача данных в коммутируемой локальной сети 504
Пропускная способность коммутируемой локальной сети 505
Коммутируемые локальные сети и эталонная модель OSI 505
Контрольные вопросы 506
Дополнительные источники 506

Глава 31. Коммутация в режиме ATM 509

Стандарты 509
Устройства ATM и сетевая среда 510
Основной формат ячейки ATM 510
Устройства ATM 511

Сетевые интерфейсы ATM 511
Формат заголовка ячейки ATM 512
Поля заголовка ячейки ATM 513
Службы ATM 513
Виртуальные соединения ATM 514
ATM-коммутация 514
Эталонная модель ATM 514
Физический уровень ATM 515
Адаптационные уровни ATM: AAL1 516
Адаптационные уровни ATM: AAL2 517
Уровни адаптации ATM: AAL3/4 517
Уровни адаптации ATM: AAL5 518
Адресация ATM 519
Подсетевая модель адресации 519
Формат NSAP ATM-адресов 519
Поля адреса ATM 520
ATM-соединения 521
ATM и многоадресатная передача 522
Качество обслуживания ATM 523
Сигнализация и установка соединения ATM 523
Установка ATM-соединения 524
Маршрутизация и согласование запросов на соединение 524
Сообщения управления соединением ATM 524
Интерфейс PNNI 525
Интерфейс ILMI 525
Эмуляция LAN 526
Архитектура протокола LANE 526
Компоненты LANE 527
Типы соединений в эмулированной LAN 529
Функционирование LANE 530
Многопротокольная схема в ATM 532
Контрольные вопросы 533
Дополнительные источники 534

Глава 32. Коммутация MPLS 537

Введение 537
Терминология MPLS 538
Функционирование коммутации MPLS 539
Структура коммутации MPLS и коммутации по тегам 540
Компонент управления 541
Протокол распространения меток 542
Компонент пересылки по метке 543
Инкапсуляция меток 545
Коммутация по метке в сетях ATM 545
Иерархическая маршрутизация 546
Виртуальные частные сети на основе коммутации MPLS 547
Качество обслуживания в сетях коммутации MPLS 549
Перераспределение потоков в MPLS-сетях 549
Резюме 550

Контрольные вопросы 551
Дополнительные источники 551

Глава 33. Технология DLSw 553

Введение 553
Сравнение DLSw и SRB 554
Поддержка SNA в технологии DLSw 555
Протокол SSP 556
Функционирование DLSw 556
Процессы DLSw 558
Форматы DLSw-сообщений 561
Контрольные вопросы 564

Часть VI. Сетевые протоколы 567

Глава 34. Протоколы взаимодействия открытых систем 569

Введение 569
Сетевые протоколы OSI 569
Физический и канальный уровни OSI 569
Сетевой уровень OSI 570
Протоколы OSI транспортного уровня 573
Протоколы OSI сеансового уровня 574
Протоколы OSI уровня представления 574
Протоколы OSI уровня приложений 575
Контрольные вопросы 577

Глава 35. Протоколы Internet 579

Введение 579
Протокол IP 580
Формат IP-пакета 580
IP-адресация 582
Основные сведения о протоколе ARP 587
Маршрутизация Internet 588
IP-маршрутизация 588
Протокол ICMP 589
Сообщения протокола ICMP 589
Протокол IDRP 589
Протокол TCP 590
Установка TCP-соединения 590
Подтверждение приема и повторная передача 591
Скользящее окно TCP 591
Формат TCP-пакета 592
Описание полей TCP-пакета 592
Протокол UDP 593
Internet-протоколы уровня приложений 593
Резюме 594
Контрольные вопросы 595

Глава 36. Протокол IPv6 **597**
Заголовок пакета IPv6 597
Шестнадцатеричный формат 598
Адресация 598
Способы передачи 598
Одноадресатная передача 599
Многоадресатная передача 599
Широковещательная передача 599
Резюме 601
Контрольные вопросы 601
Дополнительные источники 602

Глава 37. Протоколы NetWare **605**
Введение 605
Доступ NetWare к среде передачи 605
Основные сведения о протоколе IPX 606
Типы инкапсуляции протокола IPX 607
Протокол SAP 608
Фильтры SAP 608
Транспортный уровень NetWare 609
Протоколы и службы верхнего уровня NetWare 609
Службы NetWare уровня приложений 610
Формат пакета IPX 610
Резюме 611
Контрольные вопросы 611

Глава 38. Протоколы AppleTalk **613**
Введение 613
Компоненты сетей AppleTalk 613
Сокеты 614
Узлы 615
Сети 615
Зоны 616
Физический и канальный уровни в сетях AppleTalk 616
EtherTalk 617
Протокол LocalTalk 619
Протокол TokenTalk 620
Протокол FDDITalk 620
Сетевые адреса 621
Назначение сетевого адреса 621
Протокол AARP 622
Таблица соответствия адресов 622
Сбор адресов 623
Функционирование AARP 623
Основные сведения о протоколе DDP 623
Процесс передачи данных по протоколу DDP 624
Транспортный уровень AppleTalk 624

Основные сведения о протоколе RTMP 625
Основные сведения о протоколе NBP 625
Протокол AURP 627
Протокол ATP 628
Протокол AEP 629
Протоколы верхнего уровня в сетях AppleTalk 629
Протокол ADSP 629
Протокол ZIP 630
Протокол ASP 630
Основные сведения о протоколе PAP 630
Протокол AFP 631
Стек протоколов AppleTalk 631
Формат DDP-пакетов 632
Резюме 632
Контрольные вопросы 634
Дополнительные источники 634

Глава 39. Протоколы сетевой архитектуры IBM 637

Введение 637
Традиционные среды SNA 637
Системная сетевая архитектура IBM 638
Физические элементы IBM SNA 639
Управление каналом в архитектуре IBM SNA 639
Адресуемые сетевые модули IBM 641
Узлы IBM SNA 641
Равноправная сеть IBM 642
Компоненты APPN 642
Типы узлов IBM APPN 643
Службы APPN IBM 643
Формат базового информационного модуля 646
Поля BIU 646
Формат маршрутного информационного модуля 647
Поля PIU 648
Резюме 649
Контрольные вопросы 649
Дополнительные источники 649

Глава 40. Протоколы DECnet 651

Введение 651
Архитектура DECnet Phase IV 652
Уровни DNA Phase IV 652
Адресация протокола DECnet Phase IV 653
Архитектура DECnet/OSI 654
Реализации DNA DECnet/OSI 654
Доступ DECnet к среде передачи 654
Маршрутизация DECnet 655
Уровень конечных коммуникаций DECnet 656
Протокол NSP 656

Транспортный уровень DECnet/OSI 656
Верхние уровни DECnet Phase IV 657
Уровень пользователя 657
Уровень управления сетью 657
Уровень сетевых приложений 658
Уровень управления сеансом 658
Верхние уровни DECnet/OSI 658
Уровень приложений 658
Уровень представления 659
Сеансовый уровень 659
Резюме 659
Контрольные вопросы 659

Часть VII. Протоколы маршрутизации 663

Глава 41. Протокол BGP 665

Введение 665
Атрибуты протокола BGP 666
Атрибут Weight 667
Атрибут Local Preference 667
Атрибут Multi-exit Discriminator 668
Атрибут Origin 668
Атрибут AS_path 669
Атрибут Next-Hop 669
Атрибут Community 671
Выбор маршрута по протоколу BGP 672
Контрольные вопросы 673
Дополнительные источники 674

Глава 42. Протокол EIGRP 677

Возможности и атрибуты протокола Enhanced IGRP 677
Основные процессы и технологии 678
Концепции маршрутизации 679
Таблицы соседних маршрутизаторов 679
Топологические таблицы 680
Состояния маршрутов 680
Маркировка маршрута 680
Типы пакетов протокола Enhanced IGRP 681
Резюме 681
Контрольные вопросы 682
Дополнительные источники 682

Глава 43. Маршрутизация в системной сетевой архитектуре IBM 685

Введение 685
Сеансовые соединители SNA 685
Группы передачи SNA IBM 686
Явные и виртуальные маршруты SNA IBM 686

Класс обслуживания SNA IBM 687
CoS при подзональной маршрутизации 687
Механизм классов CoS при использовании маршрутизации APPN 688
Подзональная маршрутизация SNA IBM 689
Маршрутизация IBM APPN 689
Маршрутизация узлов типа 2.1 в APPN IBM 690
Маршрутизация промежуточного сеанса 691
Маршрутизация DLUR/S APPN IBM 692
Сеть соединений APPN 693
Граничный узел APPN IBM 693
Контрольные вопросы 693

Глава 44. Протокол IGRP 697

Характеристики протокола IGRP 697
Функции повышения стабильности 698
Таймеры 699
Резюме 700
Контрольные вопросы 700
Дополнительные источники 700

Глава 45. Многоадресатная рассылка 703

Введение 703
Понятие группы многоадресатной рассылки 703
IP-адреса многоадресатной рассылки 704
IP-адреса класса D 704
Зарезервированные локальные адреса 705
Глобальные адреса 705
Адреса ограниченного радиуса действия 705
Статические адреса (GLOP-адресация) 705
Адреса многоадресатной рассылки 2-го уровня 706
Преобразование MAC-адреса Ethernet 706
Протокол IGMP 706
Протокол IGMP версии 1 707
Протокол IGMP версии 2 708
Многоадресатная рассылка в среде коммутации на 2-м уровне 708
Протокол CGMP 709
IGMP-прослушивание 709
Связующие деревья многоадресатной рассылки 710
Дерево от источника 710
Дерево общего доступа 710
Многоадресатная рассылка 712
Обратная передача 713
Независимая от протокола многоадресатная рассылка 714
Плотный режим протокола PIM 714
Разреженный режим PIM 715
Разреженно-плотный режим 715
Протокол MBGP 715
Протокол MSDP 716

Альтернативная и логическая точки рандеву 717
Протокол MADCAP 718
Протокол MZAP 718
Протокол надежной многоадресатной рассылки 719
Контрольные вопросы 719
Дополнительные источники 719

Глава 46. Протокол NSLP 721

Введение 721
Иерархическая маршрутизация в NSLP 722
Эффективность иерархической маршрутизации 722
Смежность в NSLP 723
Отправка пакетов приветствия в LAN 724
Функционирование NSLP 724
Иерархическая адресация протокола NSLP 725
Пакеты приветствия NSLP 726
Пакет приветствия WAN 726
Пакеты приветствия NSLP LAN 727
Контрольные вопросы 729

Глава 47. Протокол OSPF 731

Иерархия маршрутизации 732
Алгоритм SPF 733
Формат пакета 734
Дополнительные функции протокола OSPF 735
Контрольные вопросы 736

Глава 48. Протоколы маршрутизации OSI 739

Введение 739
Терминология OSI 739
Обзор операций маршрутизации протокола OSI 740
Протокол ES-IS 741
Конфигурирование протокола ES-IS 741
Адресация протокола ES-IS 742
Протокол IS-IS 742
Объединенный протокол IS-IS 742
Структура маршрутизации протокола IS-IS 743
Типы пакетов 744
Значения TLV 747
Метрики протокола IS-IS 748
Обработка LSP-пакетов протокола IS-IS 749
Выбор DIS-системы протокола IS-IS 750
Обход "черных дыр" с использованием протокола IS-IS 750
Проникновение маршрутов 751
Перераспределение потоков в сетях MPLS 751
Протокол IDRP 751
Терминология IDRP 752
IDRP-маршрутизация 753

Резюме 753
Контрольные вопросы 753
Дополнительные источники 754

Глава 49. Протокол RIP 757

Введение 757
Обновление маршрутов 757
Метрика маршрута RIP 758
Функции обеспечения устойчивости протокола RIP 758
Таймеры RIP 758
Форматы пакетов 759
Формат пакета RIP 759
Формат пакета RIP 2 759
Резюме 760
Контрольные вопросы 761
Дополнительные источники 761

Глава 50. Протокол RSVP 763

Введение 763
Потоки данных протокола RSVP 763
Обработка потоков данных по протоколу RSVP 765
Качество обслуживания RSVP 766
Запуск сеанса RSVP 766
Стиль резервирования RSVP 766
Стиль групповой фильтрации 766
Стиль фиксированной фильтрации 767
Стиль явного совместного резервирования 767
Гибкое состояние RSVP 768
Функционирование RSVP 768
Основные операции протокола RSVP 768
Туннели протокола RSVP 769
RSVP-сообщения 770
Запросы на резервирование 770
Маршрутные сообщения 771
Сообщения об ошибках и подтверждения 771
Сообщения о разрыве 771
Формат пакета RSVP 772
Поля заголовка RSVP-сообщения 772
Поля объектов RSVP 773
Резюме 773
Контрольные вопросы 775
Дополнительные источники 775

Глава 51. Протокол SMRP 777

Введение 777
Многоадресатные транспортные службы SMRP 779
Управление групповыми SMRP-адресами 779
Протокол многоадресатной передачи SMRP 780

Управление SMRP-узлами 781
Многоадресатные маршруты протокола SMRP 782
Управление многоадресатными группами SMRP 782
Передача многоадресатных дейтаграмм 783
Обработка изменений SNMP-топологии 784
Пример передачи данных SNMP 784
Формат SMRP-пакета 785
Контрольные вопросы 786

Часть VIII. Управление сетями 789

Глава 52. Технологии защиты сетей 791

Почему важно обеспечить безопасность сети? 791
Различные виды угроз безопасности сетей 792
Несанкционированный доступ 792
Низкий уровень аутентификации 793
Пароли 793
Анализаторы пакетов 793
Уровень приложений 794
Вирусы, черви и "троянские кони" 794
Подделка IP-адреса 794
Атака типа "отказ в обслуживании" 795
Политика безопасности 795
Поэтапное решение задачи обеспечения безопасности 796
Ослабление угроз безопасности сетей 799
Средства защиты сетей 800
Резюме 802
Контрольные вопросы 803
Дополнительные источники 803
Web-сайты 803
Книги 804
Группа новостей 804
Глоссарий 804

Глава 53. Сетевые каталоги 807

Объективно-ориентированное моделирование информации 807
Модели данных в различных хранилищах 809
Реализация информационной модели 810
Основы теории каталогов 812
Каталоги и службы каталогов 813
Традиционное применение каталогов 816
Причины применения DEN в интеллектуальных сетях 816
Распределение интеллектуальных функций между сетевыми приложениями 818
Использование каталогов в интеллектуальной сети 820
Проблемы современных служб каталогов 820
Обзор DEN 821
Сети и DEN 821

Служба каталогов и управление сетью 823
Расширенная схема и другие схемы устройств 824
Сетевые приложения, интегрированные с каталогом и другими сетевыми протоколами 824
Преимущества DEN 825
Использование DEN в продуктах Cisco 826
Перспективы сетей со службами каталогов 827
Резюме 827
Контрольные вопросы 828
Дополнительные источники 828

Глава 54. Технологии сетевого кэширования 833

Введение 833
Сетевое кэширование 833
Функционирование Web-кэширования 834
Достоинства локализации типов потоков данных 834
Интегрированный сетевой кэш 835
Прокси-серверы 835
Автономные кэши 836
Кэширование в браузере клиента 836
Сетевое кэширование по протоколу WCCP 837
Функция обратного прокси-кэширования 845
Обновление содержимого 845
Стандарты HTTP-кэширования 846
Средства контроля устаревания содержимого в кэш-процессоре 847
Средства контроля устаревания в браузере 847
Резюме 847
Контрольные вопросы 848

Глава 55. Сети для хранения информации 851

Что представляет собой система SAN? 852
Протокол Fibre Channel 856
Топологии протокола Fibre Channel 858
Типы портов протокола Fibre Channel 859
Коммуникационная модель протокола Fibre Channel 861
Адресация протокола Fibre Channel 863
Формат фрейма протокола Fibre Channel 864
Классы обслуживания протокола Fibre Channel 866
Маршрутизация в структуре протокола Fibre Channel 867
Управление потоками в сети Fibre Channel 868
Распределенные службы коммутируемых структур протокола Fibre Channel 868
Протокол iSCSI 870
Коммуникационная модель протокола iSCSI 870
Формат фрейма протокола iSCSI 871
Службы протокола iSCSI 872
Резюме 874
Контрольные вопросы 875
Дополнительные источники 876

Книги 876
URL-адреса 876

Глава 56. Управление сетями IBM 879

Введение 879
Функциональные области управления сетями IBM 880
Управление конфигурацией IBM 880
Управление производительностью и учетными записями 880
Управление отказами 880
Управление операциями 881
Управление изменениями 881
Архитектуры сетевого управления IBM 882
Открытая сетевая архитектура 882
SystemView 882
Платформы управления сетями IBM 882
NetView 883
LAN Network Manager 884
Протокол SNMP 884
Контрольные вопросы 884

Глава 57. Удаленный мониторинг 887

Введение 887
Группы RMON 887
Контрольные вопросы 889

Глава 58. Протокол SNMP 891

Введение 891
Базовые компоненты протокола SNMP 891
Основные команды протокола SNMP 892
База управляющей информации протокола SNMP 893
Протокол SNMP и представление данных 894
Протокол SNMP версии 1 895
Протокол SNMPv1 и структура управляющей информации 896
Операции протокола SNMPv1 897
Протокол SNMPv2 897
SNMP 2 и структура управляющей информации 897
Информационные модули SMI 898
Операции протокола SNMPv2 898
Вопросы безопасности 899
Протокол SNMP версии 3 899
Угрозы безопасности 899
Модульная архитектура 900
Архитектура безопасности 902
Модель защиты сети для отдельного пользователя 902
Модель управления доступом на основе View 903
Управление посредством SNMP 904
Справочные данные протокола SNMP: форматы сообщений SNMP 904
Заголовок сообщения SNMP 904

Модуль данных SNMP 904
Trap PDU Format 906
Резюме 906
Контрольные вопросы 906

Глава 59. Качество обслуживания 909

Введение 909
Концепции QoS 910
Базовая архитектура QoS 911
Идентификация и маркировка QoS 911
Классификация 912
Функции QoS в пределах одного сетевого элемента 912
Управление перегрузкой 912
Управление очередями 912
Методы повышения эффективности канала 913
Формирование потока и применение политик 913
Управление QoS 914
Уровни сквозного QoS 914
Интерфейс командной строки модульного качества обслуживания QoS 915
Различные архитектуры QoS 916
Архитектура интегрированных служб 916
Архитектура дифференцированных служб 917
Байт дифференцированных служб 917
Задание политики QoS и основанная на политике маршрутизация 918
Согласованная скорость передачи CAR: установка IP-очередности 919
NBAR: динамическая идентификация потоков 921
Средства управления переполнением 921
Очередность FIFO: простейший способ промежуточного хранения 922
PQ: задание данным приоритетов 922
CQ: гарантированная полоса пропускания 923
Основанная на потоках очередность WFQ: создание равноправных потоков 924
Управление очередями (средства предотвращения переполнения в сети) 929
WRED: устранение перегрузок 929
Взаимодействие алгоритма WRED и технологий сигнализации QoS 929
Потоковый RED: RED для потоков, не совместимых с TCP 930
Средства формирования потоков и конфигурирования политик 931
CAR: политики доступа к полосе пропускания 932
Общее формирование потоков GTS: управление исходящим потоком данных 932
FRTS: управление потоками данных Frame Relay 933
Механизмы повышения эффективности канала 934
LFI: фрагментация и чередование данных протокола IP 935
Сжатие заголовков RTP: повышение эффективности при передаче данных реального времени 935
Протокол RSVP: гарантии QoS 936
Управление QoS 937
QoS в Ethernet 938
MPLS: гибкое построение передачи потоков данных 939
Управление политиками QoS 939

SNA ToS 940
QoS для речевых пакетов 940
QoS при передаче видеопотоков 941
Автоматизация QoS 942
Резюме 943
Будущее QoS 944
Контрольные вопросы 944
Дополнительные источники 944

Часть IX. Приложения 947

Приложение А. Ответы на контрольные вопросы 949

Глава 1 949
Глава 2 949
Глава 3 950
Глава 4 950
Глава 5 951
Глава 6 951
Глава 7 952
Глава 8 952
Глава 9 953
Глава 10 954
Глава 11 954
Глава 12 955
Глава 13 955
Глава 14 956
Глава 15 956
Глава 16 957
Глава 17 958
Глава 18 958
Глава 19 959
Глава 20 959
Глава 21 961
Глава 22 961
Глава 23 962
Глава 24 963
Глава 25 964
Глава 26 964
Глава 27 965
Глава 28 966
Глава 29 966
Глава 30 967
Глава 31 968
Глава 32 970
Глава 33 970
Глава 34 971
Глава 35 973

Глава 36 974
Глава 37 974
Глава 38 975
Глава 39 976
Глава 40 976
Глава 41 977
Глава 42 978
Глава 43 979
Глава 44 979
Глава 45 980
Глава 46 981
Глава 47 982
Глава 48 982
Глава 49 983
Глава 50 984
Глава 51 984
Глава 52 985
Глава 53 986
Глава 54 988
Глава 55 988
Глава 56 990
Глава 57 991
Глава 58 991
Глава 59 991

Приложение Б. Традиционные технологии **995**

Сети Token Ring/IEEE 802.5 **995**
Физические соединения 996
Функционирование сети Token Ring 996
Система приоритетов 997
Механизмы ликвидации сбоев в сети 998
Формат фрейма 998
Поля фрейма Token Ring 999
Поля фрейма данных/управления 999
Резюме 1000
Сетевые системы Xerox **1000**
Введение 1000
Иерархия стека протоколов XNS 1001
Доступ к среде передачи 1002
Сетевой уровень 1002
Транспортный уровень 1004
Протоколы верхних уровней 1004
Резюме 1005
Сетевая служба Banyan Vines **1005**
Введение 1005
Доступ к передающей среде 1005
Сетевой уровень 1005
Межсетевой протокол VINES 1006

Протокол таблицы маршрутизации 1010
Протокол преобразования адресов 1011
Межсетевой протокол управления 1011
Транспортный уровень 1011
Протоколы верхних уровней 1012
Резюме 1012
Дополнительные источники 1012

Предметный указатель **1013**

Введение

Работа в сети и использование Internet стали одними из самых влиятельных факторов нашей повседневной жизни. Они продолжают изменять наш стиль учебы, работы, отдыха, развлечений и жизни в целом. Менее чем за десять лет весь мир оказался объединенным глобальной сетью, что дало нам возможность легко, недорого и практически мгновенно связаться с любой точкой планеты. Немногие будут спорить с тем, что Internet изменил все стороны нашей жизни. Использование глобальной сети Internet повысило уровень образования и сделало возможным получение студентом любой информации в любое время и в любой точке земного шара. С помощью Internet мы общаемся с друзьями и родственниками, с его помощью мы планируем наш отпуск. Теперь весь мир и вся информация стали легко доступны, что создает новые благоприятные возможности для работы, управления, образования и развития личности.

В настоящей книге авторы попытались дать читателю общее понимание различных понятий и технологий, используемых в сфере сетевых коммуникаций. Она представляет собой обширный справочник, в котором описан ряд различных сетевых технологий, протоколов и концепций; в нее наряду с самыми современными технологиями также включены традиционные технологии. Сотрудники издательства Cisco Press надеются, что читатель оценит книгу как современную, содержательную и полезную, независимо от того, является ли он сетевым инженером, другим сетевым профессионалом или руководителем, принимающим решения в этой области. Эта книга окажется полезной также и тем, кто просто хочет больше узнать о сети Internet и технологиях, которые в ней используются.

Цели авторов

В настоящей книге представлена базовая техническая информация о различных сетевых технологиях. Она предназначена для использования как вместе с другими книгами издательства Cisco Press, так и в качестве самостоятельного справочного пособия.

Авторы книги не ставили перед собой цель предоставить всю возможную информацию об описываемых технологиях; вместо этого в ней представлен общий обзор, в котором подчеркнуты наиболее значительные и важные особенности каждой технологии.

Изменения в четвертом издании

При подготовке четвертого издания настоящей книги авторы добавили новые главы, в которых рассматриваются оптоволоконные сети, передача голосовых данных по протоколу IP (Voice over IP — VoIP), протоколы DPT/SRT, EAP, сети для хранения данных, качество обслуживания QoS и операционная система IOS Cisco. Внесено также большое количество обновлений в уже имевшиеся главы, в том числе изменений, отражающих самые последние разработки в рассматриваемой области.

Для кого предназначена эта книга

"Руководство по технологиям объединенных сетей" написано для всех, кто хочет изучить устройство глобальных сетей. Мы надеемся, что сведения, представленные в данном издании, помогут пользователям оценить применимость тех или иных технологий в их сетевой среде и позволят читателю понять основы технологий межсетевого взаимодействия.

Структура книги

Настоящее руководство состоит из описанных ниже девяти частей.

Часть I, "Основы теории объединенных сетей". В этой части приводится информация об основных сетевых понятиях и технологиях, включая технологии локальных сетей LAN и распределенных сетей WAN, программное обеспечение IOS Cisco, использование мостов и коммутаторов, протоколы маршрутизации и управление сетями.

Часть II, "Технологии локальных сетей". В этой части приводится описание стандартных протоколов локальных сетей и используемых в этих сетях технологий.

Часть III, "Технологии распределенных сетей". В этой части обсуждаются различные технологии распределенных сетей WAN, включая технологии Frame Relay, HSSI, ISDN, PPP, SMDS, технологию удаленного доступа, SDLC, X.25 и виртуальные сети VPN.

Часть IV, "Технологии мультисервисного доступа". В этой части приведен обзор технологий доступа к сетям, включая интеграцию голосовых и обычных данных, беспроводной доступ, технологию цифровых абонентских каналов DSL, кабельные сети, оптоволоконные сети, передачу голосовых данных по протоколу IP (Voice over IP — VoIP), протоколы DPT/SRT и EAP.

Часть V, "Мосты и переключатели". В этой части обсуждается использование мостов и коммутаторов, включая прозрачные мостовые соединения, мостовые соединения с использованием различных сред передачи, мосты "источник-маршрут", коммутацию в локальных сетях и виртуальные сети VLAN, сети ATM, коммутацию MPLS и коммутацию на канальном уровне.

Часть VI, "Сетевые протоколы". В этой части описываются сетевые протоколы, включая протоколы OSIP, IP, IPv6, Netware, Appletalk, IBM SNA и DECnet.

Часть VII, "Протоколы маршрутизации". В этой части приведена обзорная информация о протоколах маршрутизации, включая протоколы BGP, усовершенствованный IGRP (Enhanced IGRP), SNA IBM, IGRP, Internet Protocol Multicast, протокол канальных служб Netware (Netware Link-Services), OSPF, OSIRP, протокол маршрутной информации, протокол резервирования ресурсов и протокол SMRP.

Часть VIII, "Управление сетями". В этой части обсуждаются различные технологии обеспечения безопасности, сети с функциями каталогов (directory-enabled networking), технологии сетевого кэширования и сети для хранения информации (storage networking).

Часть IX, "Приложения". В приложениях приведены ответы на контрольные вопросы и обсуждены некоторые традиционные технологии.

Благодарности участникам настоящего издания

Издательство Cisco Press хотело бы выразить свою глубокую признательность талантливым авторам, которые внесли свой вклад в четвертое издание этой книги. Без их помощи и оценки мы не смогли бы его выпустить. Благодарим всех тех, кто помог написать и отредактировать главы этого нового издания. Хотелось бы перечислить всех авторов (в алфавитном порядке):

Брюс Александер (Bruce Alexander) является менеджером по маркетингу отдела беспроводных технологий корпорации Cisco Systems. Он оказался в корпорации Cisco после того, как она присоединила к себе компанию Aironet Wireless Communications, в которой Брюс работал директором технической поддержки. Брюс Александр работал в сфере RF-технологий в течение более 27 лет, и в сфере распределенных RF-технологий более 17 лет. Он много работал с инженерной группой RF компании Texlon, как с программным, так и с аппаратным обеспечением, выполняя обязанности старшего инструктора для национальных центров образования. Кроме того, он обладает лицензией радиолюбителя с 1978 года. Брюс является одним из учредителей американской компании радиолюбителей (American Amateur Radio Company). Он посещал курсы университета в Акроне (Acron), где повышал свою квалификацию в компьютерном программировании и в коммерческом администрировании.

Тони Аллен (Tony Allen) награжден медалью CD (Canadian Decoration), является инженером-консультантом в области сетевых технологий и работает в Cisco Systems находясь в канадском городе Торонто. В течение последних пяти лет помогал провайдерам служб планировать, проектировать и реализовывать их сети. До прихода в корпорацию Cisco Тони в течение 27 лет служил в канадском военно-морском флоте, занимая различные инженерные должности и выполняя работы по поддержке телекоммуникаций и управлению ими. В настоящее время специализируется на проектировании, разработке и тестировании сетей VoIP, оптических беспроводных технологий и широкополосных сетей.

Матт Карлинг (Matt Carling) работает инженером-консультантом в группе перспективных служб корпорации Cisco Systems. Работая в корпорации Cisco в течение последних трех лет, он тесно сотрудничал с многими провайдерами служб, обеспечивая эффективные сетевые оптимизационные решения, реализацию технологий и служб, а также последних разработок корпорации Cisco. Он имеет более чем 12-летний опыт работы в сетевой сфере. Матт имеет степень бакалавра инженерных наук в сфере компьютерных технологий и диплом об окончании курса наук управления в университете Канберры (Австралия).

Бредли Дансмор (Bradley Dunsmore) является инструктором по новым продуктам группы перспективных служб корпорации Cisco Systems в Research Triangle Park, N.C (штат Северная Калифорния). Имеет Cisco-сертификаты CCNP, CCDP, CCSI и CSS-1, также сертификат MCSE+Internet корпорации Microsoft. В своей нынешней должности Бредли разрабатывает сетевые топологии для новых курсов в своей группе и обучает инструкторов, ведущих курсы. Кроме того, он проектирует сети, которые позволяют надежно загружать эти курсы в режиме удаленного доступа. Специализируется на решениях по соединениям Interconnection SS7, на коммуникациях в среде распределенных сетей WAN и на разработке продуктов обеспечения безопасности корпорации Cisco.

Сэчин Гупта (Sachin Gupta) работает менеджером по программным продуктам для коммутаторов Cisco Catalyst 6500. Имеет сертификат CCIE по маршрутизации и коммутации. До работы в своем нынешнем качестве работал в корпорации Cisco в качестве инженера по техническому маркетингу в отделе Internet-технологий, где предметом его деятельности были технологии программного обеспечения Cisco. До этого Гупта работал инженером поддержки пользователей в корпорации Cisco. Имеет степень магистра в электроинженерии, полученную в Стэнфордском университете.

Вейн Хики (Wayne Hickey) имеет более чем двадцатилетний опыт работы в сфере телекоммуникаций и компьютерных данных, включая работу с SONET, SDH, DWDM,IP,ATM, Frame Relay, HPC, голосовыми и видеосетями, а также с протоколом SSEM. В настоящее время работает менеджером по программным продуктам отдела оптической технической коммерции в корпорации Cisco Systems. Ранее в течение 19 лет работал в компании Aliant Telecom (NBTel), которая является третьим по значимости провайдером телекоммуникаций в Канаде, где его деятельность концентрировалась на разработке передающих сетей и оценке разрабатывавшихся технологий доступа и передачи. Хики был автором и соавтором нескольких статей по дисперсии режима поляризации (Polarization Mode Dispersion) и дальних систем передачи данных. Имеет несколько патентных свидетельств по первичным и вторичным проектам для гибридных коаксиальных оптоволоконных кабелей (Hybryd Fiber Coaxial — HFC).

Кьянг Хуанг (Qiang Huang), сертификат CCIE #4937, является инженером по поддержке пользовательских сетей в группах корпорации Cisco, работающих в сфере виртуальных частных сетей VPN и сетевой безопасности. Он обладает обширными познаниями во многих продуктах и технологиях обеспечения безопасности и был в течение нескольких лет техническим руководителем своей группы. Хуанг имеет несколько сертификаций CCIE, включая сертификаты по удаленному доступу ISP, маршрутизацию и коммутацию, а также вопросы безопасности. Получил степень магистра по электроинженерии и компьютерным наукам в университете штата Колорадо.

Венкат Канкипати (Venat Kankipati) в течение шести лет работал в корпорации Cisco в качестве менеджера по разработке программного обеспечения. Его опыт охватывает широкий ряд технологий, включая протоколы SNA, сетевую безопасность и увеличение производительности сети. До прихода в корпорацию Cisco он работал в компании Bay Networks. Канкипати имеет степень магистра компьютерных наук, полученную в университете штата Массачусетс, степень магистра по компьютерным приложениям, полученную в университете Мадраса и степень бакалавра, полученную в Бомбейском университетете (Индия).

Марчело Нобрега (Marcelo Nobrega), CCIE #8069, работает старшим консультантом-инженером в группе перспективных служб корпорации Cisco Systems. Марчело занимается размещением проектов, администрированием и устранением неисправностей (отладкой) крупных сетей провайдеров служб с 1994 года. В корпорации Cisco Systems работает с 2000 года. Его деятельность концентрируется на базовых IP-протоколах и протоколах маршрутизации, сетевом управлении, IP-телефонии и, в самое последнее время, на центрах IP-вызовов. Нобрега имеет степени бакалавра в электроинженерии и магистра компьютерных наук, полученные в католическом университете Pontifica Universidade Рио-де-Жанейро (Бразилия).

Том Нозелла (Tom Nosella), CCIE #1935, является старшим менеджером технического маркетинга в группе технологий хранения данных корпорации Cisco Systems. Он и его команда создают, утверждают и содействуют реализации проектов для промышленных пользователей и провайдеров служб Cisco. До прихода в корпорацию

Cisco он был техническим директором компании Bell Canada корпорации Residential and Commercial Internet Services, где возглавлял команду старших инженеров. Имеет степень бакалавра инженерных наук и управления, полученную в университете McMaster провинции Онтарио (Канада).

Иван Пепельняк (Ivan Pepelnjak), CCIE #1354, имеет более чем десятилетний опыт работы в области проектирования, установки и отладки крупных локальных и распределенных сетей промышленных потребителей и провайдеров служб. В настоящее время является главным техническим советником компании NIL Data Communications. Он является создателем программы Академии провайдеров служб компании NIL (NIL Service Provider Academy), одним из создателей учебной программы для провайдеров служб в корпорации Cisco Systems и ведущим разработчиком нескольких курсов для провайдеров служб по коммутации MPLS, протоколу BGP и протоколу IP. В Европе Пепельняк является одним из авторитетных специалистов по маршрутизации Cisco. Вышла его книга "Проектирование сетей протокола EIGRP"; он также является соавтором книги "Коммутация MPLS и архитектура виртуальных сетей VPN", вышедшей в издательстве Cisco Press.

Данни Родригес (Danny Rodriguez) работает инженером по сетевой безопасности в организации консультативных служб по безопасности сетей корпорации Cisco Systems, где он выполняет оценку уровня безопасности и обзоры проектов обеспечения безопасности для компаний Fortune 500. Он также отвечает за обучение и повышение квалификации других инженеров по сетевой безопасности в своей группе. Во время работы в корпорации Cisco выполнял функции специалиста по образованию группе обучения и решений Internet (Internet Learning and Solutiuon Group — ILSG) корпорации Cisco. Он является автором Cisco-курса по обнаружению вторжений в сети и внес свой вклад в разработку лабораторных работ для курсов базовой безопасности Cisco. Данни также вел курсы по безопасности сетей для инженеров корпорации Cisco, для компании Cisco learning and Channel Partners и для конечных пользователей. Родригес внес существенный вклад в программу сертификации CCSP. Имеет сертификаты CCDA и CSS-1.

Саед Сардар (Saeed Sardar) работает в качестве инженера-проектировщика в группе высокоскоростной коммутации корпорации Cisco Systems более двух лет. Он имеет большой опыт в области тестирования в решении вопросов управляющей плоскости и плоскости данных операционной системы IOS Cisco на коммутаторах Cisco Catalyst серии 6000 в применении к протоколам IPv4, IPv6, технологиям MPLS, QoS и многоадресатной маршрутизации и аппаратной пересылке на различных модулях локальных и распределенных сетей.

Маркус Зитцман (Marcus Sitsman), CCIE #9004, работает инженером по сетевой безопасности в корпорации Cisco Systems. Он имеет более чем шестилетний опыт работы в сетевой сфере. С момента прихода в корпорацию Cisco в 2000 году продолжал заниматься технологиями безопасности и программными продуктами. В настоящее время обеспечивает оценку уровня безопасности в сетях и консультации по защите сетей для пользователей корпорации Cisco. Он вел курсы повышения квалификации в сфере безопасности для других инженеров корпорации Cisco и был техническим представителем в Cisco Networkers Convention.

Алан Троуп (Alan Troup) разрабатывает технические руководства для семейства коммутаторов MDS 9000, используемых в сетях хранения данных. Ранее был менеджером по техническим публикациям одного из подразделений оптических коммутато-

ров Cisco. Имеет степень бакалавра по английскому языку, полученную в университете штата Сан-Хосе.

Сринивас Вегесна (Srinivas Vegesna) , CCIE 1399, является менеджером по разработке программного обеспечения инженерной группы базового IP (Core IP Engineering) корпорации Cisco Systems. До работы в своей нынешней должности был инженером-консультантом и менеджером группы консультирования провайдеров служб (Service Provider Consulting Services) корпорации Cisco. Имеет опыт работы с базовыми IP-сетями, в особенности с протоколом IP и QoS протокола IP. За более чем восемь лет работы в корпорации Cisco Вегесна работал с многими провайдерами служб и промышленными пользователями, помогая им проектировать, реализовать и отлаживать крупномасштабные IP-сети. Имеет степень магистра, полученную в университете штата Аризона, и MBA, полученную в университете Санта-Клара.

Участники третьего издания

В разработке третьего издания принимали участие (в алфавитном порядке): Марк Бресникер (Mark Bresniker), Джерри Бургесс (Gerry Burgess), Дейв Бустер (Dave Buster), Кевин Гамильтон (Kevin Hamilton), Брайан Юнилла (Braian Junilla), Эндрю Кесслер (Andrew Kessler), Уильям Лейн (William Lane), Кевин Малер (Kevin Mahler), Эрик Мар (Erick Mar), Кевин Муссо (Kevin Mousseau), Джим О'Ши (Jim O'Shea), Джим Паркхерст (Jim Parkhurst), Эди Квироз (Edie Quiroz), Нейл Рейд (Neil Reid), Франк Ривест (Frank Rivest), Марк Сортак (Mark Sportack), Джон Страсснер (John Strassner) и Натали Тиммз (Natalie Timms).

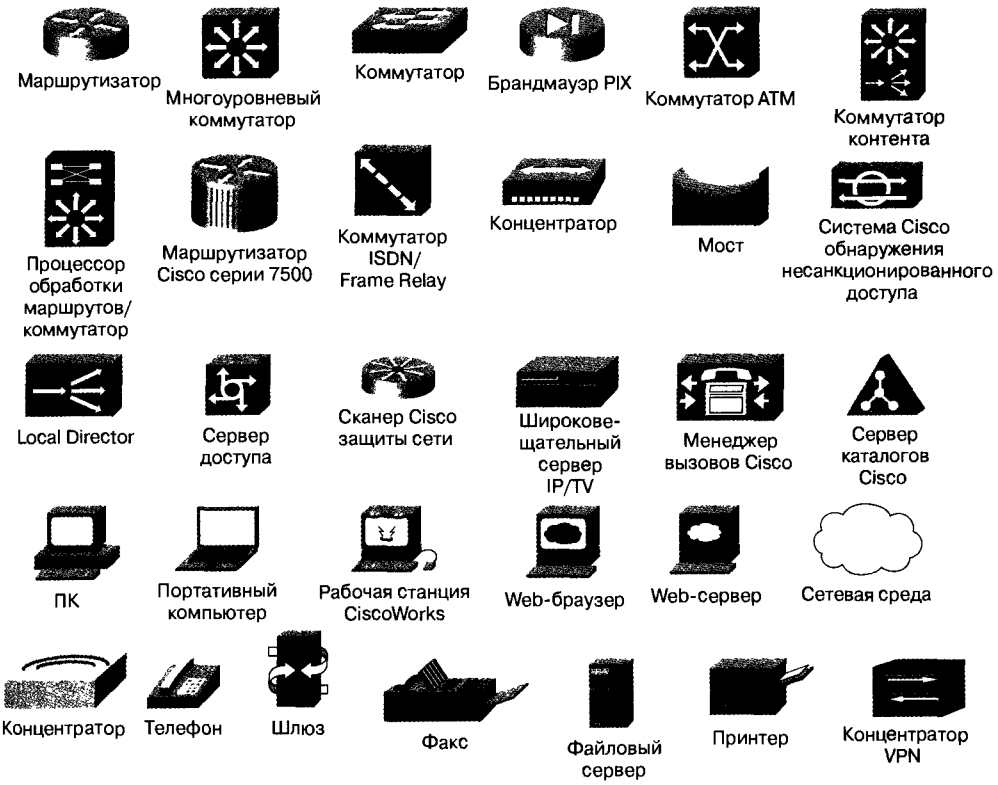
Авторы первого издания

Главными авторами первого издания этой книги были Мэрили Форд (Merilee Ford), Ким Лью (H.Kim Lew), Стив Спаньер (Steve Spanier) и Тим Стевенсон (Tim Stevenson).

Используемые в книге пиктограммы

Для графического изображения различных сетевых устройств корпорацией Cisco приняты следующие стандартные пиктограммы, многие из которых используются в настоящей книге.

Корпорация Cisco использует приведенные ниже стандартные пиктограммы для отображения различных сетевых устройств. Они будут использованы в данной книге.



Обозначения, используемые в командах

Обозначения, используемые в книге при записи команд, соответствуют тем, которые используются в справочниках команд операционной системы IOS Cisco. В справочнике команд эти обозначения описываются следующим образом.

- Вертикальная черта (|) разделяет альтернативные, взаимно исключающие друг друга элементы.
- Квадратные скобки ([ ]) указывают на необязательный характер ключевых слов или аргументов.
- Фигурные скобки ({ }) указывают на обязательность выбора какого-либо из приведенных значений.
- Фигурные скобки внутри квадратных скобок ([{}]) указывают на обязательность выбора одного из значений внутри необязательного элемента.

- Команды и ключевые слова, которые вводятся в неизменном виде, набраны **полужирным** шрифтом. В примерах конфигураций и в текстах, которые выводятся на экран (но не в общем описании синтаксиса команды), **полужирный** шрифт указывает названия команд, вводимые пользователем (например, команды **show),** в отличие от выводимого текста.
- Аргументы, которые замещаются значениями, вводимыми пользователем, показаны *курсивом.*

От издательства

Вы, читатель этой книги, и есть главный ее критик и комментатор. Мы ценим ваше мнение и хотим знать, что было сделано нами правильно, что можно было сделать лучше и что еще вы хотели бы увидеть изданным нами. Нам интересно услышать и любые другие замечания, которые вам хотелось бы высказать в наш адрес.

Мы ждем ваших комментариев и надеемся на них. Вы можете прислать нам бумажное или электронное письмо, либо просто посетить наш Web-сервер и оставить свои замечания там. Одним словом, любым удобным для вас способом дайте нам знать, нравится или нет вам эта книга, а также выскажите свое мнение о том, как сделать наши книги более интересными для вас.

Посылая письмо или сообщение, не забудьте указать название книги и ее авторов, а также ваш обратный адрес. Мы внимательно ознакомимся с вашим мнением и обязательно учтем его при отборе и подготовке к изданию последующих книг. Наши координаты:

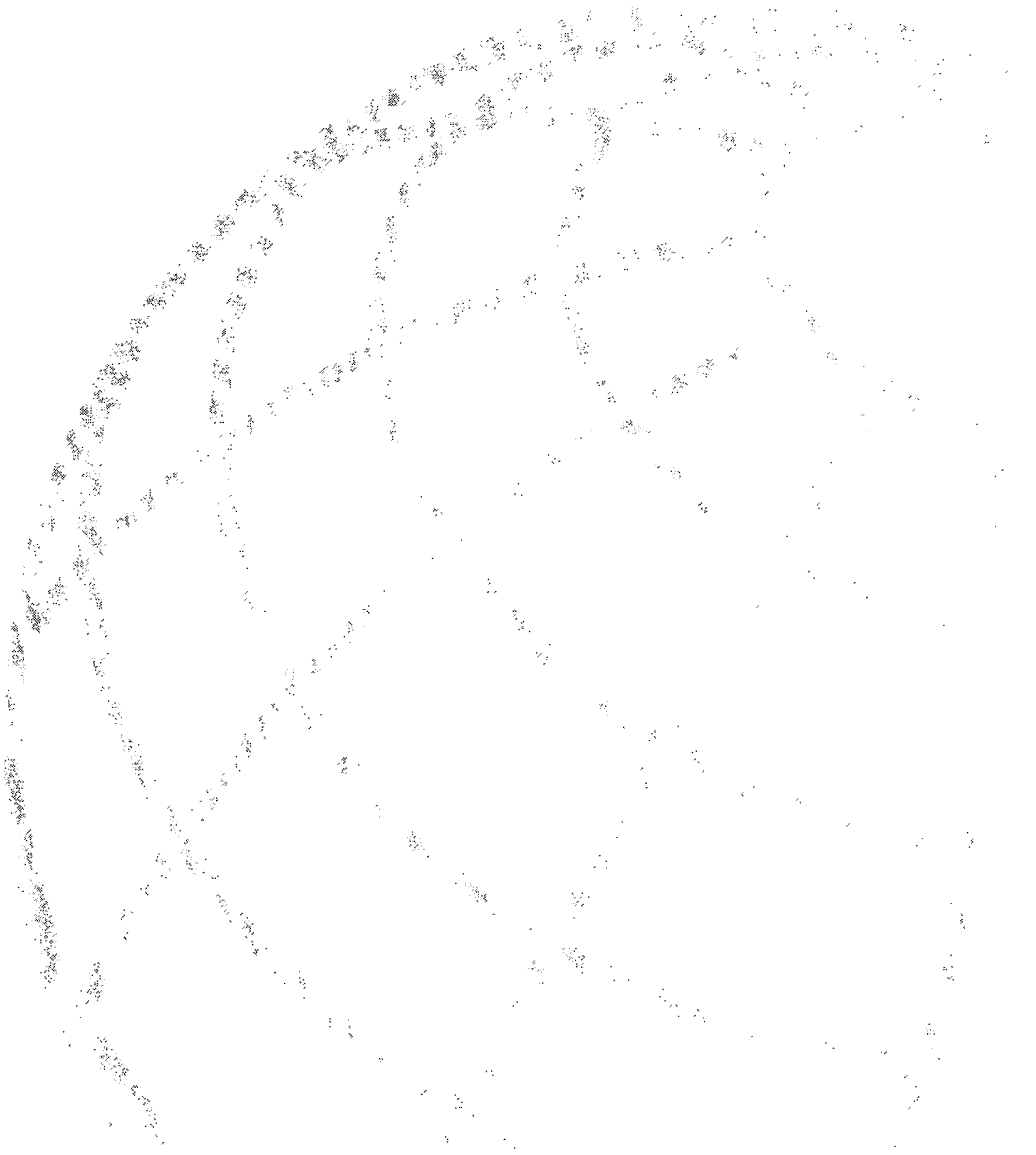
E-mail: `info@williamspublishing.com`

WWW: `http://www.williamspublishing.com`

Информация для писем из:

России: 115419, Москва, а/я 783

Украины: 03150, Киев, а/я 152



Часть

Основы теории объединенных сетей

Глава 1. Основы теории объединенных сетей
Глава 2. Основы протоколов локальных сетей
Глава 3. Основные технологии распределенных сетей
Глава 4. Начальные сведения о программном обеспечении IOS Cisco
Глава 5. Основы мостовых и коммутируемых соединений
Глава 6. Основы маршрутизации
Глава 7. Основные принципы управления сетями

В этой главе...

- Определяется понятие объединенной сети;
- Рассматриваются основы эталонной модели OSI;
- Описываются различия между службами, ориентированными на соединение, и службами, не требующими подтверждения соединения;
- Описываются типы адресов, используемых в объединенных сетях;
- Рассматриваются основы управления потоками и контроля ошибок.

Глава 1

Основные понятия теории объединенных сетей

Эта и последующие шесть глав служат основой для дальнейшего обсуждения различных технологий объединенных сетей. В настоящей главе рассматриваются некоторые фундаментальные принципы и понятия, используемые в постоянно изменяющемся языке теории объединенных сетей. Подобно тому, как вся книга посвящена основам современных сетей, данная глава посвящена некоторым общим темам, на которых будет базироваться все дальнейшее изложение. Это такие темы, как управление потоком, контроль ошибок и мультиплексирование, однако основное внимание в настоящей главе будет уделено реализации модели взаимодействия открытых систем (Open System Interconnection — OSI) в функциях сетевого/межсетевого обмена, а также в принципах схем адресации. Эталонная модель OSI представляет собой набор компонентов, из которых строятся объединенные сети. Принципиальное понимание эталонной модели OSI дает возможность проанализировать те сложные составляющие, из которых складывается объединенная сеть.

Что такое объединенная сеть?

Объединенная сеть (internetwork) представляет собой объединение отдельных сетей, соединенных промежуточными сетевыми устройствами, функционирующее как одна большая сеть. Понятие объединенной сети включает в себя технологии, устройства и процедуры, которые позволяют решить задачу создания и администрирования объединенной сети. На рис. 1.1 показано, как несколько различных типов сетей могут быть связаны между собой с помощью маршрутизаторов и других сетевых устройств и образовать объединенную сеть.

История объединенных сетей

Первые сети работали в режиме разделения времени и состояли из мэйнфреймов с подключенными к ним терминалами. Такие среды строились как на основе системной архитектуры сети IBM (Systems Network Architecture — SNA), так и на основе сетевой архитектуры Digital.

Возникновение *локальных сетей (Local-Area Network — LAN)* связано с широким использованием персональных компьютеров PC. Локальные сети позволяют нескольким

пользователям, расположенным в относительно небольшой географической области, обмениваться файлами и сообщениями, а также совместно использовать общие ресурсы, такие как файловые серверы и принтеры.

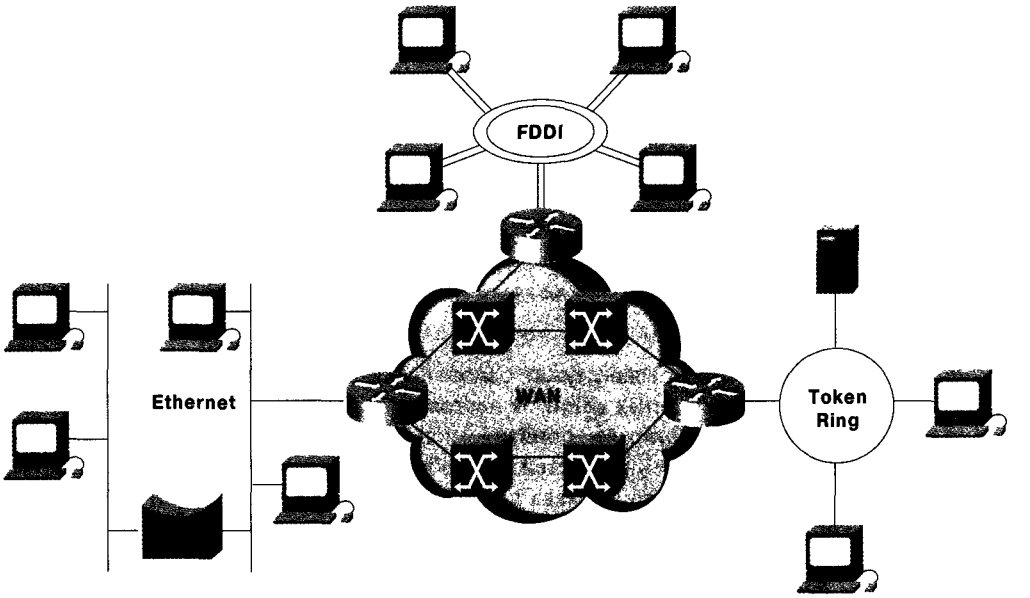


Рис. 1.1. Сети, использующие различные технологии, могут быть соединены между собой и образовать объединенную сеть

Распределенные сети (Wide-Area Network — WAN) объединяют между собой локальные сети для того, чтобы обеспечить связь между пользователями, расположенными далеко друг от друга. Для объединения локальных сетей используются такие технологии, как T1, T3, ATM, ISDN, ADSL, Frame Relay, радиосвязь и другие. С каждым днем появляются все новые способы соединения удаленных друг от друга локальных сетей.

В настоящее время область применения высокоскоростных локальных сетей и коммутируемых объединенных сетей продолжает расширяться, поскольку они работают на очень высоких скоростях и поддерживают такие приложения, как мультимедиа и видеоконференции, которые требуют большой полосы пропускания.

Объединенные сети развивались как средство решения трех основных задач: объединение изолированных локальных сетей, исключение дублирования ресурсов и более эффективное управление сетями. Изолированность локальных сетей друг от друга делает невозможным обмен электронной информацией между офисами и отделами. Дублирование ресурсов означает установку в каждом офисе или отделе одного и того же оборудования и программного обеспечения, с отдельным персоналом технической поддержки. Недостаточно эффективное управление сетью означает отсутствие централизованных систем управления сетями и поиска неисправностей.

Проблемы создания объединенных сетей

Функциональная реализация объединенной сети является непростой задачей. При этом возникает много проблем, особенно в плане обеспечения связи, надежности, эффектив-

ного управления сетью и гибкости. Каждая из вышеперечисленных задач является критически важной при создании качественной и эффективной объединенной сети.

При соединении различных систем возникает проблема обмена данными между сетями, использующими принципиально разные технологии. Например, в различных узлах для передачи данных могут использоваться различные передающие среды, работающие с разными скоростями, или даже различные типы сетей, между которыми требуется осуществлять обмен данными.

Поскольку эффективность работы компаний в значительной степени зависит от информационного обмена, объединенные сети должны обеспечивать определенный уровень надежности. Сетевая среда во многом непредсказуема, поэтому в большинстве крупных объединенных сетей предусмотрена т.н. избыточность, позволяющая не прерывать обмен данными даже в случае возникновения проблем.

Кроме того, управление сетью и поиск неисправностей в объединенной сети должны быть централизованными. Для того чтобы объединенная сеть работала без сбоев, необходимо правильно выбрать конфигурацию, настроить систему безопасности, добиться максимальной производительности и решить другие вопросы. Система безопасности является неотъемлемой частью объединенной сети. Многие ошибочно полагают, что система безопасности в сети необходима только для защиты частной сети от внешних нападений. Однако не менее важно защитить сеть от внутренних атак, особенно с учетом того, что чаще всего система защиты нарушается именно изнутри. Поэтому необходима также защита от использования внутренней сети в качестве средства для атаки внешних узлов.

В начале 2000 года многие крупные Web-узлы стали жертвами распределенных атак типа "отказ в обслуживании" (Distributed Denial Of Service Attack — DDOS attack). Такие атаки стали возможными по той причине, что многие частные сети, подключенные к Internet, не были должным образом защищены и послужили средством нападения.

Поскольку все в мире изменяется, объединенные сети должны обладать достаточной гибкостью, чтобы их можно было изменить в соответствии с новыми требованиями.

Эталонная модель взаимодействия открытых систем

Эталонная модель взаимодействия открытых систем (Open System Interconnection — OSI) описывает способ передачи информации по сети от приложения на одном компьютере к приложению на другом. OSI является концептуальной моделью, имеющей семь уровней, каждый из которых определяет некоторые функции сети. Эта модель была разработана Международной организацией по стандартизации (International Organization for Standardization — ISO) в 1984 году и в настоящее время считается основной архитектурной моделью передачи информации между компьютерами. Модель OSI представляет задачу перемещения информации по сети между компьютерами в виде семи более легко решаемых отдельных задач. Затем решение задачи или группы задач ассоциируется с одним из семи уровней модели OSI. Эти уровни более или менее независимы друг от друга, так что задачи, связанные с каждым из них, могут выполняться отдельно. Это позволяет изменять средства их решения на одном уровне, не вызывая конфликта с другими уровнями. Ниже перечислены семь уровней эталонной модели OSI:

- уровень 7 — уровень приложений;
- уровень 6 — уровень представления данных;
- уровень 5 — уровень сеанса связи;
- уровень 4 — транспортный уровень;
- уровень 3 — сетевой уровень;
- уровень 2 — канальный уровень;
- уровень 1 — физический уровень.

Внимание!

Удобным способом запомнить семь уровней модели OSI является предложение "All people seem to need data processing". Начальная буква каждого предложения соответствует названию уровня модели OSI.

- All — Application layer;
- People — Presentation layer;
- seem — Session layer;
- to — Transport layer;
- need — Network layer;
- data — Data link layer;
- processing. — Physical layer.

На рис. 1.2 показана состоящая из семи уровней эталонная модель OSI.

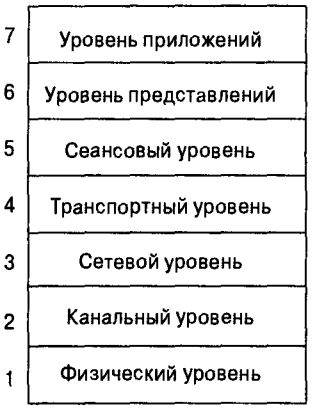


Рис. 1.2. Эталонная модель OSI содержит семь независимых уровней

Характеристики уровней эталонной модели OSI

Семь уровней эталонной модели OSI можно разделить на две категории: верхние инижние.

Верхние уровни модели OSI работают с приложениями и обычно реализуются только на уровне программного обеспечения. Самый верхний уровень, уровень приложений, наиболее близок к конечному пользователю. Процессы, протекающие на уровне пользователя и приложения, взаимодействуют с прикладным программным обеспечением, содержащим коммуникационные компоненты. "Верхним уровнем" иногда называют уровень, находящийся выше того уровня, о котором идет речь.

Нижние уровни модели OSI решают задачи транспортировки данных. Физический и канальный уровни реализуются в виде аппаратных средств и программного обеспечения. Самый нижний уровень, физический, находится ближе всего к физической сетевой среде (например, к сетевым кабелям) и непосредственно отвечает за размещение информации на носителе.

На рис. 1.3 показано подразделение уровней OSI на верхние и нижние.

Рис. 1.3. Две группы уровней эталонной модели OSI

Протоколы

Модель OSI определяет принципиальную схему обмена данными между компьютерами, но сама не является способом такого обмена. Обмен данными становится возможным благодаря коммуникационным протоколам. В контексте передачи данных по сети термин *"протокол"* представляет собой формальный набор правил и соглашений, регламентирующих обмен информацией между компьютерами по сети. Протокол реализует функции одного или нескольких уровней OSI.

Существует большое количество протоколов обмена данными. В частности, это протоколы локальных и распределенных сетей, сетевые протоколы и протоколы маршрутизации. *Протоколы локальных сетей* работают на физическом и канальном уровнях модели OSI и определяют правила обмена данными в различных средах передачи, применяемых в локальных сетях. *Протоколы распределенных сетей* работают на трех самых нижних уровнях модели OSI и определяют правила обмена данными по различным глобальным линиям связи. *Протоколы маршрутизации* работают на сетевом уровне и отвечают за обмен информацией между маршрутизаторами, с тем чтобы последние могли выбрать наилучший путь для передаваемых по сети данных. Наконец, к *сетевым протоколам* относятся различные протоколы высокого уровня,

присутствующие в некотором наборе протоколов (часто такие наборы называются стеками). Работа многих протоколов основывается на других протоколах. Например, протоколы маршрутизации для обмена данными между маршрутизаторами часто используют сетевые протоколы. Такой принцип построения сети на базе уже существующих уровней является основополагающим в модели OSI.

Модель OSI и обмен данными между компьютерными системами

Информация, передаваемая по сети из приложения, расположенного на одном компьютере, в приложение на другом компьютере, должна пройти через несколько уровней модели OSI. Например, если приложению на компьютере A необходимо передать информацию приложению на компьютере B, то приложение на компьютере A сначала передает ее на уровень приложений (уровень 7) компьютера A. Затем с уровня приложений информация передается на уровень представления (уровень 6), который перенаправляет ее на уровень сеанса связи (уровень 5), и так далее, вплоть до физического уровня (уровень 1). На физическом уровне информация помещается на физический сетевой носитель и пересылается по нему на компьютер B. Физический уровень компьютера B извлекает информацию с физического носителя и передает ее на канальный уровень (уровень 2), который в свою очередь передает ее на сетевой уровень (уровень 3), и так далее, пока информация не достигнет уровня приложений (уровень 7) компьютера B. На последнем этапе уровень приложений компьютера B передает информацию приложению-получателю, чем и завершается процесс обмена данными.

Взаимодействие уровней эталонной модели OSI

Каждый уровень модели OSI обычно взаимодействует с тремя другими уровнями: теми, что находятся непосредственно над и под ним, а также с таким же уровнем других компьютерных систем, подключенных к сети. Например, канальный уровень системы A взаимодействует с сетевым и физическим уровнями системы A, а также с канальным уровнем системы B (рис. 1.4).

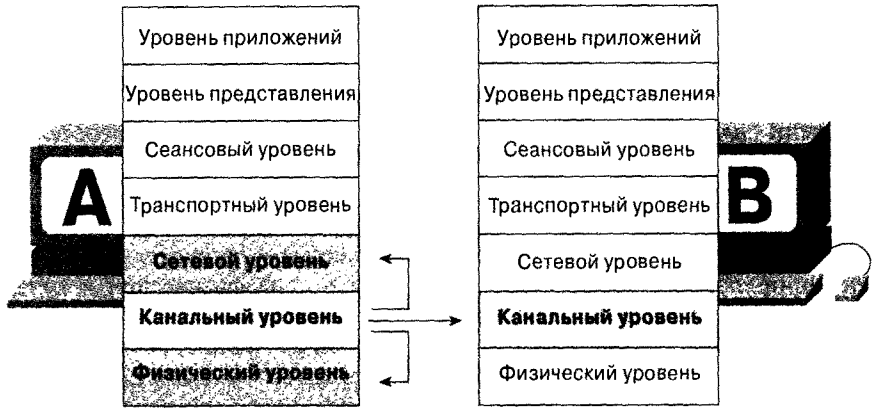


Рис. 1.4. Каждый уровень модели OSI взаимодействует с тремя другими уровнями

Службы уровней OSI

Каждый уровень модели OSI взаимодействует с другими уровнями для того, чтобы воспользоваться предоставляемыми ими службами. Эти службы дают возможность определенному уровню OSI взаимодействовать с таким же уровнем другой компьютерной системы. Говоря о службах уровней, необходимо дать определение трем базовым элементам: пользователь службы, провайдер службы и точка доступа к службе.

В данном контексте *пользователь службы* представляет собой уровень OSI, который запрашивает службы смежного уровня OSI, а *провайдером службы* является уровень OSI, который предоставляет пользователю доступ к службе. Уровни OSI могут предоставлять службы нескольким пользователям. *Точка доступа к службе* (Service Access Point — SAP) является тем уровнем, на котором один уровень OSI может запрашивать службы другого уровня.

На рис. 1.5 показана схема взаимодействия этих трех элементов на сетевом и канальном уровнях.

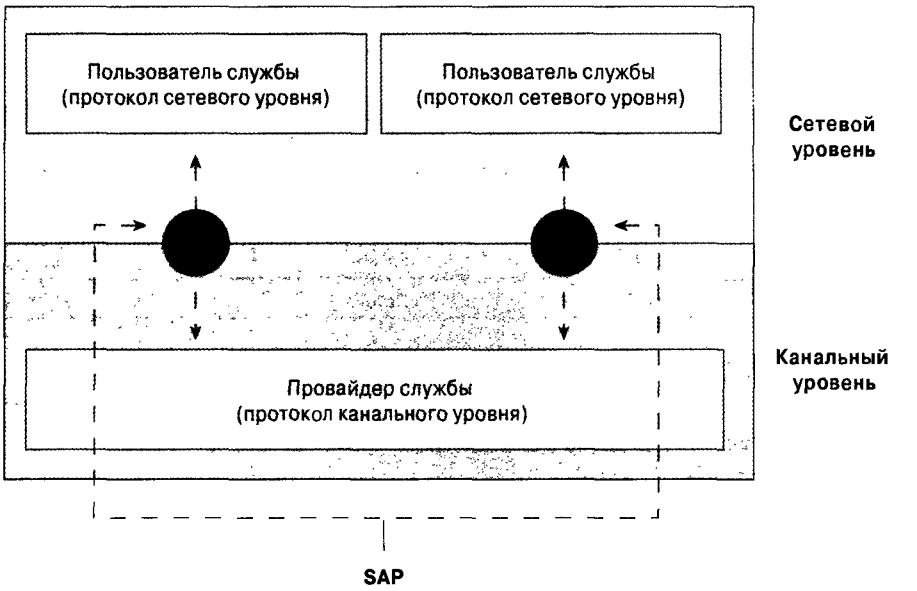


Рис. 1.5. Взаимодействие пользователей и провайдеров служб, а также точек доступа к службам (SAP) на сетевом и канальном уровнях

Уровни модели OSI и обмен информацией

На семи уровнях OSI используются различные формы управляющей информации для обмена данными с такими же уровнями других компьютерных систем. Эта *управляющая информация* состоит из особых запросов и инструкций, которыми обмениваются одноименные уровни OSI.

Управляющая информация делится на два типа: заголовки и трейлеры. *Заголовки* (header) предшествуют данным, передаваемым с верхних уровней на более низкие. *Трейлеры* (trailers) присоединяются после таких данных. Присоединение каким-либо уровнем OSI заголовка или трейлера к данным, поступившим с верхних уровней, не является обязательным.

Понятия заголовка, трейлера и данных являются относительными, они зависят от того, на каком уровне анализируется модуль данных. Например, на сетевом уровне модуль данных состоит из заголовка уровня 3 и собственно данных. Однако на канальном уровне вся информация, переданная с сетевого уровня, (т.е. заголовок уровня 3 и данные) рассматривается как данные.

Иными словами, та часть информации, которая на определенном уровне OSI рассматривается как данные, потенциально может содержать заголовки, трейлеры и данные всех высших уровней. Такой способ организации данных называется *инкапсуляцией* (encapsulation). На рис. 1.6 показано, как заголовок и данные одного уровня инкапсулируются в поле данных уровня, расположенного непосредственно под ним.

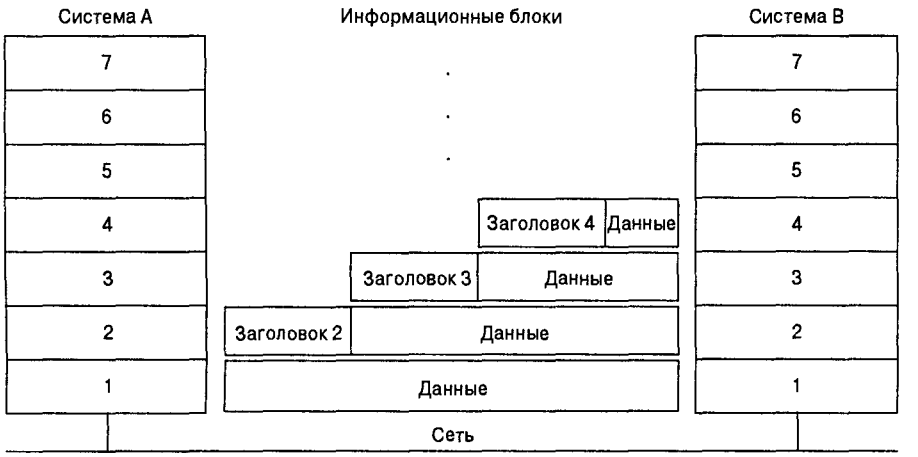


Рис. 1.6. Инкапсуляция заголовков и данных при обмене информацией

Процесс обмена информацией

Обмен информацией происходит между одинаковыми уровнями модели OSI. Каждый уровень компьютерной системы-источника добавляет к данным управляющую информацию, а каждый уровень системы-получателя, анализирует ее и отделяет от нее данные.

Если компьютерная система А имеет данные приложения для передачи в систему В, то эти данные сначала передаются на уровень приложений. Затем уровень приложений системы А добавляет к данным всю управляющую информацию, необходимую для уровня приложений системы В, включая ее в заголовок. Полученный модуль данных (заголовок и данные) передается на уровень представления данных, который добавляет собственный заголовок, содержащий управляющую информацию для уровня представления данных системы В. По мере перехода с одного уровня на другой, размер модуля данных растет, так как каждый уровень присоединяет к полученным данным собственный заголовок (а иногда и трейлер), содержащий управляющую информацию для использования тем же уровнем системы В. На физическом уровне весь модуль данных помещается на сетевой носитель.

Физический уровень системы В получает модуль данных и передает его на канальный уровень. Этот уровень системы В просматривает управляющую информацию, содержащуюся в заголовке, помещенном в модуль данных на канальном уровне систе-

мы А. После этого заголовок удаляется, а оставшаяся часть модуля данных передается на сетевой уровень. На остальных уровнях происходит то же самое: заголовок, переданный одноименным уровнем системы А, просматривается, удаляется, а оставшийся модуль данных передается на вышестоящий уровень. После того как эти действия будут выполнены на уровне приложений, данные передаются приложению-получателю системы В в том же виде, в каком они были переданы приложением системы А.

Физический уровень модели OSI

Физический уровень определяет электрические, механические, процедурные и функциональные спецификации по активированию, поддержке и прекращению физической связи между обменивающимися информацией сетевыми системами. Спецификации физического уровня определяют такие характеристики, как уровни напряжения, синхронизацию изменений напряжения, физическую скорость передачи данных, максимальное расстояние, на которые могут передаваться данные, а также характеристики физических соединителей кабелей и устройств. Варианты реализации физического уровня можно разделить на категории в зависимости от спецификаций локальных и распределенных сетей. На рис. 1.7 представлены некоторые общепринятые варианты реализации физического уровня в локальных и распределенных сетях.

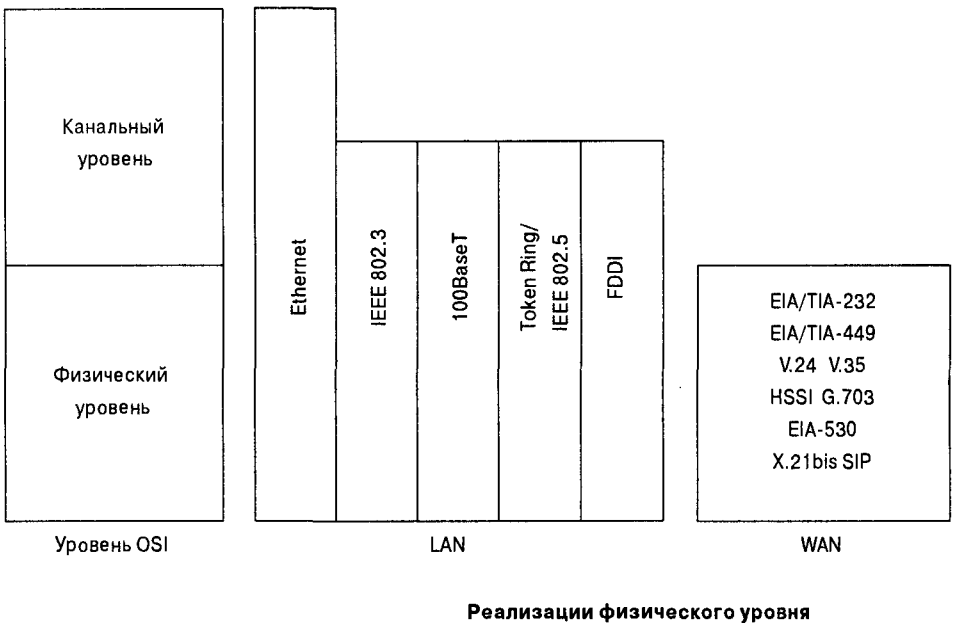


Рис. 1.7. Физический уровень реализуется в виде спецификаций локальных или распределенных сетей

Канальный уровень эталонной модели OSI

Канальный уровень обеспечивает надежную передачу данных по физической сети. Спецификации канального уровня определяют характеристики сети и протоколов, включая физическую адресацию, топологию сети, сообщения об ошибках, регистрацию последовательности фреймов и управление потоком. Физическая адресация

(в отличие от сетевой) определяет способы обращения к устройствам на канальном уровне. Сетевая топология состоит из спецификаций канального уровня, которые зачастую определяют способ физического соединения устройств — например, шинная или кольцевая топология. Сообщения об ошибках предупреждают протоколы высшего уровня, что при передаче данных произошла ошибка, а система управления последовательностью фреймов возвращает на свои места фреймы, переданные в неправильной последовательности. Наконец, система управления потоком регулирует передачу данных таким образом, чтобы интенсивность потока данных, поступающего на вход принимающего устройства, соответствовала возможностям его обработки.

Стандарты института IEEE (Institute of Electrical and Electronics Engineers — IEEE) подразделяют канальный уровень на два подуровня: управление логическим каналом (Logical Link Control — LLC) и управление доступом к носителю (Media Access Control — MAC). Подуровни IEEE канального уровня показаны на рис. 1.8.

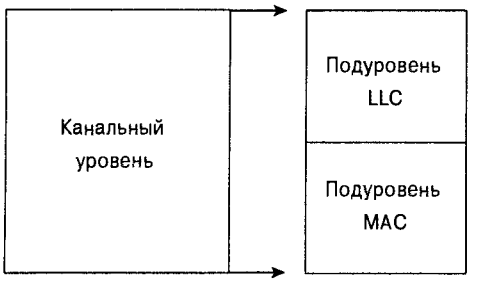


Рис. 1.8. Канальный уровень подразделяется на два подуровня

Подуровень *управления логическим каналом (Logical Link Control — LLC)* управляет обменом данными между устройствами в сети по одной линии связи. Подуровень LLC описан в спецификации IEEE 802.2 и поддерживает как службы, не требующие подтверждения соединения, так и службы, ориентированные на соединение, используемые протоколами высших уровней. Спецификация IEEE 802.2 определяет ряд полей во фреймах канального уровня, которые позволяют нескольким протоколам высших уровней совместно использовать один и тот же физический канал передачи данных. Подуровень *управления доступом к среде передачи (Media Access Control — MAC)* управляет доступом протокола к физическому сетевому носителю. MAC-спецификация IEEE определяет MAC-адреса, которые позволяют нескольким устройствам безошибочно распознавать друг друга на канальном уровне.

Сетевой уровень эталонной модели OSI

На сетевом уровне определяется сетевой адрес (его следует отличать от MAC-адреса). Некоторые реализации сетевого уровня, например протокол Internet (Internet Protocol —IP), определяют сетевые адреса таким образом, чтобы выбор маршрута мог быть сделан с помощью известного алгоритма, например, путем сравнения сетевого адреса источника с сетевым адресом приемника/получателя и наложения маски подсети. Поскольку сетевой уровень определяет логическую структуру сети, маршрутизаторы могут использовать этот уровень для того, чтобы определить направление последующей пересылки пакета. Вследствие этого значительная часть работы по проектированию и конфигурированию объединенных сетей происходит на 3-м (сетевом)уровне.

Транспортный уровень эталонной модели OSI

Транспортный уровень принимает данные от сеансового уровня и сегментирует их для передачи по сети. Как правило, транспортный уровень отвечает за доставку данных без ошибок и в правильной последовательности. Обычно управление потоком происходит именно на этом уровне.

Система управления потоком следит за передачей данных между устройствами для того, чтобы передающее устройство не отправляло больше данных, чем может обработать принимающее устройство. Мультиплексирование позволяет передавать по одному физическому каналу данные от нескольких приложений. На транспортном уровне также создаются, поддерживаются и ликвидируются виртуальные каналы. В целях контроля ошибок создаются различные механизмы распознавания ошибок передачи, а для их исправления выполняются определенные действия, например, запрос на повторную передачу данных.

В сети Internet применяются транспортные протоколы TCP и UDP.

Сеансовый уровень модели OSI

На сеансовом уровне устанавливаются сеансы обмена данными, происходит управление ими и их завершение. Сеансы взаимодействия состоят из запросов к службам и ответов от них, передаваемых между приложениями, находящимися на разных сетевых устройствах. Эти запросы и ответы координируются протоколами, реализованными на сеансовом уровне. В качестве примеров реализации сеансового уровня можно привести протокол Zone Information Protocol (ZIP), используемый в сетях AppleTalk и координирующий процесс привязки имен, протокол управления сеансом (Session Control Protocol — SCP) и протокол сеансового уровня DECnet Phase IV.

Уровень представления эталонной модели OSI

Уровень представления данных обеспечивает выполнение различных операций кодирования и преобразования, которым подвергаются данные уровня приложений. Эти функции гарантируют, что информация, полученная с уровня приложений одной системы, может быть прочитана уровнем приложений другой системы. В качестве примеров схем кодирования и преобразования уровня представления можно привести общеупотребительные форматы представления данных, преобразование символьных форматов, общепринятые схемы сжатия и шифрования данных.

Стандартные форматы представления данных, в том числе изображений, звука и видео, позволяют обмениваться данными приложениям, установленным на компьютерных системах различных типов. Для обмена информацией с системами, использующими различные представления текста и данных, такие как EBCDIC и ASCII, применяются схемы преобразования. Стандартные схемы сжатия позволяют правильно распаковывать, а схемы шифрования — расшифровывать на устройстве-получателе данные, сжатые или зашифрованные на устройстве-источнике.

Реализации уровня представлений обычно не связаны с каким-либо определенным стеком протоколов. В число популярных стандартов для передачи видеоданных входят QuickTime и Motion Picture Experts Group (MPEG). QuickTime является спецификацией компании Apple Computer для обработки видео и аудиоданных, а MPEG представляет собой стандарт сжатия и кодирования видеоданных.

Среди популярных форматов графических изображений следует назвать стандарты Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG) и Tagged Image File Format (TIFF). GIF и JPEG являются стандартами сжатия и кодирования графических изображений, а стандарт TIFF определяет только кодирование данных.

Уровень приложений модели OSI

Уровень приложений представляет собой ближайший к пользователю уровень OSI. Уровень приложений эталонной модели OSI, как и пользователь, непосредственно взаимодействуют с прикладным программным обеспечением.

Этот уровень взаимодействует с приложениями, имеющими в своем составе коммуникационные компоненты. Такие приложения выходят за рамки эталонной модели OSI. Функции уровня приложений обычно состоят в том, чтобы определить партнеров по обмену данными, доступность ресурсов и синхронизировать обмен информацией.

Определяя партнеров по обмену данными, уровень приложений идентифицирует их и определяет их доступность для приложения, которое передает данные. Определяя доступность ресурсов, уровень приложений должен выяснить, имеются ли достаточные сетевые ресурсы для удовлетворения запроса на обмен данными. При синхронном обмене данными взаимодействие между приложениями требует согласованности, которая обеспечивается уровнем приложений.

В качестве примеров реализации уровня приложений можно привести протоколы Telnet, протокол передачи файлов (File Transfer Protocol — FTP) и простой протокол передачи электронной почты (Simple Mail Transfer Protocol — SMTP).

Информационные форматы

Данные и управляющая информация, передаваемые по сети, принимают множество форм. В сетевой индустрии еще нет устоявшейся терминологии для обозначения этих информационных форматов, и иногда под одним термином подразумеваются разные понятия. Общеупотребительными форматами передачи информации являются фреймы, пакеты, дейтаграммы, сегменты, сообщения, ячейки и модули данных.

Фрейм (frame) представляет собой модуль данных, который передается от источника к получателю на канальном уровне. Фрейм состоит из заголовка (и, возможно, трейлера) канального уровня и данных верхнего уровня. Заголовок и трейлер содержат управляющую информацию, предназначенную для канального уровня системы-получателя. Данные, переданные с верхних уровней, инкапсулируются между заголовком и трейлером канального уровня. Основные компоненты фрейма канального уровня показаны на рис. 1.9.

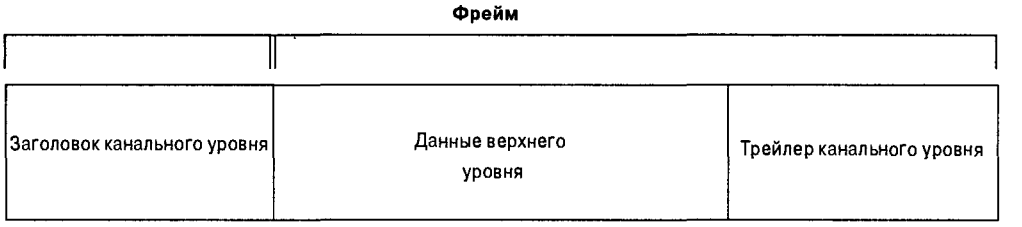


Рис. 1.9. Фрейм канального уровня образован данными, переданными с высших уровней

Пакет представляет собой модуль данных, который передается от источника к получателю на сетевом уровне. Пакет состоит из заголовка (и, возможно, трейлера) сетевого уровня и из данных верхнего уровня. Заголовок и трейлер содержат управляющую информацию, предназначенную для обработки на сетевом уровне системы-получателя. Данные, переданные с верхних уровней, инкапсулируются между заголовком и трейлером сетевого уровня. Основные компоненты пакета сетевого уровня показаны на рис. 1.10.

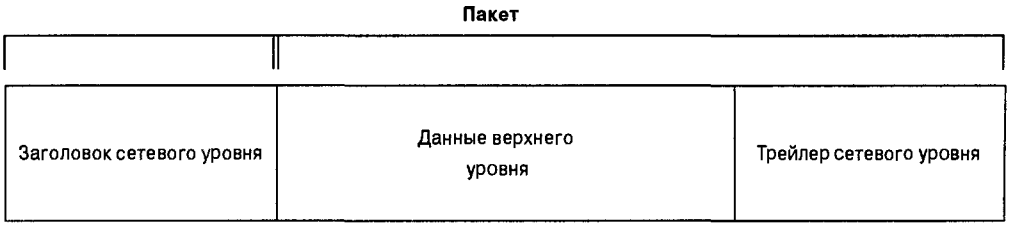


Рис. 1.10. Пакет сетевого уровня состоит из трех основных компонентов

Дейтаграммой (datagram) обычно называют модуль данных, который передается от источника к получателю на сетевом уровне с помощью сетевой службы, не требующей подтверждения соединения.

Сегментом обычно называют модуль данных, который передается от источника к получателю на транспортном уровне.

Сообщение представляет собой модуль данных, который передается от источника к получателю на уровнях выше сетевого (чаще всего это уровень приложений).

Ячейка представляет собой модуль данных фиксированного размера, который передается от источника к получателю на канальном уровне. Ячейки используются в коммутируемых средах, таких как сети асинхронного режима передачи (Asynchronous Transfer Mode — ATM) и коммутируемой мультимегабитовой службы данных (Switched Multimegabit Data Service — SMDS). Ячейка состоит из заголовка и тела. Заголовок содержит управляющую информацию, предназначенную для обработки на канальном уровне принимающей системы, и обычно имеет длину 5 байтов. Тело ячейки представляет собой данные вышестоящих уровней, которые инкапсулируются после заголовка ячейки. Обычно оно имеет длину 48 байтов. Длина поля заголовка и тела во всех ячейках одинакова. Компоненты типичной ячейки показаны на рис. 1.11.

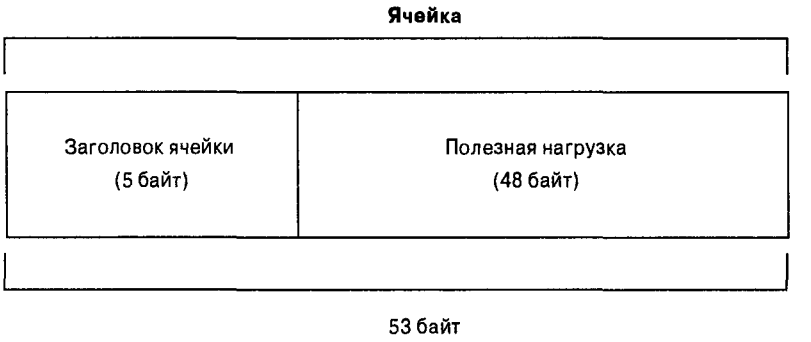


Рис. 1.11. Обычная ячейка состоит из двух компонентов

Модуль данных (data unit) представляет собой базовый термин, обозначающий различные блоки информации. Примерами таких модулей могут служить модули данных служб (Service Data Unit — SDU), модули данных протокола (Protocol Data Unit — PDU) и модули данных протокола моста (Bridge Protocol Data Unit — BPDU). Модули SDU являются модулями данных протоколов верхнего уровня, которые определяют запрос на обслуживание протоколом более низкого уровня. Модулем PDU в терминологии OSI называется пакет. Модули BPDU используются алгоритмом связующего дерева в качестве сообщений приветствия (hello messages).

Иерархия сетей по стандарту ISO

Крупные сети обычно имеют иерархическую структуру. Иерархическая организация имеет такие преимущества, как простота управления, гибкость и сокращение передачи лишних данных. Международная организация по стандартизации (International Organization for Standardization — ISO) ввела некоторые терминологические соглашения для обозначения элементов сети. В этом разделе будут даны определения следующих ключевых терминов: конечная система (ES), промежуточная система (IS), зона и автономная система (AS).

Конечная система (End System — ES) представляет собой сетевое устройство, которое не выполняет маршрутизации или других функций перенаправления данных. Обычно к конечным системам относятся такие устройства, как терминалы, персональные компьютеры и принтеры.

Промежуточная система (Intermediate System — IS) представляет собой сетевое устройство, осуществляющее маршрутизацию или другие функции перенаправления данных. Обычно к промежуточным устройствам относят такие устройства, как маршрутизаторы, коммутаторы и мосты. Существует два вида сетевых промежуточных систем: внутридоменные и междоменные. Внутридоменные IS осуществляют обмен данными с устройствами внутри одной автономной системы, а междоменные — как внутри своей автономной системы, так и с другими автономными системами.

Зона (area) представляет собой логическую группу сетевых сегментов и подключенных к ним устройств. Зоны являются подразделениями автономных систем.

Автономная система (Autonomous System — AS) представляет собой набор сетей, администрируемых совместно и использующих одну и ту же стратегию маршрутизации. Автономные системы делятся на зоны. Иногда автономные системы AS называются доменами. Иерархически организованная сеть и ее компоненты показаны на рис. 1.12.

Сетевые службы, ориентированные на соединение, и службы, не требующие подтверждения соединения

Обычно транспортные протоколы делятся на соединения, требующие подтверждения, и соединения, не требующие его. Службы, ориентированные на соединение, прежде чем передавать данные, должны сначала установить соединение с требуемой службой. Службы, не требующие подтверждения соединения, могут пересылать данные без предварительной установки соединения. Как правило, службы, ориентированные на соеди-

нение, предоставляют некоторую гарантию доставки, тогда как службы, не требующие подтверждения соединения, не могут этого гарантировать.

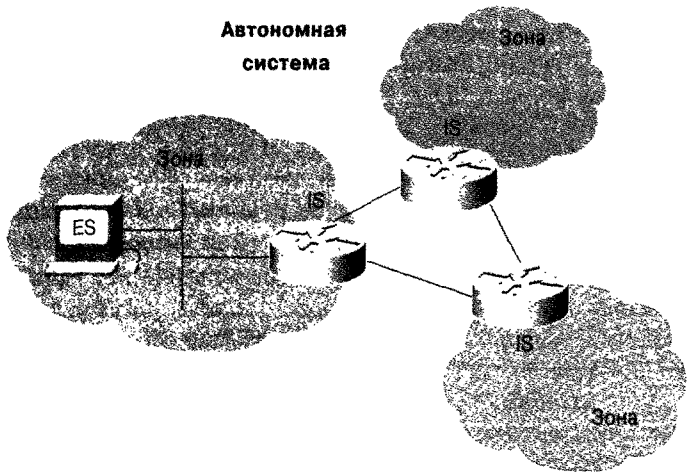


Рис. 1.12. Компоненты иерархической сети

Служба, ориентированная на соединение, работает в три этапа: устанавливает соединение, передает данные и ликвидирует соединение.

При установке соединения конечные узлы могут зарезервировать ресурсы для этого соединения. Они также могут провести переговоры и установить определенные критерии передачи данных, например размер окна, как это делается при использовании соединений протокола TCP. Именно резервирование ресурсов иногда используется для атак типа "отказ в обслуживании" (Denial Of Service — DOS). Атакующая система посылает большое количество запросов на установку соединения, но не разрывает эти соединения. В результате на атакуемом компьютере все ресурсы оказываются зарезервированы для незаконченных соединений, и при попытке установить настоящее соединение оказывается, что для этого не хватает ресурсов.

Этап передачи данных начинается в тот момент, когда по установленному соединению начинается пересылка самих данных. Во время передачи данных большинство служб, ориентированных на соединение, следит за тем, чтобы пакеты не пропадали, и если это все же случается, то запрашивает их повторную передачу. Как правило, протоколы отвечают также за расположение принятых пакетов в правильной последовательности, прежде чем данные будут переданы выше по стеку протоколов.

Когда передача данных окончена, конечные узлы разрывают соединение и освобождают зарезервированные для него ресурсы.

Сетевые службы, ориентированные на соединение, вызывают в сети большую нагрузку, чем службы, не требующие подтверждения соединения, так как первым требуется провести переговоры для установки соединения, передать данные или ликвидировать

соединение, а вторым достаточно просто отправить данные, не загружая сеть созданием и ликвидацией соединений. Каждый из этих способов передачи находит свое применение в объединенных сетях.

Адресация в объединенных сетях

Межсетевые адреса (internetwork addresses) идентифицируют устройства отдельно или в качестве членов некоторой группы. Схема адресации зависит от используемого семейства протоколов и уровня OSI. Широко используются три вида межсетевых адресов: адреса канального уровня, адреса управления доступом к носителю, или MAC-адреса (Media Access Control — MAC), и адреса сетевого уровня.

Адреса канального уровня

Адрес канального уровня уникальным образом идентифицирует каждое физическое соединение устройства с сетью. Такие адреса иногда называют *физическими* или *аппаратными адресами*. Адреса канального уровня обычно образуют линейное пространство адресов. Они заранее и, как правило, жестко привязаны к определенному устройству.

Конечные системы обычно имеют только одно физическое соединение с сетью, и следовательно, только один адрес канала передачи данных. Маршрутизаторы и другие межсетевые устройства чаще всего имеют несколько физических сетевых соединений и, соответственно, несколько адресов канала передачи данных. На рис. 1.13 показано, как интерфейсы устройства уникальным образом идентифицируются адресом канала передачи данных.

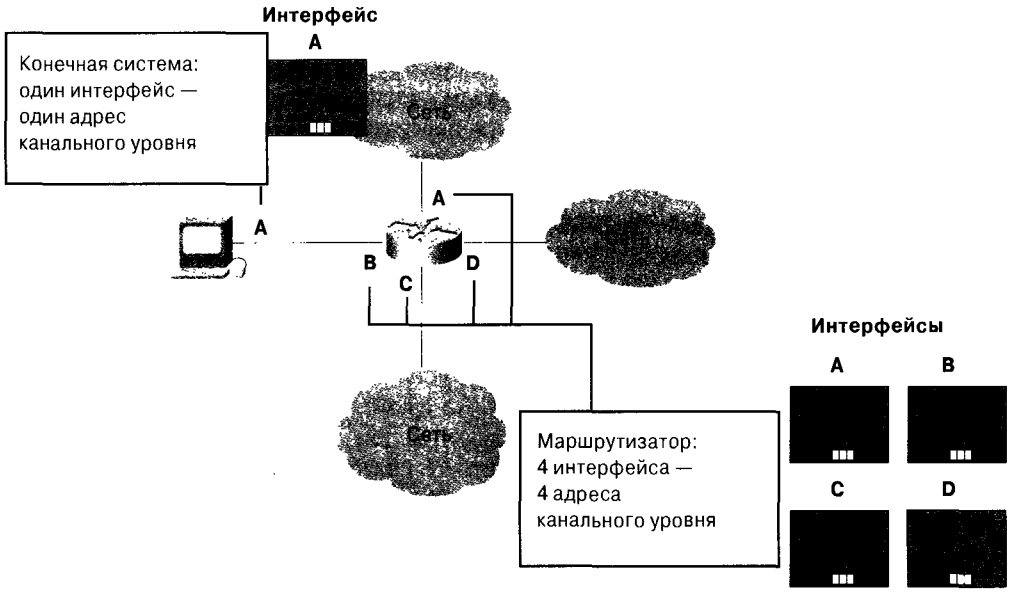


Рис. 1.13. Каждый интерфейс устройства уникальным образом идентифицируется адресом канального уровня

MAC-адреса

Адреса *управления доступом к среде передачи (Media Access Control — MAC)* состоят из набора адресов канального уровня. MAC-адреса идентифицируют сетевые устройства в локальных сетях с использованием адреса канального уровня согласно стандарту IEEE MAC. Как и большинство адресов канала передачи данных, MAC-адреса уникальны для каждого интерфейса локальной сети LAN. Отношения между MAC-адресами, адресами канала передачи данных и подуровнями канального уровня согласно стандарту IEEE показаны на рис. 1.14.

MAC-адреса являются 48-разрядными и записываются в виде 12-значного шестнадцатеричного числа. Первые 6 шестнадцатеричных цифр, которые определяются стандартом IEEE, идентифицируют производителя или поставщика и поэтому являются уникальным идентификатором организации (Organizationally Unique Identifier — OUI). Последние 6 шестнадцатеричных цифр содержат серийный номер интерфейса или другое значение, определяемое стандартом указанного производителя. MAC-адреса иногда называют *прошитыми адресами (Burned-In Address — BIA)*, так как они находятся в постоянной памяти (ROM) и копируются оттуда в оперативную память (RAM) при инициализации интерфейсной платы. Формат MAC-адреса показан на рис. 1.15.

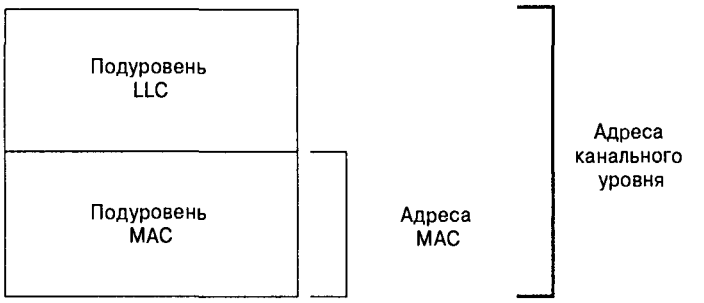


Рис. 1.14. Взаимосвязь MAC-адресов, адресов канального уровня и канальных подуровней согласно стандарту IEEE

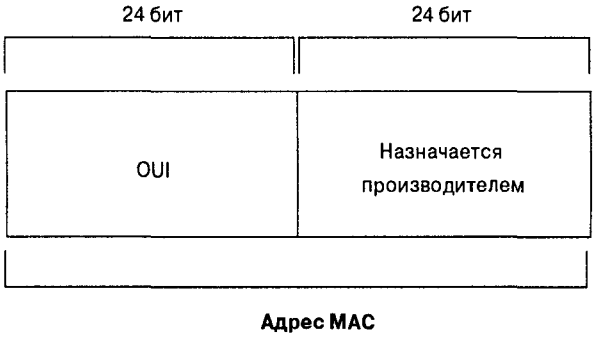


Рис. 1.15. MAC-адрес представляет собой уникальное шестнадцатеричное число

Преобразование адресов

Поскольку для маршрутизации пакетов в объединенных сетях используются, как правило, сетевые адреса, возникает необходимость в их преобразовании в MAC-адреса. На сетевом уровне определяется сетевой адрес станции-получателя, однако при передаче по физической сети необходимо использование MAC-адреса. Различные наборы протоколов используют разные методы такого преобразования, но наиболее популярным методом является использование протокола преобразования адресов (Address Resolution Protocol — ARP).

В различных наборах протоколов применяются разные методы определения MAC-адреса устройства. Наиболее часто используются следующие методы: протокол ARP, преобразующий сетевые адреса в MAC-адреса, и протокол приветствия, позволяющий сетевым устройствам распознавать MAC-адреса других сетевых устройств. MAC-адреса либо внедряются в адрес сетевого уровня, либо генерируются по особому алгоритму.

Протокол преобразования адресов (Address Resolution Protocol — ARP) представляет собой метод преобразования адресов, используемый в наборе протоколов TCP/IP. Когда сетевому устройству требуется отправить данные другому устройству в той же сети, он использует для этого сетевые адреса источника и получателя данных. Прежде чем направить данные, устройство должно преобразовать адрес получателя в MAC-адрес. Сначала рабочая станция, отправляющая данные, просматривает свою ARP-таблицу, проверяя, был ли в нее ранее занесен MAC-адрес рабочей станции-получателя. Если в таблице такой адрес отсутствует, то станция посылает в сеть широковещательный запрос, содержащий IP-адрес станции-получателя. Все станции в сети, получившие этот запрос, сравнивают содержащийся в нем IP-адрес с собственным, и только та станция, чей IP-адрес совпал с запрошенным, посылает отправляющей станции пакет, содержащий ее MAC-адрес. После этого первая станция добавляет эту информацию в ARP-таблицу для случая, если он потребуется в будущем и пересылает данные.

Если устройство-получатель находится в удаленной сети, подключенной через маршрутизатор, то выполняется этот же процесс, но станция, отправляющая данные, отправляет ARP-запрос на получение MAC-адреса своего шлюза, используемого по умолчанию. После этого она направляет информацию на шлюз, а он в свою очередь передает ее в соответствующем направлении, чтобы доставить пакет в сеть, где находится устройство-получатель. Затем маршрутизатор сети, в которой находится устройство-получатель, использует пл ARP для получения MAC-адреса этого устройства и доставляет ему пакет.

Протокол приветствия (Hello protocol) представляет собой протокол сетевого уровня, позволяющий сетевым устройствам идентифицировать друг друга и сообщать всем другим устройствам о своем присутствии в сети. Например, когда включается очередная конечная система, она рассылает по сети сообщения приветствия и получает от других устройств этой сети ответы на них. Затем рассылка сообщений приветствия повторяется через определенные интервалы времени, чтобы сообщить о том, что устройство продолжает присутствовать в сети. Сетевые устройства узнают MAC-адреса других устройств, просматривая пакеты протокола приветствия.

Предсказуемые MAC-адреса используются тремя протоколами: Xerox Network Systems (XNS), протоколом межсетевого пакетного обмена (Novell Internetwork Packet Exchange — IPX) и протоколом DECnet Phase IV. В этих наборах протоколов MAC-адреса предсказуемы потому, что сетевой уровень либо включает MAC-адрес в адрес сетевого уровня, либо использует алгоритм определения MAC-адреса.

Адреса сетевого уровня

Адрес сетевого уровня идентифицирует объект на сетевом уровне модели OSI. Сетевые адреса обычно образуют иерархическое пространство и иногда называются *виртуальными* или *логическими адресами*.

Отношения между сетевым адресом и устройством — логические и непостоянные; они обычно основываются либо на физических характеристиках сети (устройство находится в определенном сегменте сети), либо на группировании, не имеющем под собой физической основы (например, когда устройство является частью зоны AppleTalk). Конечные системы требуют одного адреса сетевого уровня для каждого поддерживаемого ими протокола сетевого уровня (исходя из предположения, что устройство имеет только одно физическое сетевое соединение.) Маршрутизаторы и другие межсетевые устройства требуют одного адреса сетевого уровня на каждое физическое сетевое соединение для каждого поддерживаемого протокола сетевого уровня. Например, маршрутизатор с тремя интерфейсами, каждый из которых поддерживает протоколы AppleTalk, TCP/IP и OSI, должен иметь по три адреса сетевого уровня для каждого интерфейса. Таким образом, у этого маршрутизатора должно быть девять адресов сетевого уровня. Каждому сетевому интерфейсу назначается сетевой адрес для каждого поддерживаемого им протокола (рис. 1.16).

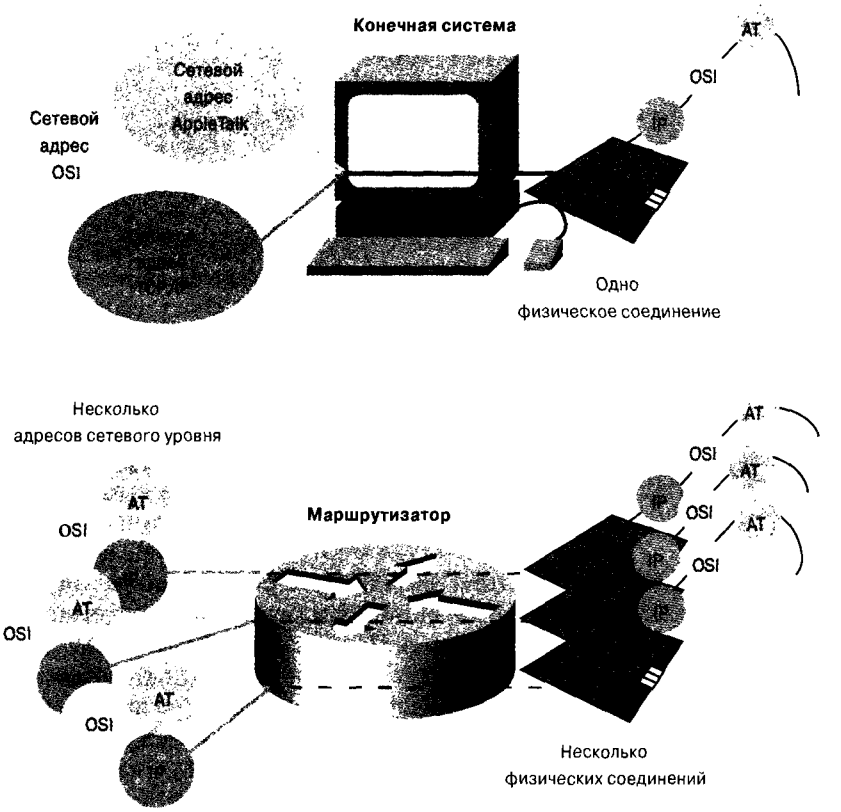


Рис. 1.16. Каждому сетевому интерфейсу должен назначаться сетевой адрес для каждого поддерживаемого им протокола

Иерархическое и линейное пространства адресов

Существует два способа построения пространства адресов в объединенной сети: иерархическое и линейное. *Иерархическое пространство адресов (hierarchical address space)* организовано в виде многочисленных подгрупп, каждая из которых последовательно сужает адресуемую область, пока не получится указатель на одно устройство (наподобие почтовых адресов). *Линейное пространство адресов (flat address space)* организовано в виде одной группы (наподобие номеров социального страхования).

Иерархическая адресация имеет определенные преимущества перед линейной. Сортировка и выборка адресов упрощается благодаря операциям сравнения. Например, наличие в почтовом адресе слова "Ирландия" исключает все остальные страны. Различия между иерархическим и линейным пространствами адресов показаны на рис. 1.17.

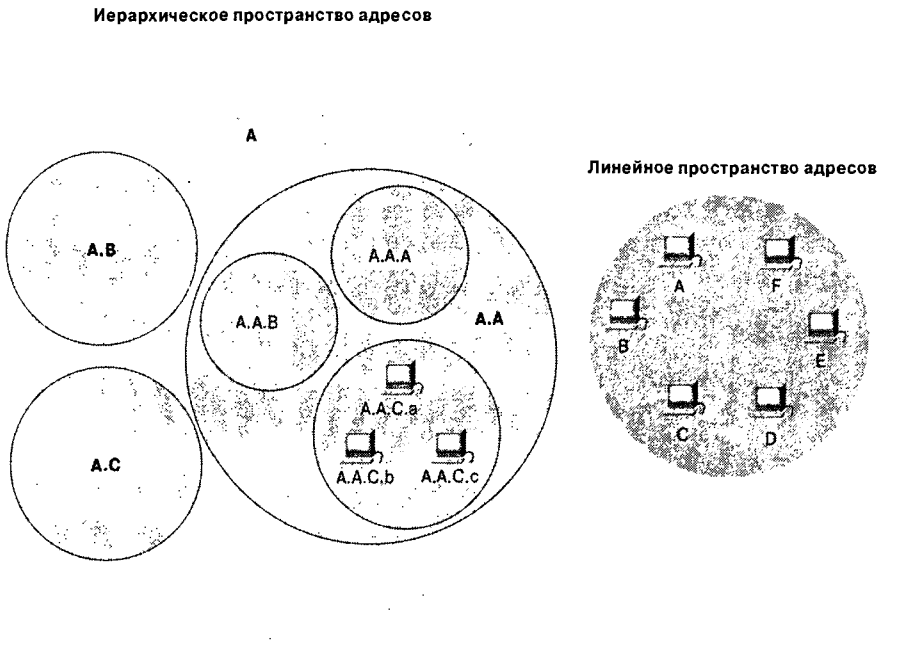


Рис. 1.17. Иерархическое и линейное пространства адресов различаются в операциях сравнения

Назначение адресов

Адреса, назначаемые устройствам, бывают двух видов: статические и динамические. *Статические адреса* назначаются администратором сети в соответствии с предварительно составленным планом межсетевой адресации. Статический адрес остается неизменным до тех пор, пока он не будет изменен администратором сети. При подключении устройства к сети, оно получает *динамический адрес*, причем процедура его назначения зависит от протокола. При использовании динамических адресов адрес устройства обычно изменяется при каждом подключении к сети. В некоторых сетях адреса назначаются сервером. После отключения устройства от сети его адрес, назначенный сервером, может быть назначен другому устройству, а это устройство при следующем подключении к сети, вероятнее всего, будет иметь другой адрес.

Адреса и имена устройств

Межсетевым устройствам обычно назначаются как имя, так и адрес. Для межсетевых имен характерна независимость от расположения устройства. Эти адреса закрепляются за устройством и не изменяются при его перемещении (например, из одного здания в другое). Межсетевые адреса обычно зависят от расположения устройства и изменяются при его перемещении (MAC-адреса — исключение из этого правила). Подобно тому, как сетевые адреса преобразуются в MAC-адреса, имена обычно трансформируются в сетевые адреса посредством какого-либо протокола. В сети Internet для преобразования имени устройства в его IP-адрес используется система имен домена (Domain Name System — DNS). Запомнить адрес www.cisco.com значительно проще, чем соответствующий IP-адрес. В том случае, когда пользователю требуется получить доступ к Web-узлу Cisco, ему достаточно ввести в браузере имя www.cisco.com. После этого компьютер формирует DNS-запрос на получение IP-адреса Web-сервера Cisco, а затем обменивается с ним данными, используя сетевой адрес.

Основы управления потоком

Управление потоком представляет собой функцию, которая предотвращает перегрузку сети, гарантируя, что передающие устройства не отправляют данных больше, чем способны обработать принимающие устройства. Например, высокоскоростной компьютер может генерировать данные для передачи быстрее, чем сеть имеет возможность его передать, или быстрее, чем устройство-получатель может его принять и обработать. Существует три общеупотребительных способа избежать перегрузки сети: с помощью буферизации, путем отправки сообщений, снижающих скорость передачи данных, и с использованием окон.

Буферизация применяется для временного хранения в памяти сетевых устройств порций данных до тех пор, пока не освободится обрабатывающее устройство. При помощи буферизации можно справиться с появляющимся время от времени избытком данных. Однако такие данные могут занять всю память, и тогда все последующие поступающие на устройство дейтаграммы будут отброшены.

Сообщения, снижающие скорость передачи данных, отправляются принимающими устройствами для предотвращения переполнения их буферов. Принимающее устройство посылает такие сообщения, чтобы заставить источник данных снизить текущую скорость передачи. Сначала принимающее устройство начинает отбрасывать все принятые данные из-за переполнения буферов. Затем принимающее устройство начинает посылать передающему устройству сообщения с требованием снизить скорость передачи данных, по одному на каждый отброшенный пакет. Устройство-источник получает эти сообщения и постепенно снижает скорость передачи до тех пор, пока такие сообщения не перестанут поступать. Затем устройство-источник постепенно увеличивает скорость передачи, пока такие сообщения не появятся снова.

Использование окон представляет собой схему управления потоком, в которой устройство-источник требует от устройства-получателя подтверждения после передачи определенного количества пакетов. Например, если размер окна равен 3, то источник требует подтверждения после отправки трех пакетов. Сначала устройство-источник посылает три пакета устройству-получателю. После их получения устройство-получатель направляет подтверждение устройству-источнику. Последнее принимает подтверждение и посылает еще три пакета. Если получатель по какой-либо причине,

например, из-за переполнения буферов, не получает хотя бы один из отправленных пакетов, то он не отправляет подтверждение. В этом случае устройство-источник повторяет передачу пакетов на пониженной скорости.

Основы контроля ошибок

Схемы контроля ошибок определяют, были ли переданные данные повреждены на пути от источника к получателю. Контроль ошибок реализуется на нескольких уровнях эталонной модели OSI.

Одной из наиболее часто используемых схем контроля ошибок является контроль с помощью циклического избыточного кода (Cyclic Redundancy Check — CRC), при котором поврежденные данные распознаются и отбрасываются. Функции исправления ошибок (такие как повторная передача данных) переносятся в протоколы высшего уровня. Значение CRC генерируется с помощью вычислений, выполняемых на устройстве-источнике. Устройство-получатель сравнивает это значение с результатом собственных вычислений и определяет, возникли ли ошибки при передаче. Сначала устройство-источник выполняет над содержимым передаваемого пакета заранее заданную последовательность вычислений. Затем оно помещает вычисленное значение в пакет и отправляет его получателю. Получатель выполняет над содержимым пакета те же вычисления, после чего сравнивает полученное значение с тем, которое содержится в пакете. Если эти значения равны, то считается, что пакет не содержит ошибок. В противном случае в пакете предполагается наличие ошибок и он отбрасывается.

Основы мультиплексирования

Мультиплексирование представляет собой процесс, в котором несколько каналов данных объединяются в один канал данных или в физический канал на устройстве-источнике. Мультиплексирование может быть реализовано на любом уровне OSI. Обратный процесс — разделение мультиплексированных каналов данных на устройстве-получателе — называется *демультиплексированием*. Примером мультиплексирования является случай, когда данные от нескольких приложений объединяются в один пакет низкого уровня (рис. 1.18).

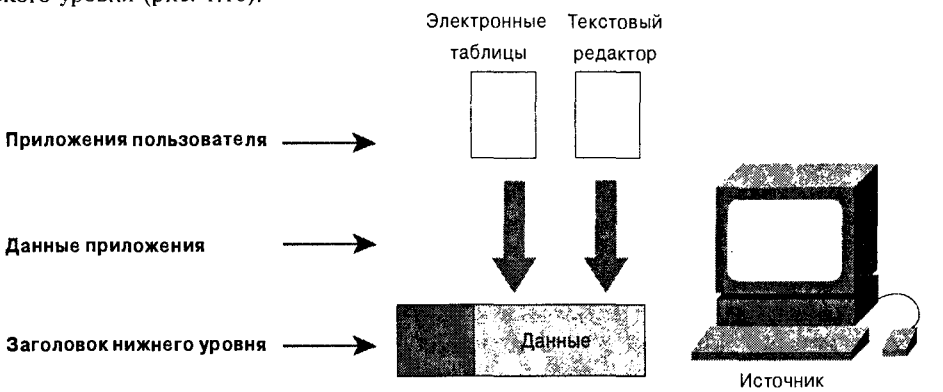


Рис. 1.18. Данные от нескольких приложений могут быть мультиплексированы в один пакет данных низкого уровня

Другим примером мультиплексирования может служить объединение данных от нескольких устройств в один физический канал с использованием устройства, называемого мультиплексором (рис. 1.19).

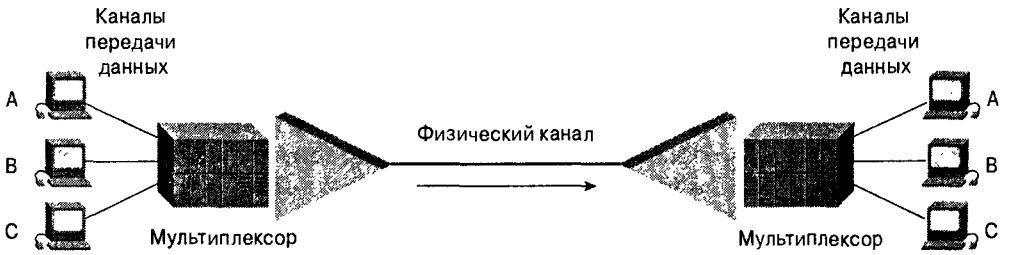


Рис. 1.19. Несколько устройств могут быть мультиплексированы в один физический канал

Мультиплексор представляет собой устройство физического уровня, объединяющее несколько потоков данных, поступающих от различных источников, в один или несколько исходящих каналов. На удаленной системе мультиплексоры выполняют демультиплексирование каналов, т.е. восстанавливают несколько исходных потоков данных, позволяя максимально эффективно использовать полосу пропускания физической среды передачи путем передачи данных одновременно от нескольких источников.

К методам мультиплексирования данных относятся мультиплексирование с разделением времени (Time-Division Multiplexing — TDM), асинхронное мультиплексирование с разделением времени (Asynchronous Time-Division Multiplexing — ATDM), мультиплексирование с разделением частоты (Frequency-Division Multiplexing — FDM) и статистическое мультиплексирование.

При использовании мультиплексирования TDM полоса пропускания для информации, поступающей из каждого канала данных, выделяется на основе предварительно назначенных временных интервалов, независимо от наличия передаваемых данных. При использовании ATDM-мультиплексирования такое выделение осуществляется по мере необходимости, а сами временные интервалы назначаются динамически. При использовании FDM-мультиплексирования полоса пропускания выделяется на основе частоты сигнала поступающих данных. При статистическом мультиплексировании полоса пропускания выделяется динамическим образом всем каналам данных, которые имеют информацию для передачи.

Разработчики стандартов

Разработкой стандартов объединенных сетей занимаются самые разные организации путем проведения форумов, превращения неформальных обсуждений в формальные спецификации и распространения их после стандартизации.

Большинство организаций, занимающихся стандартизацией, создают формальные стандарты путем проведения специальных мероприятий: формулирования организационных идей, обсуждения подходов, разработки черновых стандартов, голосования по всем или некоторым аспектам. После этого официально издается законченный стандарт.

Ниже приведены некоторые наиболее известные организации, занимающиеся стандартизацией объединенных сетей.

- **Международная организация по стандартизации (International Organization for Standardization — ISO).** ISO является международной организацией, отвечающей за самые различные стандарты, включая многие из тех, которые относятся к сетям. Ее самым известным вкладом в стандартизацию сетей является разработка модели OSI и набора протоколов OSI.
- **Американский национальный институт стандартов (American National Standards Institute — ANSI).** Институт ANSI входит в состав ISO и является координатором групп по стандартизации, формируемых в США на общественных началах. В ANSI был разработан интерфейс распределенной передачи данных по оптоволоконным каналам (Fiber Distributed Data Interface — FDDI) и другие коммуникационные стандарты.
- **Ассоциация электронной промышленности (Electronic Industries Association — EIA).** Ассоциация EIA разрабатывает стандарты передачи данных по электрическим сетям, в том числе и по компьютерным сетям. В EIA разработан широко используемый стандарт EIA/TIA-232 (ранее известный как RS-232).
- **Институт инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronic Engineers — IEEE).** IEEE является профессиональной организацией, разрабатывающей сетевые и другие стандарты. В IEEE разработаны широко используемые стандарты локальных сетей IEEE 802.3 и IEEE 802.5.
- **Международный союз по телекоммуникациям, сектор стандартизации (International Telecommunication Union Telecommunication Standardization Sector — ITU-T).** Ранее он назывался Комитетом по международной телеграфии и телефонии (Committee for International Telegraph and Telephone — CCITT). В настоящее время ITU-T является международной организацией, разрабатывающей стандарты по телекоммуникациям. В частности, в ITU-T был разработан стандарт X.25.
- **Комитет по вопросам деятельности в Internet (Internet Activities Board — IAB).** Комитет IAB представляет собой группу исследователей объединенных сетей, обсуждающих вопросы, касающиеся сети Internet, и определяющих общую политику в Internet, принимая решения и формируя для этого рабочие группы. Комитет IAB выпустил некоторые документы Request For Comments (RFC), принятые в качестве стандартов сети Internet, включая протоколы TCP/IP (Transmission Control Protocol/Internet Protocol) и SNMP (Simple Network Management Protocol).

Резюме

Объединенные сети являются сложными системами, рассмотрение которых в целом может представлять значительные трудности. Для упрощения понимания структуры объединенной сети целесообразно разделить сеть на концептуальные части. При чтении литературы по объединенным сетями и при работе с ними рекомендуется рассматривать эти сети в аспекте модели OSI и ее концептуальных составляющих.

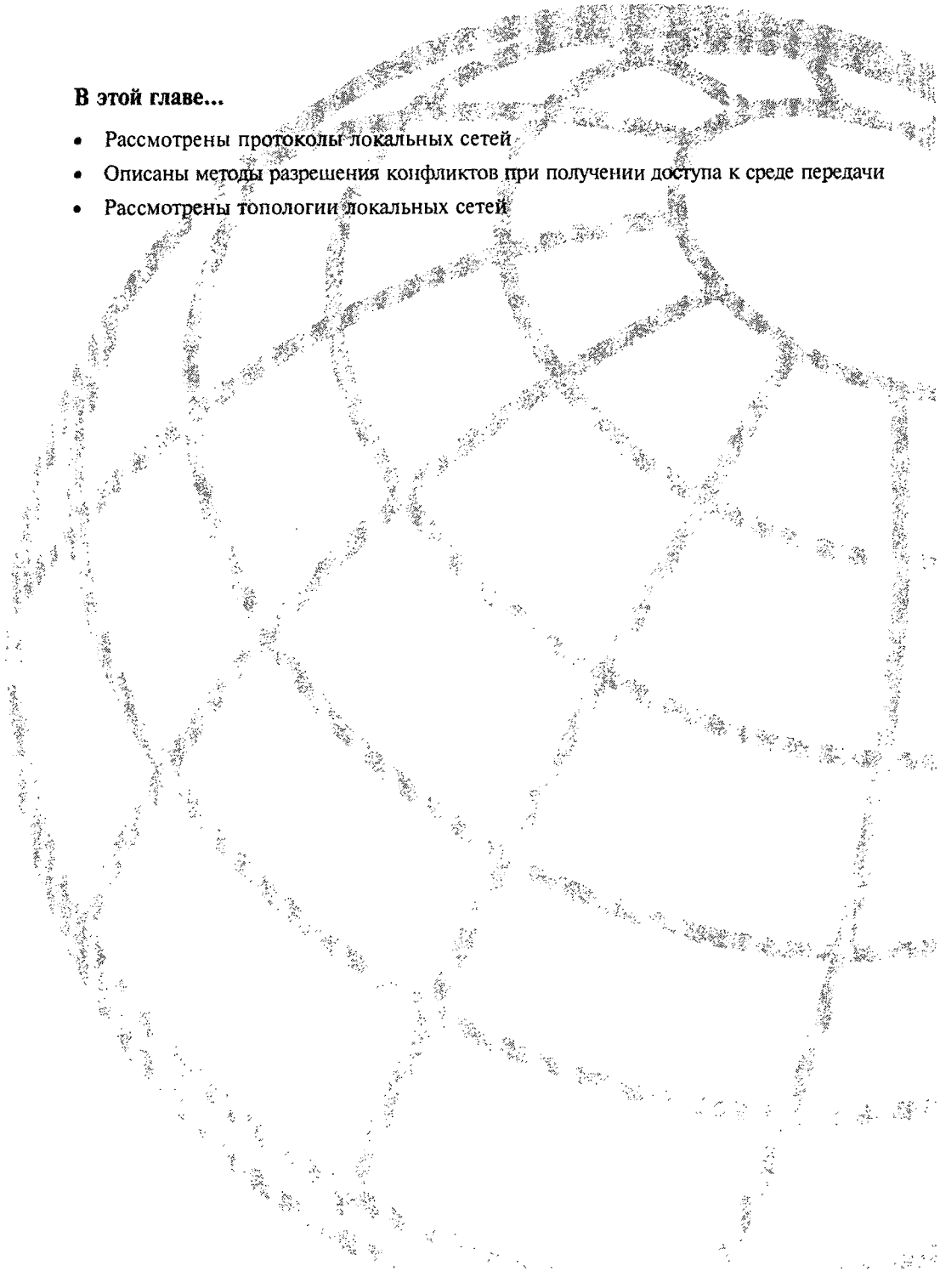
Понимание характера обмена данными между различными уровнями и протоколами позволяет проектировать и конфигурировать объединенные сети, а также проводить их диагностику. Недостаточное понимание блоков, составляющих объединенную сеть, значительно затрудняет анализ их взаимодействия.

Контрольные вопросы

1. Из каких уровней состоит модель OSI?
2. Какой уровень определяет выбор маршрута в объединенной сети?
3. Что именно определяется на физическом уровне?
4. Какие существуют методы преобразования сетевых адресов в адреса MAC?
5. Какие службы сильнее нагружают сеть: ориентированные на соединение или не требующие подтверждения соединения?

Дополнительные источники

- Важным источником дополнительной информации по рассмотренным выше темам является Web-сайт корпорации Cisco (www.cisco.com). В разделе документации этого сайта приведено подробное описание многих вопросов, затронутых в этой главе.
- Teare D. *Designing Cisco Networks.* Cisco Press, 1999.



В этой главе...

- Рассмотрены протоколы локальных сетей
- Описаны методы разрешения конфликтов при получении доступа к среде передачи
- Рассмотрены топологии локальных сетей

Глава 2

Основы протоколов локальных сетей

В настоящей главе описываются различные методы доступа к среде передачи, методы передачи данных, а также топологии и устройства, используемые в локальных сетях (local-area network — LAN). Особое внимание уделяется методам и устройствам, используемым в стандартах Ethernet/IEEE 802.3, Token Ring/IEEE 802.5 и Fiber Distributed Data Interface (Fiber Distributed Data Interface — FDDI). В части II этой книги данные протоколы будут описаны более подробно. Базовые схемы этих трех вариантов реализации LAN-сетей показаны на рис. 2.1.

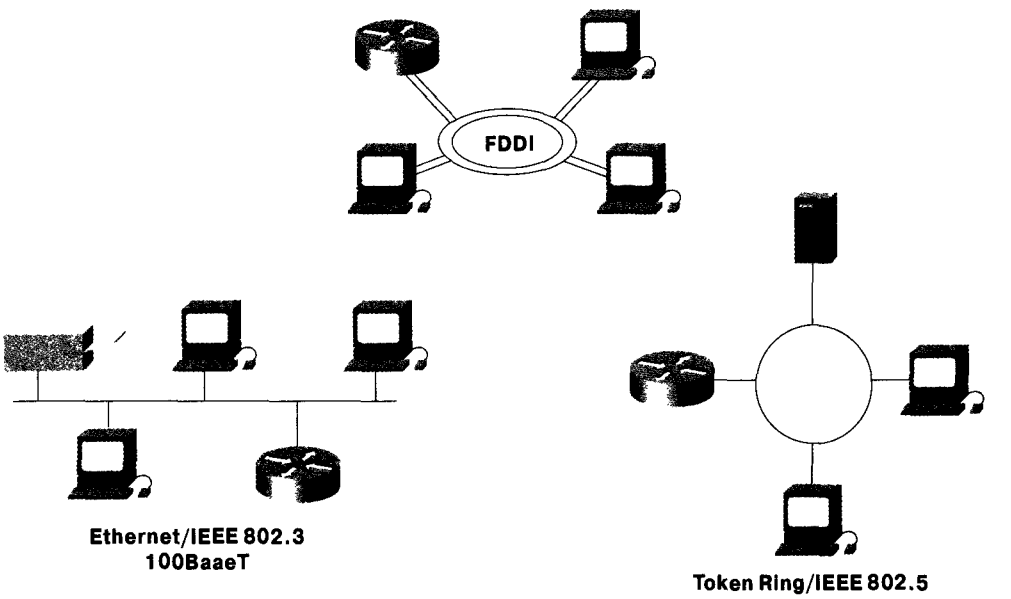


Рис. 2.1. Три наиболее часто используемые конфигурации локальных сетей

Что такое локальная сеть?

Локальная сеть (Local Area Network — LAN) представляет собой сеть с высокой скоростью передачи данных, ограниченную относительно небольшой географической

областью. Обычно в такую сеть объединяются рабочие станции, персональные компьютеры, принтеры, серверы и другие устройства. Локальные сети предоставляют пользователям компьютеров много преимуществ, включая совместный доступ к устройствам и приложениям, обмен файлами между пользователями, общение по электронной почте и другие приложения.

Протоколы локальных сетей и эталонная модель OSI

Как отмечалось в главе 1 "Основы теории объединенных сетей", протоколы локальных сетей работают на двух самых нижних уровнях эталонной модели OSI — между физическим и канальным. Соответствие нескольких наиболее распространенных протоколов локальных сетей уровням модели OSI показано на рис. 2.2.

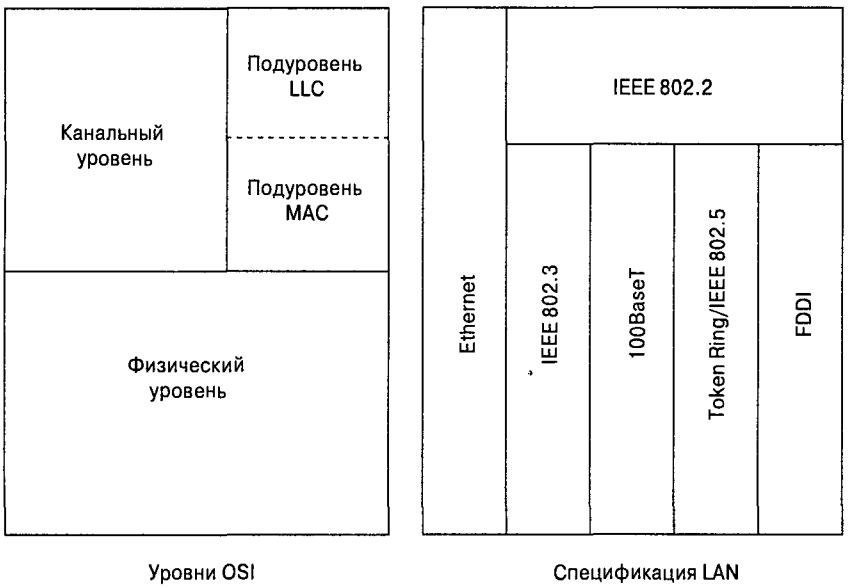


Рис. 2.2. Соответствие распространенных протоколов локальных сетей уровням модели OSI

Методы доступа к среде передачи в локальных сетях

Если сразу несколько сетевых устройств пытаются одновременно отправить данные, то возникает конфликт доступа к среде передачи. Поскольку несколько устройств не могут одновременно передавать данные по сети , требуется какой-либо метод, позволяющий в каждый момент времени обращаться к сетевой среде передачи данных только одному устройству. Для этого обычно применяется один из двух способов: множествен-

ный доступ с обнаружением несущей и обнаружением коллизий (Carrier Sense Multiple Access/Collision Detect — CSMA/CD) и передача маркера.

В сетях, использующих технологию *CSMA/CD*, таких как сети Ethernet, сетевые устройства "соперничают" за доступ к сетевой среде передачи данных. Когда устройству требуется отправить данные, оно сначала прослушивает сеть, чтобы узнать, не использует ли ее в данный момент какое-либо другое устройство. Если сеть свободна, то устройство начинает передавать свои данные. После того как передача данных закончится, устройство снова прослушивает сеть, чтобы узнать, не возникло ли коллизии. Коллизия возникает, когда два устройства посылают данные одновременно. Если коллизия произошла, то каждое из этих устройств ожидает в течение некоторого случайно выбираемого промежутка времени, а затем отправляет данные повторно. В большинстве случаев коллизия между этими двумя устройствами не повторяется. Вследствие такого "соперничества" устройств увеличение нагрузки в сети вызывает увеличение числа коллизий. Поэтому при увеличении количества устройств в сети Ethernet ее производительность резко падает.

В *сетях с передачей маркера (token-passing)*, таких как Token Ring и FDDI, по всей сети, от устройства к устройству, передается специальный пакет, называемый *маркером (token)*. Если устройству требуется отправить данные, то оно ждет, пока не будет получен маркер, и только затем посылает данные. Когда передача данных окончена, маркер освобождается, и тогда сетевая среда может быть использована другими устройствами. Основное преимущество таких сетей состоит в том, что происходящие в них процессы в них детерминированы, т.е., легко подсчитать максимальное время, в течение которого устройство должно ожидать возможности отправить данные. Этим объясняется популярность сетей с передачей маркера в некоторых средах, работающих в режиме реального времени, например, в сфере производства, где необходимо обеспечить обмен данными между устройствами через строго определенные интервалы времени.

В сетях множественного доступа CSMA/CD могут использоваться коммутаторы, которые сегментируют сеть на несколько коллизионных доменов. Это уменьшает количество устройств, "соперничающих" за среду передачи, в каждом сегменте сети. За счет создания более мелких коллизионных доменов можно существенно увеличить производительность сети без изменения системы адресации.

Обычно соединения сети CSMA/CD являются полудуплексными. Термин "полудуплексное соединение" означает, что устройство не может одновременно отправлять и получать информацию. Пока устройство передает данные, оно не может следить за поступающими данными. Это очень напоминает устройство "walkie-talkie": при необходимости что-либо сказать нажимается кнопка передачи и, пока говорящий не закончит , никто другой не может говорить на этой же частоте. Когда говорящий заканчивает, он отпускает кнопку передачи и тем самым освобождает частоту для остальных.

При использовании коммутаторов становится возможной реализация режима полного дуплекса. Полнодуплексное соединение работает так же, как и телефон: можно одновременно и слушать, и говорить. Если сетевое устройство подключено непосредственно к порту сетевого коммутатора, то эти два устройства смогут работать в режиме полного дуплекса. В этом режиме производительность сети может увеличиться. Сегмент Ethernet 100 Мбит/с способен передавать данные со скоростью 200 Мбит/с, но из них в одном направлении только 100 Мбит/с. Поскольку большинство соединений асимметричны (в одном направлении передается больше данных, чем в другом), то выигрыш оказывается не столь велик, как полагают некоторые. Однако работа в полнодуплексном режиме все же увеличивает пропускную способность многих приложений, поскольку в этом случае сетевая среда передачи уже не является общей.

Используя полнодуплексное соединение, два устройства, могут начать отправку данных сразу же после его установки.

В сетях с передачей маркера, таких как Token Ring, также можно воспользоваться преимуществами коммутаторов. В больших сетях после отправки фрейма задержка перед следующим получением маркера может оказаться весьма значительной, поскольку он передается через всю сеть.

Методы передачи данных в локальных сетях

Все пересылки данных в локальных сетях можно разделить на три категории: одноадресатная, многоадресатная и широковещательная передача. В каждом из этих случаев один пакет отправляется одному или нескольким узлам.

При *одноадресатной* передаче *(unicast transmission)* пакет пересылается по сети от источника только одному получателю. Узел-источник адресует пакет, используя адрес узла-получателя. Затем этот пакет посылается в сеть и передается получателю.

При *многоадресатной* передаче *(multicast transmission)* пакет данных копируется и отправляется некоторому подмножеству узлов сети. Узел-источник адресует пакет, используя групповой адрес. Затем пакет посылается в сеть, которая делает с него копии и отправляет по одной копии каждому узлу, соответствующему групповому адресу.

При *широковещательной* передаче *(broadcast transmission)* пакет данных копируется и отправляется всем узлам в сети. При передаче такого типа узел-источник адресует пакет, используя широковещательный адрес. Затем пакет отправляется в сеть, которая делает с него копии и посылает по одной копии каждому узлу сети.

Топологии локальных сетей

Топологии локальных сетей определяют способ организации сетевых устройств. Существует четыре распространенных топологии локальных сетей: шинная, кольцевая, звездообразная и древовидная. Эти топологии представляют собой логические структуры, однако сами устройства не обязательно должны физически образовывать эти конфигурации. Например, логические топологии шины и кольца обычно физически организованы в виде звезды. *Шинная* топология *(bus topology)* представляет собой линейную архитектуру локальной сети, в которой данные, пересылаемые от сетевых станций, распространяются по всей среде передачи и принимаются всеми остальными станциями. Из трех наиболее широко используемых конфигураций локальных сетей в сетях Ethernet/IEEE 802.3, включая 100BaseT, наиболее часто применяется шинная топология. Пример такой топологии показан на рис. 2.3.

Рис. 2.3. Логическая шинная топология

Кольцевая топология *(ring topology)* представляет собой архитектуру локальной сети, при которой группы устройств соединены между собой односторонними каналами передачи таким образом, что образуется одна замкнутая петля. Такая топология

используется в сетях Token Ring/IEEE 802.5 и в сетях FDDI. Пример кольцевой топологии локальной сети приведен на рис. 2.4.

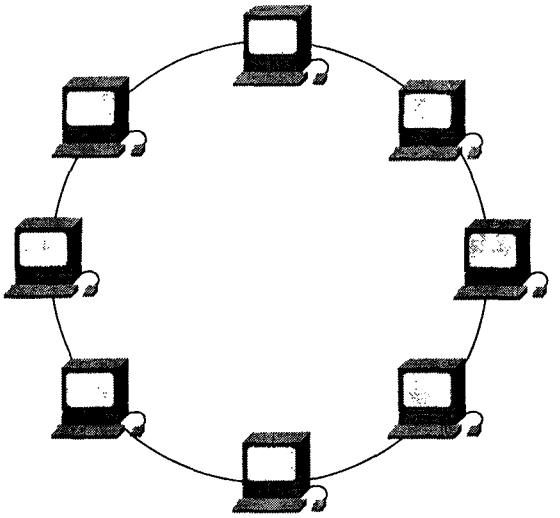


Рис. 2.4. Логическая кольцевая топология

Звездообразная топология *(star topology)* представляет собой архитектуру локальной сети, в которой конечные устройства соединены выделенными линиями с общим центральным концентратором или коммутатором. Логические топологии шины и кольца часто физически организованы в виде звезды, как показано на рис. 2.5.

Древовидная топология *(tree topology)* представляет собой архитектуру локальной сети, аналогичную шинной, но имеющую ветви, к которым подсоединены несколько узлов. Пример древовидной топологии локальной сети приведен на рис. 2.5

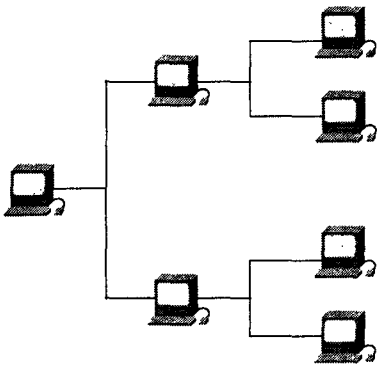


Рис. 2.5. Логическая древовидная топология может состоять из нескольких узлов

Устройства локальных сетей

К числу устройств, обычно используемых в локальных сетях, относятся повторители, концентраторы, расширители локальных сетей, мосты, коммутаторы локальных сетей и маршрутизаторы.

Примечание

В настоящем разделе кратко обсуждаются повторители, концентраторы и расширители локальных сетей. Назначение и функционирование мостов, коммутаторов и маршрутизаторов подробно рассмотрено в главе 4, "Начальные сведения о программном обеспечении IOS Cisco", и в главе 5, "Основы мостовых и коммутируемых соединений"

Повторитель *(repeater)* представляет собой устройство физического уровня, используемое для соединения в объединенной сети нескольких сегментов среды передачи. При использовании повторителя несколько кабельных сегментов могут рассматриваться как один кабель. Повторители принимают сигналы из одного сегмента сети, усиливают их, выполняют ресинхронизацию и передают их в другой сегмент сети. Повторители компенсируют неизбежное ухудшение сигнала, вызываемое большой длиной кабеля и большим количеством подключенных устройств. Повторитель не может выполнять фильтрацию или другую обработку проходящих через него данных. Более того, повторители усиливают и повторяют все электрические сигналы, включая помехи и другие ошибки. Общее количество повторителей и соединяемых ими сегментов сети ограничено из-за возможных нарушений синхронизации и по другим причинам. На рис. 2.6 показан повторитель, соединяющий два сегмента сети.

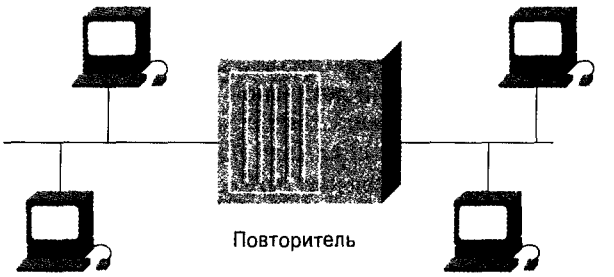


Рис. 2.6. Повторитель соединяет два сегмента сети

Концентратор *(hub)* представляет собой устройство физического уровня, соединяющее несколько пользовательских станций, каждая из которых подключается по отдельному кабелю. Электрические соединения создаются внутри концентратора. Концентраторы используются для создания физической топологии звезды с сохранением шинной или кольцевой логической конфигурации локальной сети. В определенном смысле концентратор является многопортовым повторителем.

Расширитель локальной сети (LAN extender) представляет собой многоуровневый коммутатор удаленного доступа, обеспечивающий соединение с узловым маршрутизатором. Расширители локальной сети перенаправляют потоки данных стандартных сетевых протоколов (например, IP, IPX и AppleTalk) и фильтруют их в соответствии с MAC-адресами или типом сетевого протокола. Эти расширители хорошо масштабируют сеть, поскольку узловой маршрутизатор отфильтровывает нежелательные многоадресатные и

широковещательные и пакеты. Однако расширители локальной сети не могут сегментировать сеть или выполнять функции брандмауэров. На рис. 2.7 показано несколько расширителей, соединенных с маршрутизатором через распределенную сеть.

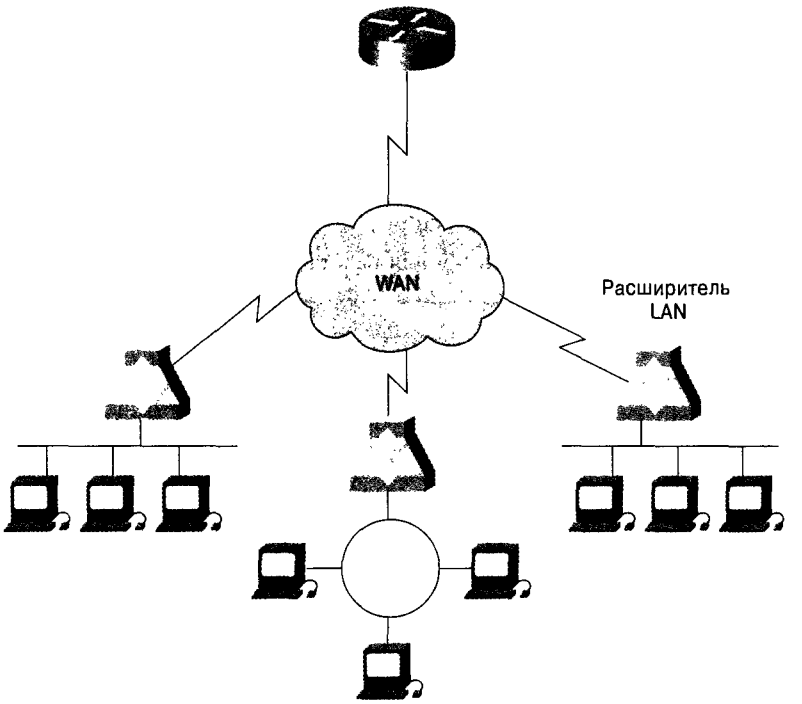


Рис. 2.7. Несколько расширителей локальной сети, подключенных к маршрутизатору через распределенную сеть

Дополнительные источники

Важным источником дополнительной информации по рассмотренным выше темам является Web-сайт корпорации Cisco (www.cisco.com). В разделе документации этого сайта подробно обсуждаются многие вопросы, затронутые в настоящей главе.

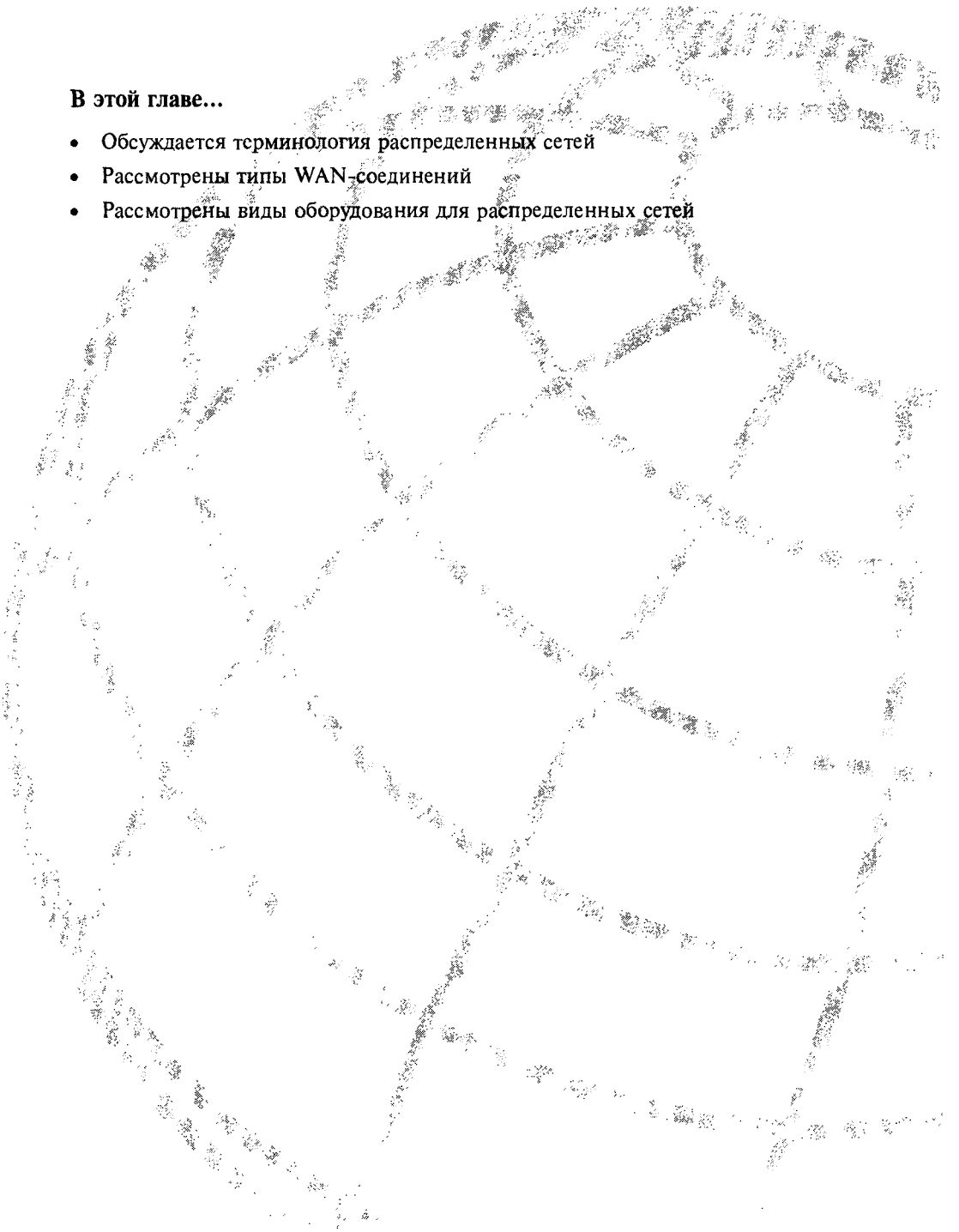
- Teare D. *Designing Cisco Networks*. Cisco Press, 1999.

Контрольные вопросы

1. Опишите способы доступа к среде передачи, используемые в сетях Ethernet.
2. Опишите способы доступа к среде передачи, используемые в сетях Token Ring.
3. Опишите одноадресатную, многоадресатную и широковещательную рассылку данных.

В этой главе...

- Обсуждается терминология распределенных сетей
- Рассмотрены типы WAN-соединений
- Рассмотрены виды оборудования для распределенных сетей



Глава 3

Основные технологии распределенных сетей

В настоящей главе описаны различные протоколы и технологии, используемые в распределенных сетях (Wide-Area Network — WAN). В частности, рассматриваются соединения типа "точка-точка", коммутация каналов, коммутация пакетов, виртуальные каналы, службы доступа по телефонному каналу и устройства, применяемые в распределенных сетях. Подробнее эти технологии описываются в части III "Технологии распределенных сетей

Что такое распределенная сеть?

Распределенная сеть *(Wide-Area Network — WAN)* представляет собой сеть передачи данных, которая охватывает относительно большую географическую область и в которой часто используются носители, предоставляемые общедоступными службами, например, телефонными компаниями. Обычно WAN-технологии функционируют на трех нижних уровнях модели OSI: физическом, канальном и сетевом. Взаимосвязь между типичными технологиями распределенных сетей и моделью OSI показана на рис. 3.1.

Соединения типа "точка-точка"

Соединение типа "точка-точка" обеспечивает отдельный, заранее установленный маршрут передачи данных по распределенной сети от пользователя через несущую сеть, например телефонную, в удаленную сеть. Линии связи "точка-точка" обычно арендуются у компаний, предоставляющих коммуникационные услуги, и поэтому их часто называют арендованными линиями. При использовании соединений типа "точка-точка" поставщик услуг связи выделяет кабельные пары и оборудование только для данной линии. Как правило, размер оплаты за аренду этих каналов зависит от полосы пропускания и расстояния между двумя соединяемыми точками. Обычно соединения типа "точка-точка" обходятся дороже, чем общедоступные службы, такие как Frame Relay. Типичное соединение "точка-точка" в распределенной сети показано на рис. 3.2.

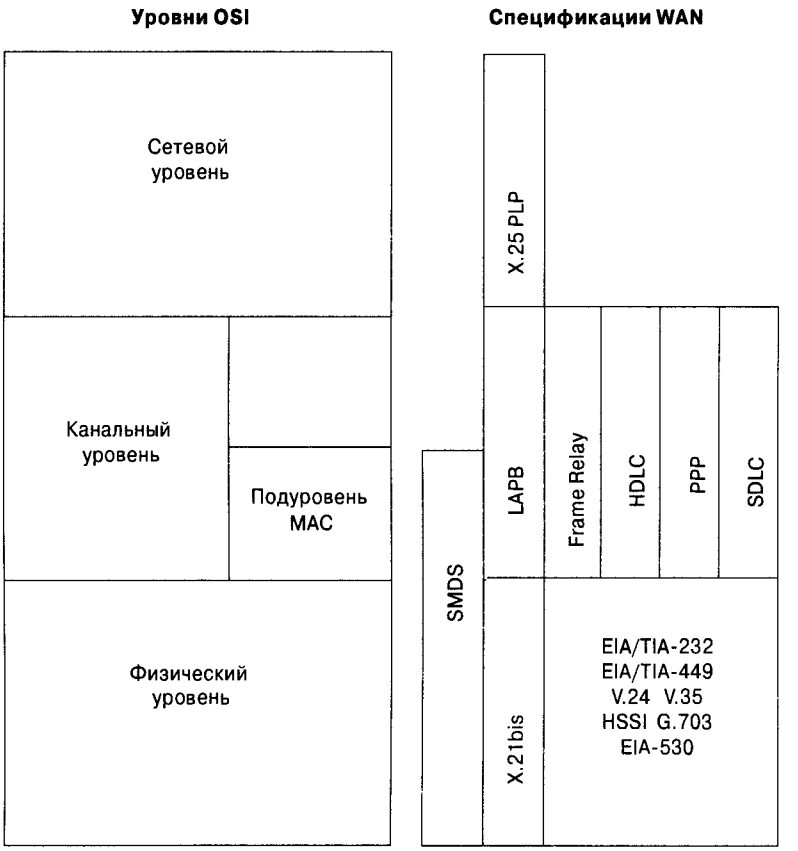


Рис. 3.1. Технологии распределенных сетей работают на трех нижних уровнях модели OSI

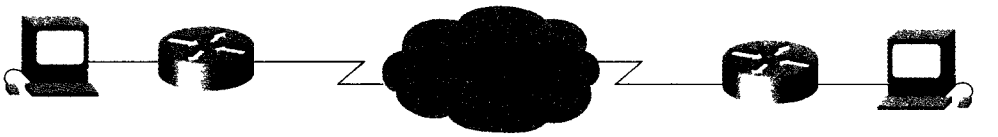


Рис. 3.2. Типичное соединение "точка-точка" передает данные через распределенную сеть WAN в удаленную сеть

Коммутация каналов

Коммутируемые каналы позволяют устанавливать соединения для передачи данных по мере необходимости и ликвидировать их по окончании сеанса связи. Они работают так же, как обычные телефонные линии. Типичным примером сети с коммутацией каналов может служить цифровая сеть интегрированных служб (Integrated Services Digital Network — ISDN). Когда маршрутизатор получает данные, которые необходимо передать удаленному узлу, устанавливается коммутируемое соединение с удаленной сетью, соответствующей указанному номеру

канала. В сети ISDN для вызова удаленной ISDN-сети используется ее телефонный номер. После соединения сетей и аутентификации запрашивающей стороны начинается передача данных, по окончании которой связь можно прервать. Пример линии связи такого типа показан на рис. 3.3.

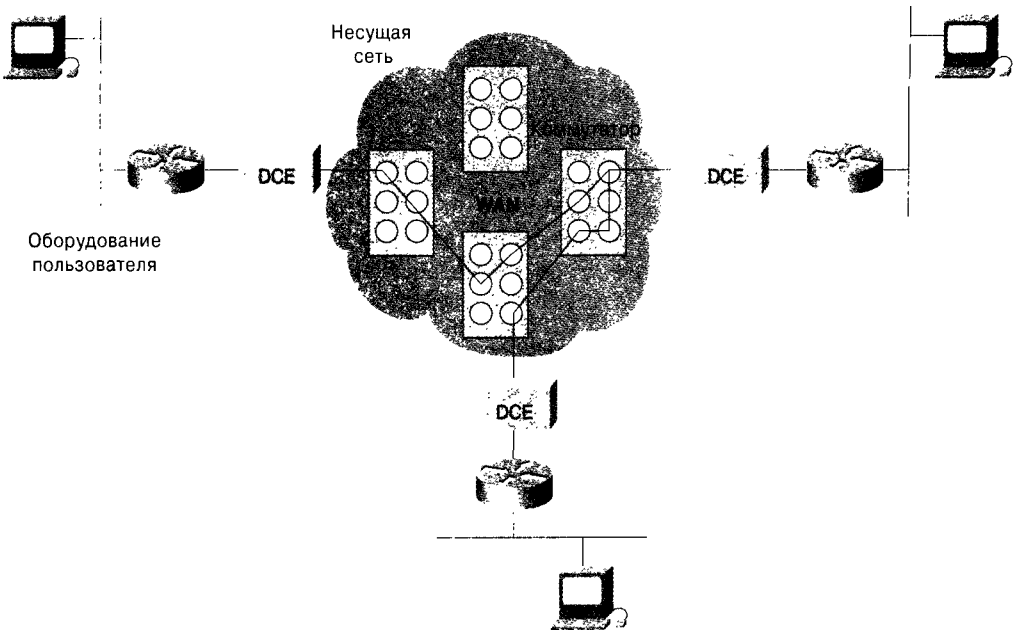


Рис. 3.3. В распределенной сети с коммутацией каналов происходят те же процессы, что и при телефонном звонке

Коммутация пакетов

Коммутация пакетов представляет собой WAN-технологию, в которой несколько пользователей совместно используют общие ресурсы несущей сети. Поскольку в этом случае у провайдера службы появляется возможность более эффективно использовать свою инфраструктуру, расходы пользователя, как правило, становятся существенно меньше, чем при использовании линий связи типа "точка-точка". При использовании коммутации пакетов сеть потребителя подключается к совместно используемой несущей сети. Поставщик услуг связи может создавать между узлами пользователей виртуальные каналы, по которым пакеты данных доставляются через сеть от одного узла к другому. Часть несущей сети, предназначенную для общего использования, часто называют *сетевой средой* или "*облаком*" (cloud).

К сетям с коммутацией пакетов относятся сети асинхронного режима передачи (Asynchronous Transfer Mode — ATM), протокола Frame Relay, сети коммутируемых мультимегабитовых служб данных (Switched Multimegabit Data Services — SMDS) и сети протокола X.25. Пример сети с коммутацией пакетов показан на рис. 3.4.

Виртуальные соединения между узлами пользователей часто называются виртуальными каналами.

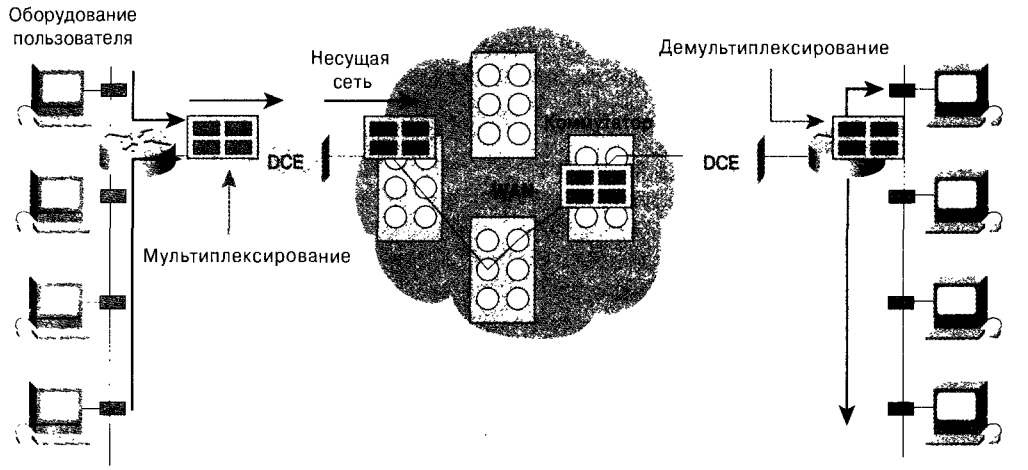


Рис. 3.4. При использовании коммутации пакетов они передаются через несущую сеть от одного узла к другому

Виртуальные каналы в распределенной сети

Виртуальный канал представляет собой логическое соединение, созданное между двумя сетевыми устройствами в общедоступной сети. Существует два вида виртуальных каналов: коммутируемые и постоянные.

Коммутируемые виртуальные каналы (Switched Virtual Circuit — SVC) создаются динамически, по мере необходимости, и ликвидируются после завершения передачи данных. Обмен данными по каналам SVC состоит из трех этапов: создание канала, передача данных и отключение связи. Сначала создается виртуальный канал между устройством-источником и устройством-получателем. По этому виртуальному каналу передаются данные между устройствами, а затем этот виртуальный канал ликвидируется. Каналы SVC используются в тех случаях, когда передача данных между устройствами имеет спорадический (нерегулярный) характер, главным образом потому, что такие каналы интенсивнее используют полосу пропускания за счет создания и ликвидации канала, но они снижают затраты, связанные с постоянным поддержанием доступности виртуального канала.

Постоянные виртуальные каналы (Permanent Virtual Circuit — PVC) существуют постоянно и работают только в одном режиме — режиме передачи данных, и используются в тех случаях, когда передача данных между устройствами имеет постоянный характер. Каналы PVC используют полосу пропускания не так интенсивно, как SVC-каналы, так как не требуют создания и разрыва виртуального канала, однако приводят к увеличению затрат, связанных с постоянным поддержанием доступности виртуального канала. Как правило, PVC-каналы, конфигурируются провайдером службы при поступлении заказа на обслуживание.

Службы удаленного доступа к распределенным сетям

Службы удаленного доступа предоставляют экономичные способы установки соединений через распределенные сети. Наиболее часто применяются две из них — маршрутизация с предоставлением канала по требованию (Dial-on-Demand Routing — DDR) и использование резервного телефонного канала (dial backup).

Служба DDR представляет собой технологию, позволяющую маршрутизатору динамически посылать вызов в коммутируемую сеть в том случае, когда требуется отправить данные. При использовании маршрутизации DDR маршрутизатор настраивается таким образом, чтобы инициировать вызов при определенных условиях, например, при необходимости передать определенный тип данных. После установки соединения данные передаются по линии связи. В конфигурации маршрутизатора указано время ожидания, по истечении которого, если линия не используется, маршрутизатор ликвидирует соединение.

Использование резервного канала *(dial backup)* представляет собой еще один способ конфигурирования маршрутизации по требованию (DDR). Однако в этом случае коммутируемый канал конфигурируется в качестве резервного и используется в случае обрыва соединения другого типа, такого как "точка-точка" или соединения с коммутацией пакетов. Маршрутизатор конфигурируется таким образом, чтобы при обнаружении сбоя основной линии устанавливалось соединение по резервному каналу. Эта линия поддерживает WAN-соединение до тех пор, пока не будет восстановлена основная линия связи, после чего резервное соединение ликвидируется.

Устройства, применяемые в распределенных сетях

В распределенных сетях применяются многочисленные специальные устройства. В последующих разделах обсуждаются такие устройства, как коммутаторы распределенных сетей, серверы доступа, модемы, модули CSU/DSU и адаптеры терминалов ISDN. К числу других устройств, использующихся для обмена данными в средах распределенных сетей WAN, относятся маршрутизаторы, коммутаторы ATM и мультиплексоры.

Коммутатор распределенной сети

Коммутатор распределенной сети представляет собой многопортовое межсетевое устройство, используемое в несущих сетях. Эти устройства обычно коммутируют потоки данных протоколов Frame Relay, X.25 и SMDS и работают на канальном уровне эталонной модели OSI. На рис. 3.5 показаны два маршрутизатора на концах распределенной сети, соединенные через коммутаторы WAN.

Сервер доступа

Сервер доступа является точкой концентрации для входящих и исходящих соединений удаленного доступа. На рис. 3.6 показан сервер доступа, на котором концентрируются исходящие соединения для передачи через распределенную сеть.

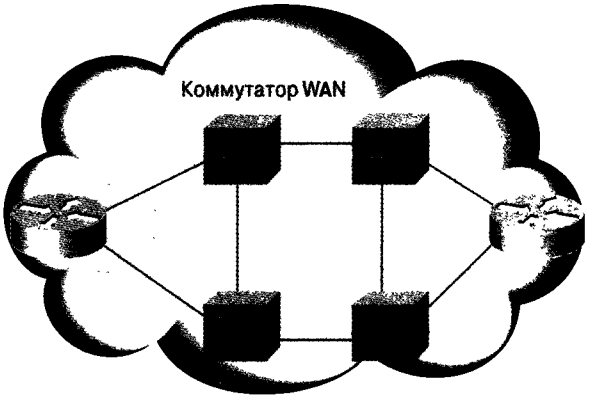


Рис. 3.5. Два маршрутизатора на концах распределенной сети, соединенные через коммутаторы

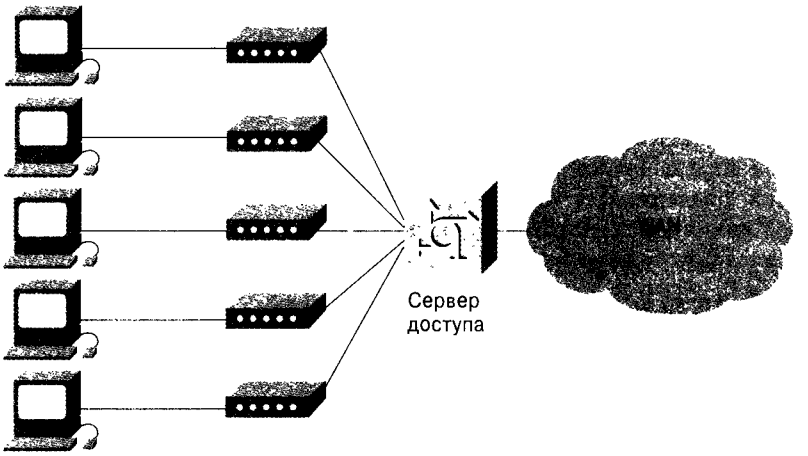


Рис. 3.6. На сервере доступа концентрируются соединения для передачи данных через распределенную сеть

Модем

Модем представляет собой устройство, преобразующее цифровые сигналы в аналоговые и наоборот, что позволяет передавать цифровые данные по телефонным линиям. В устройстве-источнике модем преобразует цифровые сигналы в форму, позволяющую осуществлять передачу данных по аналоговым линиям связи, а модем на устройстве-приемнике вновь преобразует аналоговые сигналы в цифровую форму. Пример соединения "модем-модем" по распределенной сети показан на рис. 3.7.

Модули CSU/DSU

Модули *CSU/DSU* (Channel Service Unit/Digital Service Unit — модуль обслуживания канала/модуль обработки данных) представляет собой устройство цифрового интерфейса, используемое для соединения маршрутизатора с цифровым каналом

(например с каналом T1), а также для синхронизации сигнала. На рис. 3.8 показано расположение устройства CSU/DSU в распределенной сети.

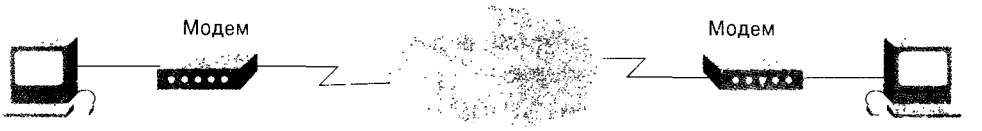


Рис. 3.7. При модемном соединении по распределенной сети происходит преобразование цифровых сигналов в аналоговые и наоборот

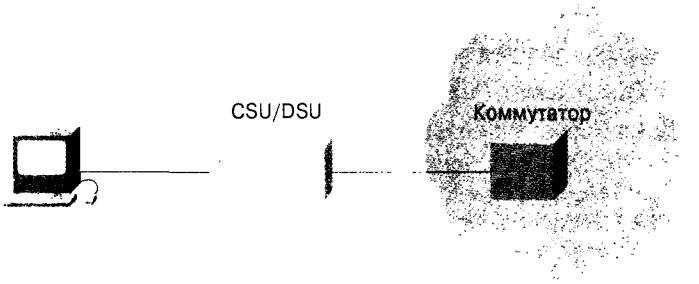


Рис. 3.8. Устройства CSU/DSU устанавливаются между коммутатором и терминалом

Терминальный адаптер сети ISDN

Терминальный адаптер сети ISDN представляет собой устройство, используемое для подсоединения на маршрутизаторе базового интерфейса сети ISDN (ISDN Basic Rate Interface — BRI ISDN) к другому интерфейсу, например, EIA/TIA-232. Хотя это устройство называется терминальным адаптером, в сущности, оно является модемом ISDN, так как на самом деле не преобразует сигналы из аналоговой формы в цифровую. Расположение терминального адаптера в среде ISDN показано на рис. 3.9.

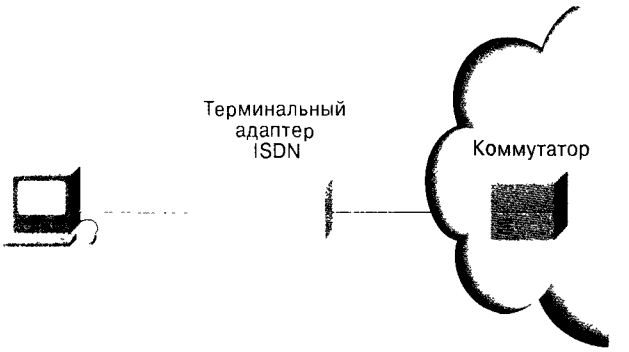


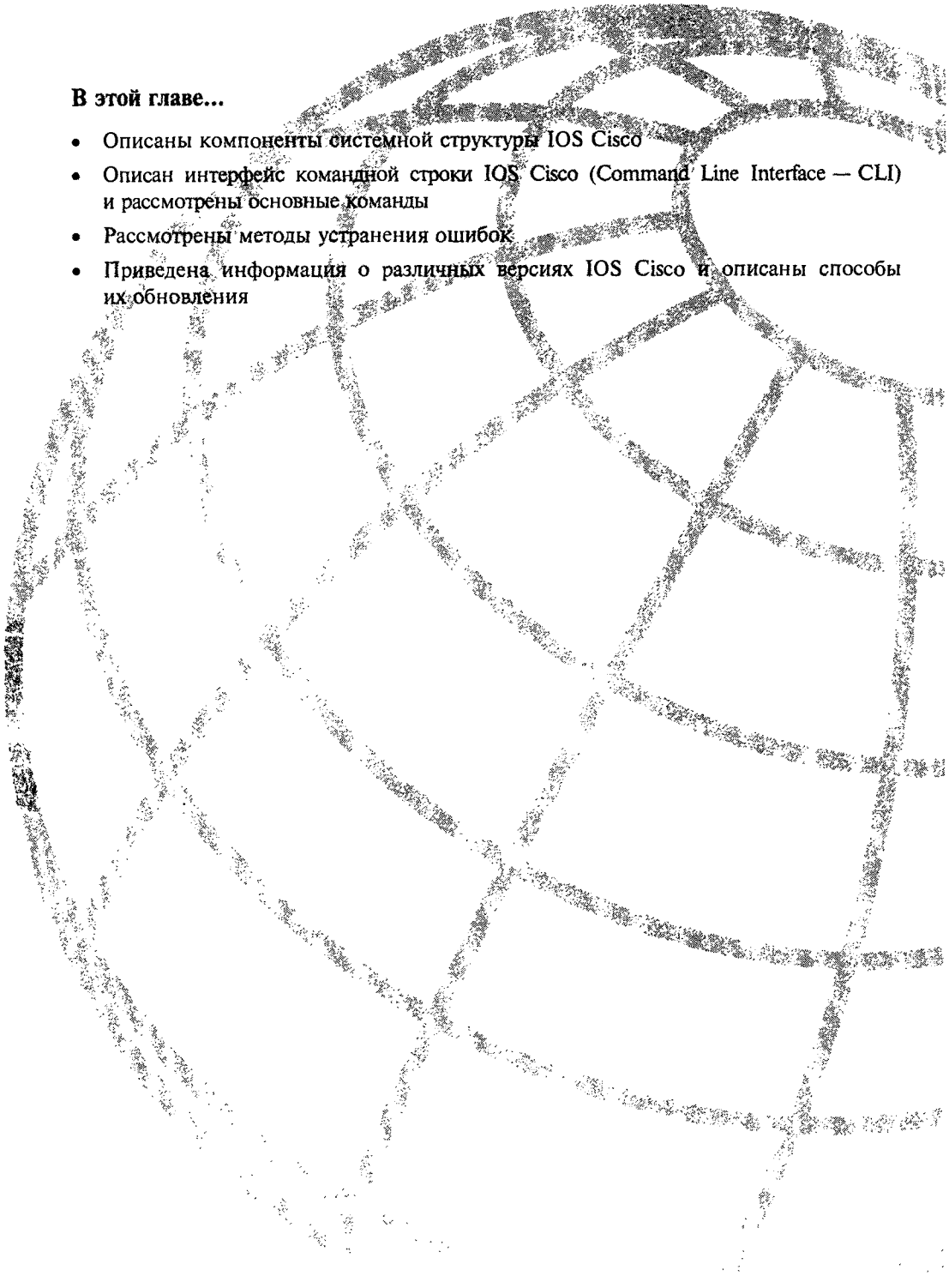
Рис. 3.9. Адаптер терминала обеспечивает соединение с другими интерфейсами

Контрольные вопросы

1. Какие типы каналов используются в распределенных сетях WAN?
2. Что представляет собой маршрутизация по требованию (DDR) и чем она отличается от создания резервного канала?
3. Для чего используется модуль CSU/DSU?
4. В чем состоит различие между модемом и терминальным адаптером ISDN?

Дополнительные источники

- Mahler K. *CCNA Training Guide*. New Riders, 1999.
- *Cisco IOS Dial Solutions*. Cisco Press, 1998.
- *Cisco IOS Wide Area Networking Solutions*. Cisco Press, 1999.



В этой главе...

- Описаны компоненты системной структуры IOS Cisco
- Описан интерфейс командной строки IOS Cisco (Command Line Interface — CLI) и рассмотрены основные команды
- Рассмотрены методы устранения ошибок
- Приведена информация о различных версиях IOS Cisco и описаны способы их обновления

Глава 4

Начальные сведения о программном обеспечении IOS Cisco

Программное обеспечение IOS Cisco применяется в сетях на маршрутизаторах и коммутаторах Cisco. Оно используется для конфигурирования и мониторинга системы, а также для устранения ошибок.

Системная структура

Как и компьютер, маршрутизатор имеет центральный процессор CPU, возможности и производительность которого зависят от используемой платформы маршрутизатора. В качестве примера процессоров, используемых в маршрутизаторах Cisco, можно привести модели Motorola 68030 и Orion/R6400. Программному обеспечению IOS Cisco, установленному на маршрутизаторе, требуется, чтобы CPU или иной процессор принимал решения о маршрутизации и мостовой маршрутизации, поддерживал таблицы маршрутизации и выполнял другие функции управления системой. Для принятия решений и получения инструкций процессор CPU должен иметь доступ к находящимся в памяти данным.

Как правило, маршрутизатор Cisco имеет приведенные ниже четыре типа оперативной памяти.

- **ПЗУ, постоянное запоминающее устройство (Read-only Memory — ROM).** Память ROM обычно представляет собой микросхему или набор микросхем и находится на материнской плате (плате процессора) маршрутизатора. Эта память используется только для чтения; это означает, что запись данных в нее невозможна. В ROM-памяти обычно хранится стартовое программное обеспечение, которое начинает работать при запуске маршрутизатора Cisco и называется *загрузочным программным обеспечением (bootstrap software)*. Оно автоматически вызывается при включении маршрутизатора.
- **Флэш-память (flash memory).** Флэш-память расположена в модуле SIMM на материнской плате, но может быть расширена с использованием устанавливаемых отдельно плат PCMCIA. Флэш-память чаще всего используется для хранения одного или большего количества образов программного обеспечения IOS Cisco. Во флэш-память также могут быть скопированы файлы конфигурации или системная информация. В некоторых современных сис-

темах флэш-память также используется для хранения загрузочного программного обеспечения.

- **Оперативная память RAM (Random Access Memory — RAM).** Оперативная память RAM работает с очень большой скоростью, однако хранящаяся в ней информация утрачивается при перезагрузке системы. В персональных компьютерах RAM-память используется для хранения работающих приложений и данных. В маршрутизаторах память RAM используется для буферов и для хранения системных таблиц IOS. В основном память RAM используется для всех системных операций, требующих сохранения данных.
- **Память NVRAM.** На маршрутизаторах память NVRAM используется для хранения стартовой (начальной) конфигурации. Эта конфигурация представляет собой файл, который считывается при загрузке маршрутизатора. Этот вид памяти обладает исключительно большой скоростью и устойчив к перезагрузкам.

Хотя процессор CPU и память являются обязательными компонентами для работы операционной системы IOS, для пересылки пакетов маршрутизатор должен также иметь различные интерфейсы. Под интерфейсами понимаются входные и выходные соединения маршрутизатора, передающего данные, которые необходимо маршрутизировать или коммутировать. Наиболее типичными являются Ethernet-интерфейсы и последовательные интерфейсы. Аналогично тому, как компьютеру с параллельными и USB-портами требуются соответствующие драйверы, операционной системе IOS Cisco нужны драйверы для поддержки различных типов интерфейсов. Эти драйверы содержатся в самой операционной системе.

Все маршрутизаторы Cisco имеют консольный порт, который обеспечивает асинхронное последовательное соединение EIA/TIA-232. Этот консольный порт может быть подсоединен к последовательному порту компьютера для получения терминального доступа к маршрутизатору. Многие маршрутизаторы также имеют вспомогательный порт, который во многом аналогичен консольному порту, но обычно используется для модемного соединения с целью управления удаленным маршрутизатором.

В примере 4.1 приведен вывод на консоль информации нового маршрутизатора Cisco 3640, который только что был загружен. Следует обратить внимание на приводимую информацию о процессоре, интерфейсах и различных видах памяти.

Пример 4.1. Вывод на консоль начальной информации маршрутизатора Cisco 3640 при загрузке

```
System bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by Cisco Systems, Inc.
C3600 processor with 98304 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

program load complete, entry point: 0x80008000, size: 0xa8d168
Self decompression the image : ########################################
################################################(OK)

                Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Reswtricted Rights clause at FAR sec.
52.227.19 and subparagraph clause(c) (1) (ii) of the Rights in Technical Data
and Computer Software clause at DFARS sec. 252.227 - 7013.
```

```
          Cisco Systems, Inc.
          170 West Tasman Drive
          San Jose, California 95134 - 1706

Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640 - IS - M), Version 12.2(10), RELEASE SOFTWARE
(fc2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
Compiled Mon 06 - May - 02 23:23 by pwade
Image text - base: 0x60008930, data-base: 0x610D2000

cisco 3640 (R4700) processor (revision 0x00) with 94208K/4096K bytes of memory.
Processor board ID 17746964
R4700 CPU at 100 Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0
SuperLAT software (copyright 1990 by Meridian Technology Corp).
5 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)
16384K bytes of processor board PCMCIA Slot0 flash (Read/Write)

...System Configuration Dialog...
Would you like to enter the initial configuration dialog? [yes/no]:
```

При первом запуске нового маршрутизатора операционная система IOS выполняет автоустановку, во время которой пользователю предлагается ответить на несколько вопросов. После этого IOS конфигурирует систему на основе введенных данных. После завершения первоначальной установки изменения в конфигурацию вносятся, как правило, с использованием интерфейса командной строки (Command-Line Interface — CLI). В качестве других способов конфигурирования маршрутизатора используются приложения для управления сетью и протокол HTTP

Интерфейс командной строки IOS Cisco (CLI)

Операционная система IOS Cisco имеет три командных режима, каждый из которых предоставляет пользователю доступ к определенному набору команд.

- **Пользовательский режим**. Это первый режим, к которому пользователь получает доступ после загрузки маршрутизатора. Режим пользователя характеризуется наличием в командной строке символа ">" после имени маршрутизатора. Этот режим предоставляет пользователю доступ только к базовым командам, например отображению статуса (состояния) системы. Конфигурирование или перезагрузка системы в этом режиме невозможны.
- **Привилегированный режим**. Этот режим дает возможность пользователю просмотреть конфигурацию системы, перезагрузить систему и войти в режим конфигурирования. В нем также могут быть выполнены все команды пользовательского режима. Привилегированный режим характеризуется наличием в командной строке символа "#" после имени маршрутизатора. Команда пользовательского режима

enable указывает операционной системе IOS на то, что пользователь желает войти в привилегированный режим. Если ранее был установлен обычный пароль или секретный пароль, то для получения доступа к привилегированному режиму пользователю требуется ввести соответствующий правильный пароль. Если секретный пароль команды **enable** хранится в конфигурации, то для него используется более сложный метод шифрования, и следовательно, достигается более высокий уровень безопасности. Привилегированный режим позволяет пользователю выполнить на маршрутизаторе любые команды, поэтому при его использовании требуется соблюдать осторожность. Для выхода из привилегированного режима используется команда **disable**.

- **Режим конфигурирования.** Этот режим позволяет пользователю изменить текущую конфигурацию системы. Для входа в режим конфигурирования необходимо ввести в привилегированном режиме команду **configure terminal**. Режим конфигурирования имеет несколько подрежимов, первым из которых является режим глобального конфигурирования, который характеризуется наличием в командной строке системной подсказки "(config)#" после имени маршрутизатора. При смене подрежимов режима конфигурирования слова в скобках меняются, указывая на соответствующий подрежим. Например, при входе в подрежим конфигурирования интерфейса подсказка после имени маршрутизатора имеет вид (config-if)#. Для выхода из режима конфигурирования следует ввести команду **end** или нажать клавиши Ctrl+Z.

Следует отметить, что в этих режимах на любом этапе при вводе зависящей от контекста команды ? отображаются все доступные на данном уровне команды. Команда ? также может быть также использована в самой строке команды для отображения возможных вариантов ее завершения. В примере 4.2 показано применение команды ? для отображения команд, доступных в данном командном режиме.

Пример 4.2. Использование контекстно-зависимой справки

```
Router>?
Exec commands:
access-enable       Create a temporary Access-List entry
access-profile      Apply user-profile to interface
clear               Reset functions
...
```

Описанная ниже последовательность действий позволяет познакомиться с командами, используемыми для изменения командного режима, просмотра информации о системе и для задания пароля. Приведенная ниже информация о командах режима CLI получена на маршрутизаторе Cisco 3640, использующем программное обеспечение IOS Cisco.

Этап 1. Для входа в пользовательский режим следует ввести команду **enable** и нажать клавишу **Enter**.

```
Router>enable
Router#
```

Этап 2. Для того чтобы узнать номер используемой версии программного обеспечения, следует ввести команду **show version**.

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3640-IS-M), Version 12.2(10), RELEASE SOFTWARE (fc2)
Copyright (c) 1986-2002 by Cisco Systems, Inc.
Compiled Mon 06-May-02 23:23 by pwade
Image text-base: 0x60008930, data-base: 0x610D2000

ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE
(fc1)

Router uptime is 47 minutes
System returned to ROM by reload
System image file is "slot0:c3640-is-mz.122-10.bin"

cisco 3640 (R4700) processor (revision 0x00) with 94208K/4096K bytes of
memory
Processor board ID 17746964
R4700 CPU at 100 Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT sofware (copyright 1990 by Meridian Technology Corp).
5 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configurations memory.
8192K bytes of processor board System flash (Read/Write)
16384K bytes of processor board PCMCIA Slot0 flash Read/Write)

Configuration register is 0x2002
```

Из текста вывода следует, что используется маршрутизатор Cisco 3640, на котором работает программное обеспечение IOS Cisco версии 12.2(10), а образ программного обеспечения записан на флэш-карте PCMCIA, находящейся в слоте 0.

Этап 3. Далее следует задать маршрутизатору имя, например, "IOS". Для входа в режим конфигурирования используется команда **configure terminal**.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname IOS
IOS(config)#
```

Следует обратить внимание на то, что текст подсказки меняется на "IOS" сразу после ввода команды **hostname**. При использовании программного обеспечения IOS Cisco все изменения конфигурации вступают в действие немедленно.

Этап 4. После этого следует задать пароль и секретный пароль. Секретный пароль хранится с использованием более сложной шифровки и имеет более высокий приоритет, чем обычный пароль, если последний также задан. Для задания этих паролей вводятся следующие команды.

```
IOS(config)# enable password cisco
IOS(config)# enable secret san-fran
IOS(config)# exit
IOS#
```

Для входа в привилегированный режим необходимо ввести пароль **san-fran**. При вводе команды **exit** происходит переход на следующий, более высокий уровень конфигурирования или выход из текущего подрежима.

Этап 5. После задания имени маршрутизатора, ввода пароля и секретного пароля можно просмотреть текущую конфигурацию.

```
IOS(config)# show running-config
Building configuration…

Current configuration :  743 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname IOS
!
enable secret 5 $1$P7a$HClNetI.hpRdox84d.FYU.
enable password cisco
!
ip subnet zero
!
call rsvp-sync
!
interface Ethernet0/0
no ip address
shutdown
half-duplex
!
interface Serial0/0
no ip address
shutdown
no fair-queue
!
interface Ethernet2/0
no ip address
shutdown
half-duplex
!
interface Ethernet2/1
no ip address
shutdown
half-duplex
!
interface Ethernet2/2
no ip address
shutdown
half-duplex
!
interface Ethernet2/3
no ip address
shutdown
half-duplex
!
ip classless
ip http server
ip pim bidir-enable
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
!
end
```

Этап 6. Вывод по команде **show running-config** отображает текущую активную конфигурацию системы; однако эта конфигурация не будет сохранена, если произойдет

перезагрузка системы. Для сохранения этой конфигурации в памяти NVRAM необходимо ввести следующие команды.

```
IOS# copy running-config startup-config
Destination filename [startup-config]?
Building configuration…
[OK]
```

Этап 7. Для просмотра стартовой конфигурации, сохраненной в NVRAM, используется команда **show start-up config**.

В описанной ниже последовательности действий следует обратить внимание на Ethernet-интерфейсы и последовательные интерфейсы, которые отображены в файле конфигурации. Для того чтобы какой-либо интерфейс мог быть использован, необходимо установить его параметры, такие как тип инкапсуляции и адрес. Кроме того, может оказаться необходимым конфигурирование IP-маршрутизации или мостовой маршрутизации. Для получения информации и рекомендаций обо всех возможных опциях конфигурирования следует использовать руководства по установке и конфигурированию IOS Cisco для используемой версии, которые можно найти по адресу www.cisco.com.

В табл. 4.1 описаны некоторые общие команды, используемые для мониторинга системы.

Таблица 4.1. Команды, используемые для мониторинга устройств, на которых установлена операционная система IOS Cisco

Команда IOS Cisco	Описание
show interface	Отображает текущее состояние и подробности конфигурации всех интерфейсов системы
show processes cpu	Отображает использование процессора CPU и текущие процессы, происходящие в системе
show buffers	Отображает текущее распределение (выделение) буферного пространства и функционирование буферов для пересылки пакетов
show memory	Отображает выделение памяти для различных системных функций и ее использование в настоящий момент
show diag	Отображает подробную информацию о работе аппаратных плат системы
show ip route	Выводит текущую активную таблицу IP-маршрутизации
show arp	Отображает текущее активное преобразование IP-адреса в MAC-адрес в таблице ARP

Отладка и загрузка

При необходимости обнаружить и устранить ошибки в системе программное обеспечение IOS Cisco позволяет выполнить пошаговую отладку всех протоколов и происходящих в системе процессов. Более подробную информацию об отладке системы можно найти в "Справочнике по командам IOS Cisco" по адресу www.cisco.com.

Внимание!

Команду **debug** следует использовать только квалифицированным специалистам по программному обеспечению IOS, поскольку некорректное ее выполнение может оказать неблагоприятное воздействие на работу системы. При этом система может оказаться в недоступном, "замороженном" состоянии, в котором пересылка пакетов невозможна.

Системные сообщения отображаются на консоли и эта функция может быть включена для любого сеанса на маршрутизаторе. Для различных методов доступа к маршрутизатору могут быть сконфигурированы различные уровни сообщений о проблемах в сети. Ниже приведены восемь уровней сообщений, используемых для того, чтобы информировать пользователя о состоянии сети.

- **Аварийное состояние (Emergency). Уровень проблемы 0.** Система неработоспособна.
- **Экстренное предупреждение [UA10](Alert). Уровень проблемы 1.** Требуются немедленные действия.
- **Критическое состояние. (Critical). Уровень проблемы 2.** Система находится в критическом состоянии.
- **Ошибка (Error). Уровень проблемы 3.** Состояние ошибки.
- **Предупреждение (Warning). Уровень проблемы 4.** Состояние предупреждения.
- **Уведомление (Notification). Уровень проблемы 5.** Нормальное, но требующее внимания состояние.
- **Информационное сообщение (Informational). Уровень проблемы 6.** Информационное сообщение.
- **Отладка (Debugging). Уровень проблемы 7.** Отладочное сообщение.

Команда **logging** направляет вывод на различные терминалы, подсоединенные к системе физически или виртуально, как терминалы сеансов Telnet. В примере 4.3 показано, как команда **logging** может быть использована для определения уровня проблемы в отображаемых сообщениях

Пример 4.3. Команда logging

```
IOS(config)# logging ?
 Hostname or A.B.C.D   IP address of the logging host
 buffered              Set buffered logging parameters
 console               Set console logging level
 exception             Limit size of exception flush output
 facility              Facility parameter for syslog messages
 history               Configure syslog history table
 host     Set syslog server host name or IP address
monitor               Set terminal line (monitor) logging level
on                    Enable logging to all supported destinations
  rate limit            Set messages per second limit
  source-interface      Specify interface for source address in logging
transactions
  trap                  Set syslog server logging level

IOS(config)# logging console ?
<0-7>          Logging severity level
alerts         Immediate action needed      (severity=1)
critical       Critical conditions          (severity=2)
```

```
debugging      Debugging messages           (severity=7)
emergencies    System is unusable           (severity=0)
errors         Error conditions             (severity=3)
guaranteed     Guarantee console message
informational  Informational messages       (severity=6)
notifications  Normal but significant conditions severity=5)
warnings       Warning conditions           (severity=4)
<cr>
```

При включении высокого уровня сообщений отображаются также и сообщения низших уровней. На уровне отладки (уровень 7) отображаются все сообщения. Системные сообщения могут также быть помещены в буфер для последующего просмотра в привилегированном режиме с помощью команды **show logging**. Пользователь может также направить logging-сообщения на syslog-сервер, используя команду **logging host** в режиме конфигурирования. Для приема этих сообщений от маршрутизатора и размещения их в файле на UNIX-устройстве или на персональном компьютере PC может быть сконфигурирован Syslog-сервер. Это позволяет пользователю поддерживать большие файлы системных сообщений, не будучи при этом ограниченным объемом памяти маршрутизатора.

Перезагрузка и обновление программного обеспечения

Повторный запуск маршрутизатора Cisco называется *перезагрузкой (reload)*. Если по каким-либо причинам требуется перезагрузить маршрутизатор, то необходимо ввести команду **reload** в привилегированном режиме, как показано в примере 4.4. Команда **reload** позволяет также установить время перезагрузки, в результате чего система перезагрузится через заданный промежуток времени.

Пример 4.4. Опции системной перезагрузки

```
IOS# reload ?
LINE        Reason for reload
at          Reload at a specified time/date
cancel      Cancel pending reload
in          Reload after a time interval
<cr>
```

Систему можно также перезагрузить путем выключения и повторного включения питания.

Регистр конфигурации используется для задания поведения маршрутизатора в процессе перезагрузки. Его содержимое определяет, будет ли загружаться образ системы IOS, обеспечиваются ли параметры терминального доступа, а также управляет включением и отключением клавиши Esc. Содержимое регистра конфигурации может быть изменено в режиме конфигурирования с помощью команды **config-register**.

Внимание!

Команду **config-register** следует использовать только в том случае, если ее работа полностью понятна пользователю. Некорректное ее использование может сделать систему недоступной.

По умолчанию маршрутизатор сначала делает попытку, если это возможно, загрузить систему из первого образа своей системной флэш-памяти. После этого, в случае неудачи, он пытается это сделать из флэш-плат PCMCIA. Пользователь может также задать другие образы или источники, из которых можно попытаться перезагрузиться, и порядок их использования с помощью команды **boot system** в режиме конфигурирования.

```
IOS(config)# boot system slot0
```

Выполнение этой команды приведет к тому, что маршрутизатор сначала попытается загрузиться из образа системы, находящегося во флэш-памяти слота 0 PCMCIA, перед тем, как обращаться к своей собственной системной флэш-памяти.

Для обновления используемой на маршрутизаторе версии программного обеспечения IOS Cisco необходимо сначала определить нужный образ, в который оно будет помещено, с помощью планировщиков обновления, которые можно найти по адресу www.cisco.com.

Внимание!

Попытка загрузить для системы некорректный образ может сделать ее недоступной. Перед установкой нового программного обеспечения требуется удостовериться в том, что имеется корректный образ программного обеспечения и удовлетворяются требования к RAM- и флэш-памяти.

Команда **copy** копирует образ системы во флэш-память. Как показано в примере 4.5, это можно сделать многими способами.

Пример 4.5. Различные способы копирования образа операционной системы IOS Cisco во флэш-память

```
IOS# copy ?
/erase          Erase destination file system.
flash:          Copy from flash: file system
ftp:            Copy from ftp: file system
null:           Copy from null: file system
nvram:          Copy from nvram: file system
pram:           Copy from pram: file system
rcp:            Copy from rcp: file system
running-config Copy from current system configuration
Slot0:          Copy from Slot0: file system
Slot1:          Copy from Slot1: file system
startup-config Copy from startup system configuration
system:         Copy from system: file system
tftp:           Copy from tftp: file system
xmodem:         Copy from xmodem: file system
ymodem:         Copy from ymodem: file system
```

Чаще всего применяются такие методы, как использование протоколов TFTP и FTP. После того как файл был помещен на TFTP-сервер или на FTP-сервер, следует ввести в привилегированном режиме команду **copy**, а также ответить на вопросы об IP-адресе сервера и именах файлов отправителя и получателя. После указания образа, который система должна загрузить с помощью команды **boot system**, требуется выполнить команду **reload** для загрузки новой версии IOS Cisco.

Резюме

В настоящей главе описаны основы программного обеспечения IOS Cisco, используемого на маршрутизаторах и коммутаторах Cisco. Это программное обеспечение реализуется центральным процессором CPU и требует наличия нескольких типов памяти для хранения образа, конфигурации, работающих приложений и данных. Использование интерфейса командной строки (CLI) является основным методом, используемым для конфигурирования, мониторинга и устранения ошибок в системе, работающей под управлением IOS Cisco. Это программное обеспечение предоставляет широкие возможности для отладки и ведения журнала выводимой информации. Оно может быть обновлено путем загрузки новой версии с использованием различных опций и последующего выполнения ряда простых операций.

Контрольные вопросы

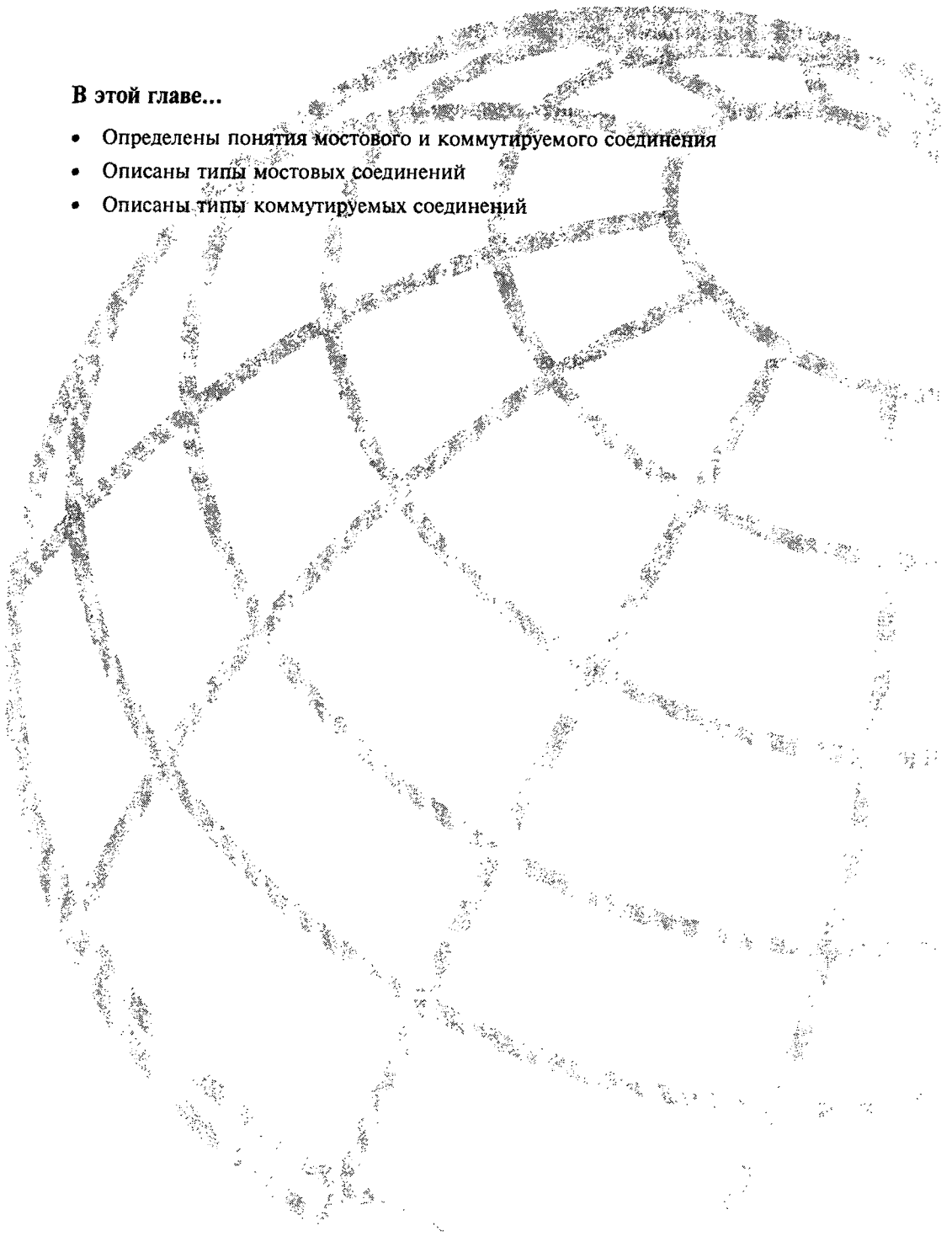
1. Каковы четыре основных типа памяти, используемые маршрутизатором?
2. Каковы три основных командных режима IOS Cisco?
3. Как называется процесс повторного запуска операционной системы IOS Cisco?

Дополнительные источники

- Документация по программному обеспечению IOS Cisco версии 12.2: www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Software:IOS:12.2&s=Documentation.
- *Cisco IOS Configuration Fundamentals*, Cisco Press, 1997, ISBN 0641049129.
- *Cisco IOS in a Nutshell*, O'Reilly & Associates, Inc., 2001, ISBN 156592942X.
- *Inside Cisco IOS Software Architecture*, Pearson Education, 2000, ISBN 1578701813.

В этой главе...

- Определены понятия мостового и коммутируемого соединения
- Описаны типы мостовых соединений
- Описаны типы коммутируемых соединений



Глава 5

Основы мостовых и коммутируемых соединений

В настоящей главе описаны технологии, применяемые в сетях, основу которых составляют устройства, обобщенно называемые мостами и коммутаторами. В ней рассматриваются основные операции устройств канального уровня, использование мостов в локальных сетях и в сетях удаленного доступа, ATM-коммутация и коммутация в локальных сетях. Более подробно эти технологии будут рассмотрены в части V настоящей книги "Мосты и переключатели".

Что такое мосты и коммутаторы?

Мосты и *коммутаторы* представляют собой устройства передачи данных, функционирующие главным образом на 2-м уровне эталонной модели OSI. По этой причине их часто называют устройствами канального уровня.

Мосты стали коммерчески доступными в начале 80-х годов прошлого столетия. В момент своего появления они соединяли однородные сети и позволяли пересылать между ними пакеты данных. Впоследствии область их применения была расширена и появились стандарты, описывающие объединение мостами сетей различных типов.

В объединенных сетях важное значение имеют несколько типов мостовых соединений. В сетях Ethernet в основном применяются *прозрачные мостовые соединения (transparent bridging)*, а в сетях Token Ring — *мостовые соединения с маршрутизацией на источнике (source-route bridging)*. *Трансляционные мостовые соединения (translational bridging)* обеспечивают переход между различными форматами и способами передачи в различных средах (обычно между сетями Ethernet и Token Ring). Наконец, *прозрачные мостовые соединения с маршрутизацией на источнике* (source-route transparent bridging) представляют собой комбинацию алгоритмов прозрачного мостового соединения и мостового соединения с маршрутизацией и позволяют организовать обмен данными в смешанных средах Ethernet/Token Ring.

В настоящее время на смену технологиям объединенных сетей на основе мостов приходят технологии коммутируемых соединений. Там, где раньше устанавливались мосты, сейчас преобладают коммутаторы. Большая пропускная способность, более высокая плотность портов при более низкой стоимости одного порта и большая гибкость способствуют тому, что коммутаторы вытесняют мосты и служат дополнением к технологии маршрутизации.

Обзор устройств канального уровня

Мостовые и коммутируемые соединения относятся к канальному уровню, на котором происходит управление потоками данных, обрабатываются ошибки передачи, обеспечивается физическая адресация (в противоположность логической) и осуществляется доступ к физической среде передачи. Мосты обеспечивают эти функции, используя различные протоколы канального уровня, которые определяют особые алгоритмы управления потоком, обработки ошибок, адресации и доступа к среде передачи. Наиболее часто используются такие протоколы канального уровня, как Ethernet, Token Ring и FDDI.

Мосты и коммутаторы не являются сложными устройствами. Они анализируют входящие фреймы, принимают решения об их пересылке, основываясь на информации, содержащейся в этих фреймах, и направляют их устройству-получателю. В некоторых случаях, например при мостовом соединении с маршрутизацией на источнике, весь маршрут к получателю содержится в каждом фрейме. В других случаях, в частности, при прозрачном мостовом соединении, при пересылке имеется информация лишь об адресе следующего перехода.

Прозрачность протоколов высокого уровня является основным преимуществом как мостовых, так и коммутируемых соединений. Поскольку устройства обоих типов работают на канальном уровне, от них не требуется анализ информации высших уровней. Это означает, что они могут практически мгновенно перенаправлять данные любого протокола сетевого уровня. Нередко по мосту из одной сети в другую передаются данные протоколов AppleTalk, DECnet, TCP/IP, XNS и других.

Мосты могут фильтровать фреймы по любым полям 2-го уровня. Например, мост можно запрограммировать таким образом, чтобы он отбрасывал все фреймы, исходящие из определенной сети. Поскольку в данных канального уровня часто содержатся ссылки на протокол более высокого уровня, мосты обычно могут фильтровать данные и по этому параметру. Кроме того, фильтры могут оказаться полезными для исключения избыточных широковещательных и многоадресатных пакетов.

Разделение большой сети на несколько автономных элементов при помощи мостов и коммутаторов предоставляет много преимуществ. Поскольку пересылается лишь часть потоков данных, использование мостов или коммутаторов уменьшает общий объем данных, получаемых устройствами всех подсоединенных сегментов сети. Мосты и коммутаторы играют роль брандмауэров, которые не пропускают некоторые потенциально опасные сетевые ошибки и обеспечивают обмен данными между большим количеством устройств, чем это возможно в одной подключенной к мосту локальной сети. Мосты и коммутаторы увеличивают фактический размер локальной сети, позволяя подключать к ней удаленные станции, что было бы невозможным без использования мостов и коммутаторов.

Хотя мосты и коммутаторы во многом похожи, между ними есть и ряд отличий. Так, мосты обычно используют для разбиения большой локальной сети на два меньших сегмента, а коммутаторы — на несколько таких сегментов. Мосты имеют, как правило, небольшое количество портов для устройств локальной сети, в то время как коммутаторы обычно обладают большим их количеством. Небольшие коммутаторы, такие как Cisco Catalyst 2924XL, имеют 24 порта, позволяющие создать 24 сегмента локальной сети. Более крупные коммутаторы, такие как Cisco Catalyst 6500, могут иметь сотни портов. Коммутаторы можно также использовать для соединения ло-

кальных сетей, использующих различные среды передачи. Например, с помощью коммутатора можно соединить 10-мегабитовую и 100-мегабитовую локальную сеть Ethernet. Некоторые коммутаторы поддерживают коммутацию без буферизации пакетов, что позволяет уменьшить задержки в сети, в то время как мосты поддерживают только коммутацию фреймов с промежуточным хранением. Наконец, коммутаторы уменьшают вероятность коллизий в сетевых сегментах, так как предоставляют каждому сетевому сегменту отдельную полосу пропускания.

Типы мостов

Можно выделить несколько категорий мостов, в зависимости от их параметров. Согласно одной из распространенных схем классификации, мосты подразделяются на локальные и удаленные. *Локальные мосты* обеспечивают прямое соединение нескольких смежных сегментов локальной сети. *Удаленные мосты* соединяют несколько сегментов локальной сети, расположенных на значительном расстоянии друг от друга, как правило, с использованием линий телекоммуникаций. Эти две конфигурации показаны на рис. 5.1.

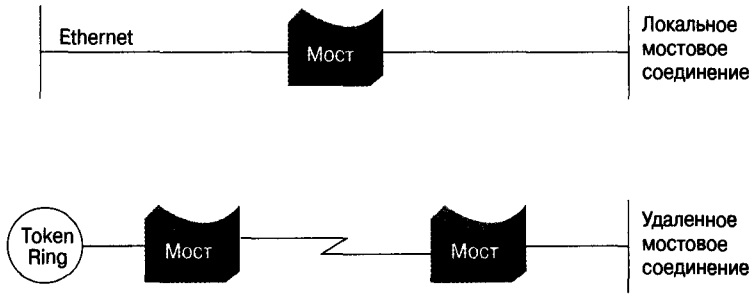


Рис. 5.1. Локальное и удаленное мостовое соединение

Использование удаленных мостовых соединений связано с рядом особых проблем межсетевого взаимодействия, одна из которых — различие скоростей передачи данных в локальной и распределенной сетях. Хотя сейчас в географически распределенных сетевых комплексах применяются некоторые технологии скоростных распределенных сетей, скорость обмена данными в локальных сетях обычно значительно выше, чем в распределенных сетях. Значительная разница в скорости может помешать пользователям работать через распределенную сеть с LAN-приложениями, чувствительными к задержкам.

Удаленные мостовые соединения не могут увеличить скорость передачи данных по распределенной сети, но могут компенсировать разницу в скоростях за счет буферов достаточного объема. Если устройство локальной сети, способное передавать данные со скоростью 3 Мбит/с, обращается к устройству удаленной локальной сети, то локальный мост должен отрегулировать 3-мегабитовый поток данных таким образом, чтобы он не переполнил 64-килобитовую последовательную линию связи. Это делается путем сохранения поступающих данных во встроенных буферах и последующей их отправки по последовательной линии связи с той скоростью, которую она обеспечивает. Однако такая буферизация эффективна только при незначительном избытке данных, не переполняющем буферы моста.

Согласно стандарту института инженеров по электротехнике и электронике (Institute of Electrical and Electronic Engineers — IEEE), канальный уровень модели OSI делится на два подуровня: *подуровень управления доступом к среде передачи MAC (Media Access Control — MAC)* и *подуровень управления логическим каналом (Logical Link Control — LLC)*. Подуровень MAC обеспечивает доступ к среде передачи и управляет им, решая такие задачи, как равноправный доступ различных устройств и передача маркера, а подуровень LLC осуществляет формирование фреймов, управление потоком, контроль ошибок и адресацию подуровня MAC.

Некоторые мосты являются *мостами MAC-уровня* и объединяют однородные сети (например, сети стандарта IEEE 802.3), в то время как мосты другого типа могут передавать данные с преобразованием из одного протокола канального уровня в другой (например, из сети IEEE 802.3 в сеть IEEE 802.5). Базовый механизм такого преобразования показан на рис. 5.2.

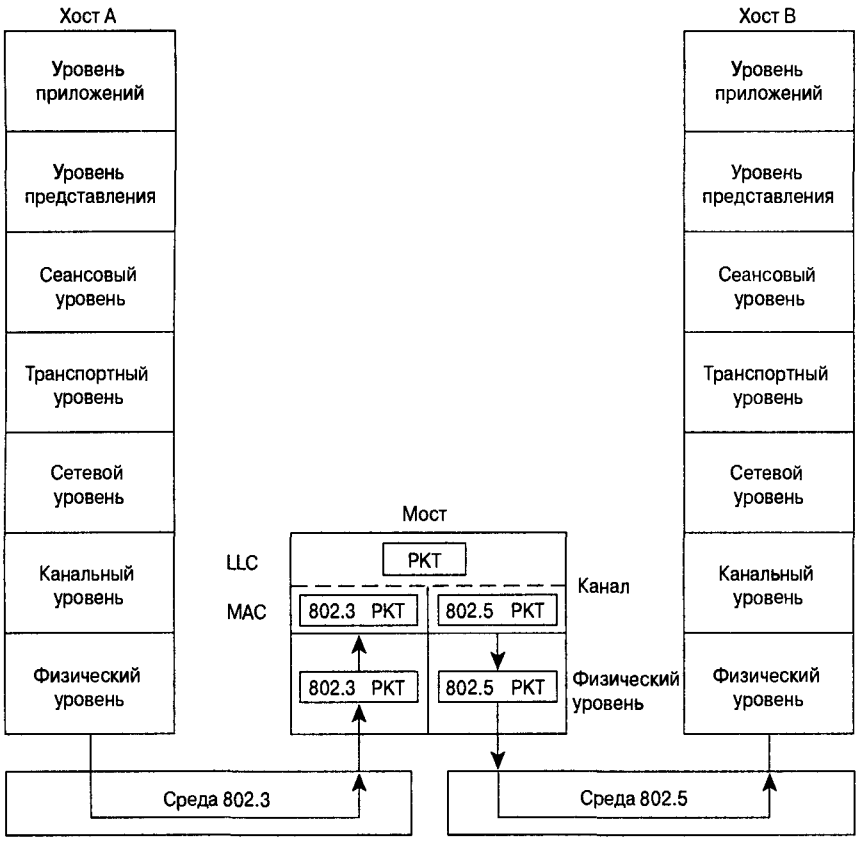


Рис. 5.2. Мост уровня MAC соединяет сети IEEE 802.3 и IEEE 802.5

На рис. 5.2 показан узел сети IEEE 802.3 (узел А), формирующий пакет, который содержит информацию приложения и инкапсулирующий этот пакет во фрейм, соответствующий спецификации IEEE 802.3, для передачи к мосту по сети IEEE 802.3. На мосту, на подуровне MAC канального уровня, из этого фрейма удаляется заголовок формата IEEE 802.3, а затем фрейм передается на подуровень LLC для дальнейшей обработки.

Затем пакет передается на уровень LLC, уже для протокола IEEE 802.5, и инкапсулируется во фрейм спецификации IEEE 802.5 для передачи по сети IEEE 802.5 узлу B.

Преобразование мостом пакетов, передаваемых между сетями различных типов, несовершенно, поскольку возможны случаи, когда одна сеть поддерживает определенные поля фрейма и функции соответствующего протокола, а другая сеть такими функциями не обладает.

Типы коммутаторов

Коммутаторы представляют собой устройства канального уровня, которые, как и мосты, позволяют соединять несколько физических сегментов локальной сети в одну крупную сеть. Подобно мостам, коммутаторы пересылают потоки данных, на основе MAC-адреса. Любое сетевое устройство создает некоторую задержку. В коммутаторах применяются различные приемы перенаправления данных, в частности, промежуточное хранение и коммутация без буферизации пакетов.

При использовании *коммутации с промежуточным хранением (store-and-forward switching)* фрейм не может быть передан дальше, пока не будет полностью получен. Это означает, что задержка при проходе через коммутатор зависит от размера фрейма: чем он больше, тем больше задержка. *Коммутация без буферизации пакетов (cut-through switching)* позволяет коммутатору начать передачу фрейма после получения части фрейма, достаточной для того, чтобы определить, куда его нужно отправить. Это уменьшает задержку при проходе через коммутатор. Промежуточное хранение позволяет коммутатору проверить фрейм на наличие ошибок перед его передачей. Такая возможность отбрасывания фреймов с ошибками является одним из преимуществ коммутаторов перед концентраторами. Коммутация без буферизации пакетов не дает подобного преимущества, и в этом случае коммутатор может пересылать даже фреймы с ошибками. Существует много типов коммутаторов, в том числе коммутаторы ATM, коммутаторы локальных сетей, а также различные типы коммутаторов распределенных сетей.

Коммутаторы ATM

Коммутаторы ATM обеспечивают высокоскоростную коммутацию и масштабируемость полосы пропускания в рабочей группе, в сетевой магистрали предприятия и в распределенной сети. Эти коммутаторы обеспечивают передачу звука, цифровой и видеоинформации. Они предназначены для передачи используемых в сетях ATM единиц информации фиксированного размера, которые называются ячейками. На рис. 5.3 показана корпоративная сеть, состоящая из нескольких локальных сетей, соединенных магистралью ATM.

Коммутаторы локальных сетей

Коммутаторы локальных сетей используются для соединения сегментов локальных сетей. Коммутация локальных сетей обеспечивает взаимодействие сетевых устройств по выделенным каналам без коллизий и с параллельной передачей нескольких потоков данных. Коммутаторы локальных сетей предназначены для коммутации фреймов данных на больших скоростях. На рис. 5.4 показана сеть, в которой коммутатор соединяет 10-мегабитовую и 100-мегабитовую локальные сети Ethernet.

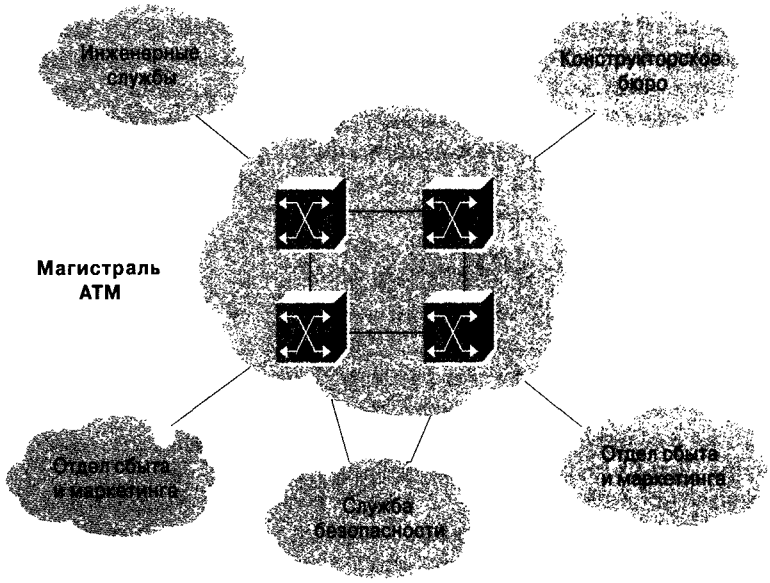


Рис. 5.3. Для объединения локальных сетей можно использовать ATM-магистраль с коммутацией ячеек

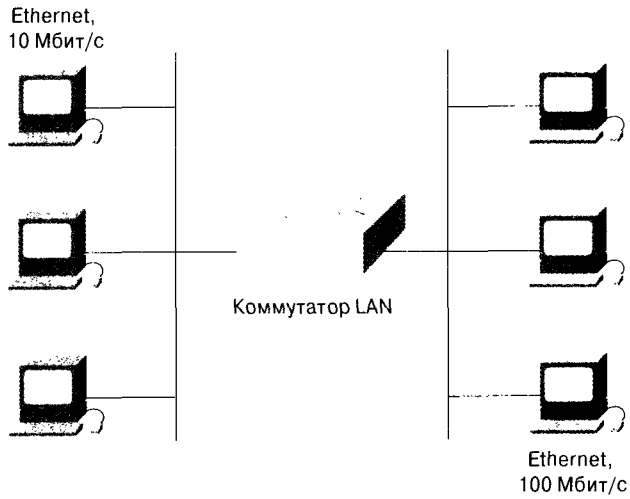


Рис. 5.4. Коммутатор локальных сетей соединяет 10-мегабитовый и 100-мегабитовый сегменты Ethernet

Контрольные вопросы

1. На каком уровне модели OSI работают мосты и коммутаторы?
2. Чем управляет канальный уровень?
3. Какие существуют типы мостов?
4. Что такое коммутатор?

Дополнительные источники

Важным источником дополнительной информации по рассмотренным выше темам является Web-сайт корпорации Cisco (www.cisco.com). В разделе документации этого сайта подробно обсуждаются многие вопросы, затронутые в настоящей главе.

- Kennedy C. and Hamilton K. *Cisco LAN Switching.* Cisco Press, 1999. (Принципы коммутации в локальных сетях Cisco. ИД "Вильямс", 2003.)
- Cisco Systems, Inc. *Cisco IOS Bridging and IBM Network Solutions.* Cisco Press, 1998.

В этой главе...

- Рассмотрены основы протоколов маршрутизации
- Описаны различия между дистанционно-векторными протоколами маршрутизации и протоколами состояния канала связи
- Рассмотрены различные метрики, используемые протоколами маршрутизации для выбора наилучшего маршрута
- Проанализировано перемещение данных от конечных станций через промежуточные до конечной станции-получателя
- Даны определения маршрутизируемых протоколов и протоколов маршрутизации и различия между ними

Глава 6

Основы маршрутизации

В настоящей главе описаны принципы, лежащие в основе большинства протоколов маршрутизации. В ней рассмотрены отдельные компоненты протоколов и используемые алгоритмы маршрутизации. Кроме того, выполнено краткое сравнение роли протоколов маршрутизации и маршрутизируемых, или сетевых, протоколов. Протоколы маршрутизации будут более подробно рассмотрены в части VII "Протоколы маршрутизации", а сетевые протоколы, использующие протоколы маршрутизации, — в части VI "Сетевые протоколы".

Что такое маршрутизация?

Маршрутизация *(routing)* представляет собой перемещение информации по объединенной сети от источника к получателю. На этом маршруте обычно встречается как минимум один промежуточный узел. Маршрутизация часто противопоставляется соединению сетей мостами, которое, на первый взгляд, выполняет те же функции. Основное отличие между ними состоит в том, что мостовое соединение работает на 2-м (канальном) уровне эталонной модели OSI, а маршрутизация — на 3-м (сетевом) уровне. Из этого следует, что в процессе перемещения данных от источника к получателю маршрутизаторы и мосты используют разную информацию и, таким образом, выполняют свою задачу разными способами.

Тема маршрутизации не сходит со страниц книг о компьютерах уже более двух десятилетий, однако коммерческое распространение маршрутизация получила только в середине 80-х годов XX века. Основная причина такого запоздания состояла в том, что сети 70-х годов были простыми, однородными средами. Крупные объединенные сети стали широко распространенными лишь сравнительно недавно.

Компоненты маршрутизации

При осуществлении маршрутизации выполняются два основных действия: определение оптимальных маршрутов и транспортировка информационных групп (обычно называемых пакетами) по объединенной сети. В терминах маршрутизации последняя операция называется коммутацией пакетов. Коммутация пакетов является относительно простым действием, однако определение оптимального маршрута может оказаться весьма сложной задачей.

Определение маршрута

Для того чтобы определить, какой из маршрутов является лучшим для передачи пакета, протоколы маршрутизации используют метрики. *Метрика* представляет собой числовую характеристику маршрута, такую, например, как полоса пропускания канала, и используется алгоритмами маршрутизации для определения оптимального пути к получателю данных. Для упрощения процесса определения маршрута алгоритмы маршрутизации создают и регулярно обновляют таблицы маршрутизации, в которых содержится информация о маршрутах. Информация о маршрутах меняется в зависимости от используемого алгоритма маршрутизации.

Алгоритмы маршрутизации заполняют таблицы маршрутизации различной информацией. Пары "получатель/следующий переход" сообщают маршрутизатору о том, что для оптимальной передачи пакета требуемому получателю его следует отправить маршрутизатору, представляющему собой "следующий пункт пересылки". Когда на вход маршрутизатора поступает пакет, маршрутизатор пытается найти связь между содержащимся в нем адресом получателя и следующим пунктом передачи. Пример таблиц маршрутизации, содержащих пары адресов "получатель/следующий переход" приведен на рис. 6.1.

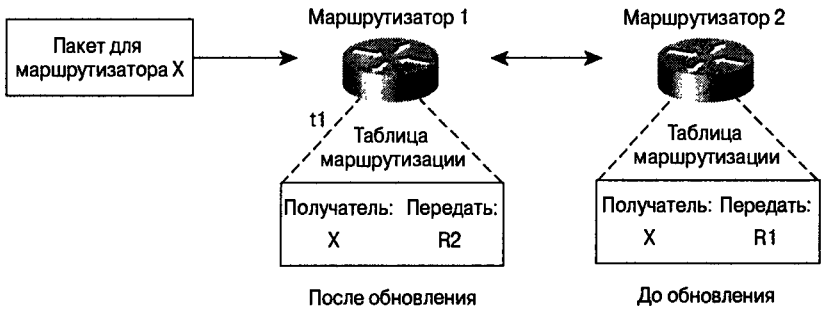


Рис. 6.1. Оптимальный маршрут прохождения данных определяется списком пар адресов "получатель/следующий переход"

Таблицы маршрутизации могут содержать и другую информацию, например данные о более предпочтительном маршруте. Для определения оптимальных маршрутов маршрутизаторы сравнивают их метрики, которые могут быть различными, в зависимости от используемого алгоритма маршрутизации. Некоторые широко применяемые метрики будут описаны ниже в данной главе.

Маршрутизаторы взаимодействуют между собой и поддерживают таблицы маршрутизации, обмениваясь различными сообщениями. Одним из таких сообщений является сообщение об обновлении маршрутов, в котором обычно содержится вся таблица маршрутизации или ее часть. Анализируя данные об обновлении маршрутов, поступающие от других маршрутизаторов, маршрутизатор получает подробное представление о топологии сети. Другим примером сообщения, передаваемого между маршрутизаторами, является сообщение о состоянии канала, которое информирует другие маршрутизаторы о состоянии каналов отправителя. Информация о состоянии каналов связи также может быть использована для составления полной картины топологии сети, позволяющей маршрутизаторам определять оптимальные маршруты к устройствам-получателям.

Коммутация

Алгоритмы коммутации относительно просты и одинаковы для большинства протоколов маршрутизации. Как правило, получив пакет, узел определяет, что он должен отправить пакет другому узлу. Выяснив каким-либо образом адрес маршрутизатора, узел-источник посылает пакет, непосредственно по физическому адресу маршрутизатора (по MAC-адресу), однако пакет при этом также содержит протокольный адрес (сетевого уровня) узла-получателя.

Проанализировав сетевой адрес получателя пакета, маршрутизатор определяет, известен ли путь, по которому можно передать пакет на следующий переход. Если такой путь маршрутизатору неизвестен, то он обычно отбрасывает пакет. Если же путь известен, то маршрутизатор заменяет физический адрес получателя на соответствующий адрес следующего перехода и пересылает пакет в этом направлении.

Следующим переходом, если это не узел-получатель, обычно является другой маршрутизатор, который выполняет те же действия по выбору направления коммутации. Пакет, проходя по объединенной сети, изменяет свой физический адрес, но его протокольный адрес остается неизменным, как показано на рис. 6.2.

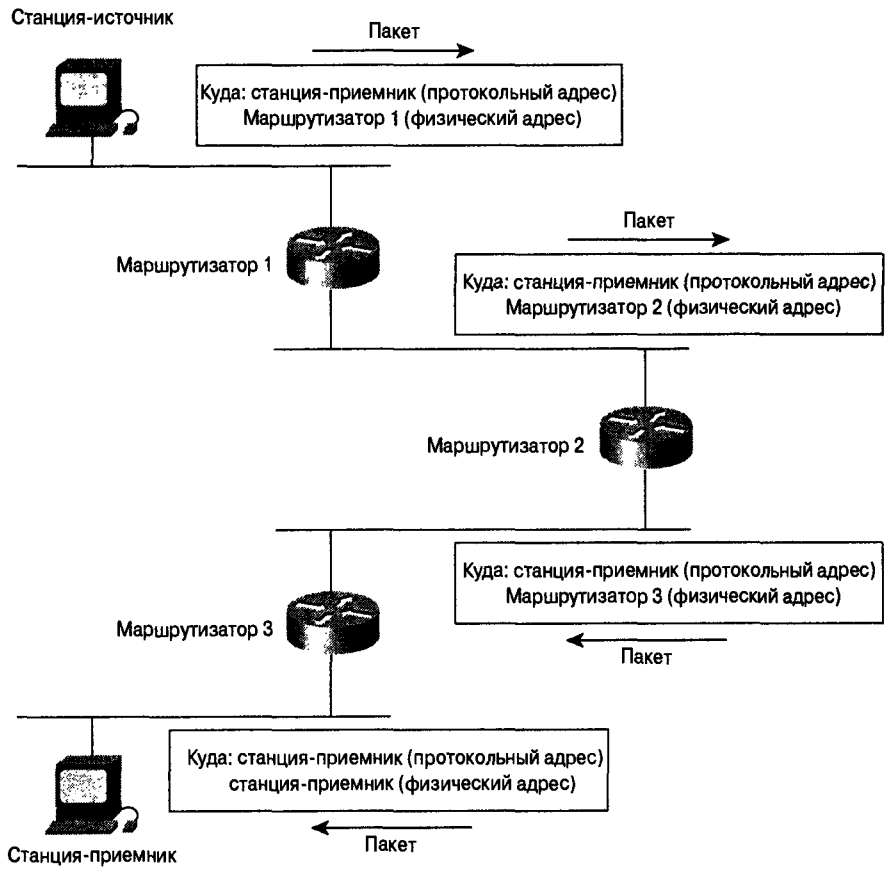


Рис. 6.2. В коммутации могут участвовать несколько маршрутизаторов

Выше описана процедура коммутации между двумя конечными системами — источником и получателем. Международная организация по стандартизации (International Organization for Standardization — ISO) разработала иерархическую терминологию, которая удобна для описания такого процесса. Согласно этой терминологии, сетевые устройства, которые не могут пересылать пакеты между подсетями, называются *конечными системами (End System — ES)*, а сетевые устройства, обладающие такой способностью, — *промежуточными системами (Intermediate System — IS)*. Промежуточные системы, в свою очередь, делятся на *внутридоменные*, которые могут обмениваться данными только с устройствами, находящимися внутри доменов маршрутизации, и *междоменные*, которые могут передавать данные как внутри доменов маршрутизации, так и между ними. *Доменом маршрутизации* обычно называют часть объединенной сети с единым администрированием и управляемую определенным набором административных правил. Домены маршрутизации также называют автономными системами. При помощи некоторых протоколов домены маршрутизации можно разбить на зоны маршрутизации, но для коммутации как внутри таких зон, так и между ними применяются внутридоменные протоколы маршрутизации.

Алгоритмы маршрутизации

Алгоритмы маршрутизации различаются по нескольким ключевым характеристикам. Во-первых, на работу протокола маршрутизации влияют цели, которые ставились разработчиком алгоритма. Во-вторых, различные виды алгоритмов по-разному используют ресурсы сети и маршрутизаторов. Наконец, алгоритмы маршрутизации применяют различные метрики, влияющие на выбор оптимальных маршрутов. Эти свойства алгоритмов маршрутизации будут проанализированы в следующих разделах.

Цели, которые ставятся при разработке алгоритмов маршрутизации

При разработке алгоритмов маршрутизации обычно ставится одна или несколько из следующих целей:

- оптимальность;
- простота и минимальный объем передаваемой служебной информации;
- надежность и устойчивость алгоритма;
- быстрая сходимость;
- гибкость.

Под *оптимальностью алгоритма маршрутизации* понимается его способность выбрать лучший маршрут, что зависит от используемой при вычислениях метрики и удельного веса отдельных параметров. Например, алгоритм маршрутизации может использовать в качестве варьируемых параметров количество пройденных узлов и величины задержек, но при вычислениях придавать задержкам более высокий удельный вес. Естественно, в протоколе маршрутизации должен быть строго определен алгоритм вычисления метрики.

Кроме того, алгоритмы маршрутизации стараются сделать как можно более простыми. Иными словами, алгоритм маршрутизации должен эффективно выполнять

свои функции с минимальными затратами на передачу служебной информации — как программными, так и аппаратными. Эффективность алгоритма особенно важна в том случае, когда реализующее его программное обеспечение работает на компьютере с ограниченными физическими ресурсами.

Алгоритмы маршрутизации должны быть *надежными*, т.е. они должны безошибочно работать в необычных или непредвиденных условиях, таких как аппаратные сбои, высокая нагрузка и неправильная установка. Поскольку маршрутизаторы располагаются в узловых точках сети, сбой в их работе может привести к серьезным проблемам. Зачастую лучшими оказываются те алгоритмы маршрутизации, которые выдержали проверку временем и подтвердили свою стабильность в различных условиях работы сети.

Кроме того, алгоритмы маршрутизации должны быстро сходиться. Под *сходимостью* понимается процесс согласования оптимальных маршрутов всеми маршрутизаторами. Когда в сети происходит такое событие, как выход из строя маршрутизатора или, наоборот, начало или возобновление его работы, другие маршрутизаторы распространяют по всем сетям сообщения об обновлении маршрутов, вследствие чего происходит повторное вычисление оптимальных маршрутов и согласование их между всеми маршрутизаторами. Если алгоритм маршрутизации медленно сходится, то это может привести к появлению петель маршрутизации или к недоступности части сети.

Формирование петли маршрутизации проиллюстрировано на рис. 6.3. Пакет поступает на маршрутизатор Router 1 в момент времени t1. Этот маршрутизатор уже получил сообщение об обновлении маршрута, и следовательно, ему известно, что следующим переходом на оптимальном маршруте к получателю является маршрутизатор Router 2, поэтому Router 1 пересылает пакет на маршрутизатор Router 2. Однако Router 2 еще не получил сообщение об обновлении маршрута, и, по его данным, следующим переходом на оптимальном маршруте к получателю является маршрутизатор Router 1. Соответственно, Router 2 пересылает пакет обратно на маршрутизатор Router 1. В результате пакет будет перемешаться между этими двумя маршрутизаторами, пока на маршрутизаторе Router 2 не будут обновлены маршруты или не будет превышено максимально допустимое количество переходов.

Чтобы пакет дошел до сети:	Его нужно отправить на:
27	Узел A
57	Узел B
17	Узел C
24	Узел A
52	Узел A
16	Узел B
26	Узел A
. . .	. . .

Рис. 6.3. Медленная сходимость и петли маршрутизации препятствуют прохождению пакетов

Алгоритмы маршрутизации также должны быть гибкими, т.е. быстро и точно адаптироваться к различным сетевым условиям. Например, предположим, что один из сетевых сегментов вышел из строя. Такая проблема учитывается во многих алгоритмах маршрутизации. В такой ситуации необходимо быстро выбрать для всех маршрутов, обычно проходящих через этот сегмент, оптимальный обходной путь. Алгоритм маршрутизации должен по возможности адаптироваться к изменениям полосы пропускания, длины очереди на маршрутизаторе и сетевым задержкам, а также к другим параметрам.

Типы алгоритмов маршрутизации

Алгоритмы маршрутизации можно классифицировать по следующим критериям:

- статическая или динамическая маршрутизация;
- наличие одного или нескольких маршрутов к одному получателю;
- линейная или иерархическая маршрутизация;
- выполнение алгоритма на исходном узле или на промежуточных маршрутизаторах;
- внутридоменная или междоменная маршрутизация;
- маршрутизация по состоянию канала или дистанционно-векторная маршрутизация.

Статическая и динамическая маршрутизация

Алгоритмы статической маршрутизации представляют собой не столько алгоритмы, сколько таблицы, составленные сетевым администратором прежде чем включить маршрутизаторы. Содержимое этих таблиц может быть изменено только сетевым администратором. Алгоритмы, использующие статические маршруты, просты и эффективно работают в сравнительно простых сетях с относительно предсказуемым характером передачи данных.

Поскольку системы статической маршрутизации не реагируют на изменения в сети, они, как правило, не подходят для современных крупных, постоянно изменяющихся сетей. Большинство используемых в настоящее время алгоритмов являются *алгоритмами динамической маршрутизации*, которые адаптируются к изменениям сетевой обстановки, анализируя поступающие сообщения об обновлении маршрутов. Если в сообщении указывается на изменения в сети, то программное обеспечение маршрутизации заново вычисляет маршруты и рассылает новые сообщения об обновлении маршрутов. Эти сообщения распространяются по сети, заставляя маршрутизаторы заново запускать алгоритмы маршрутизации и вносить соответствующие изменения в таблицы.

Иногда алгоритмы динамической маршрутизации целесообразно дополнить статическими маршрутами. Например, конечный маршрутизатор (т.е. тот, на который попадают все не поддающиеся маршрутизации пакеты) может служить хранилищем всех таких пакетов. Это гарантирует, что все сообщения будут так или иначе обработаны.

Единственный маршрут или несколько маршрутов

Некоторые сложные протоколы маршрутизации допускают существование нескольких маршрутов к одному получателю. В отличие от алгоритмов, вычисляющих только один маршрут, эти протоколы позволяют распределить потоки данных по нескольким каналам. Преимущества таких алгоритмов очевидны: они значительно ускоряют передачу данных и повышают ее надежность. Такую технологию обычно называют распределением нагрузки (load sharing).

Линейная и иерархическая маршрутизация

Одни алгоритмы маршрутизации работают в линейном пространстве, а другие строят иерархии маршрутов. В системах с *линейной* маршрутизацией *(flat routing)* все маршрутизаторы равноправны. В системах с иерархической маршрутизацией некоторые маршрутизаторы образуют аналог маршрутной магистрали. Пакеты поступают от периферийных маршрутизаторов на магистральные маршрутизаторы и передаются по магистрали, пока не достигнут зоны, где расположен получатель. Затем они с последнего магистрального маршрутизатора передаются получателю через один или несколько периферийных маршрутизаторов.

В системах маршрутизации часто создаются логические группы узлов, называемые доменами, автономными системами или зонами. В системах с *иерархической маршрутизацией* одни маршрутизаторы домена могут обмениваться данными с маршрутизаторами других доменов, а другие — только с маршрутизаторами своего домена. В очень крупных сетях иногда создаются дополнительные уровни иерархии, и тогда маршрутная магистраль образуется маршрутизаторами высшего уровня.

Основное преимущество иерархической маршрутизации состоит в том, что она повторяет структуру большинства компаний и поэтому соответствует структуре передачи их данных. Наиболее интенсивный обмен данными происходит внутри малых групп (доменов). Поскольку внутридоменным маршрутизаторам требуется информация только о маршрутизаторах, принадлежащих к их домену, их алгоритмы маршрутизации можно упростить и, соответственно, сократить количество сообщений об обновлении маршрутов.

Алгоритмы, выполняемые на узлах-источниках и на маршрутизаторах

В некоторых алгоритмах маршрутизации весь маршрут определяется узлом-источником. Обычно такой подход называется *маршрутизацией на источнике (source routing)*. В системах с маршрутизацией на источнике маршрутизаторы выполняют только функции запоминания адресов и пересылки пакетов следующему узлу.

В других алгоритмах предполагается, что узлам-источникам маршруты передачи данных неизвестны. В этих алгоритмах путь следования по объединенной сети определяется маршрутизаторами, на которых выполняется вычисление маршрута. В первой из рассмотренных выше систем узел-источник должен быть способен определять маршрут, во второй системе эти функции выполняются промежуточными маршрутизаторами.

Внутридоменная и междоменная маршрутизация

Одни алгоритмы маршрутизации работают только внутри доменов, другие — как внутри доменов, так и между ними. Природа этих двух типов алгоритмов различна, поэтому оптимальный алгоритм внутридоменной маршрутизации не всегда является оптимальным для междоменной маршрутизации.

Алгоритмы маршрутизации по состоянию канала и дистанционно-векторные алгоритмы

Алгоритмы маршрутизации *по состоянию* канала *(link-state)*, которые также называют алгоритмами определения кратчайшего маршрута, распространяют информацию о маршрутах по всем узлам объединенной сети. Однако каждый маршрутизатор посылает

только ту часть таблицы маршрутизации, которая описывает состояние его собственных каналов. В таких алгоритмах в таблице маршрутизации каждого маршрутизатора составляется картина всей сети. Дистанционно-векторные алгоритмы маршрутизации (также называемые алгоритмами Беллмана-Форда) тоже требуют от каждого маршрутизатора отправки всей таблицы маршрутизации или ее части, но только своим соседям. В сущности, алгоритмы маршрутизации по состоянию канала рассылают небольшие обновления всем остальным маршрутизаторам, а дистанционно-векторные алгоритмы отправляют больше информации, но только соседним маршрутизаторам. При использовании дистанционно-векторных алгоритмов (distance vector algorithm) маршрутизатор имеет информацию лишь о своих соседях.

Поскольку алгоритмы маршрутизации по состоянию канала сходятся быстрее, вероятность образования петель маршрутизации при их использовании несколько меньше, чем при использовании дистанционно-векторных протоколов. С другой стороны, алгоритмы маршрутизации по состоянию канала требуют большей мощности процессора и больше памяти. Поэтому алгоритмы маршрутизации по состоянию канала могут оказаться более дорогостоящими при реализации и поддержке. Протоколы маршрутизации по состоянию канала обычно более масштабируемы, чем дистанционно-векторные протоколы.

Метрики маршрутов

В таблицах маршрутизации содержится информация, используемая коммутирующим программным обеспечением для выбора наилучшего маршрута. Но как именно строятся эти таблицы? Какова природа содержащейся в них информации? Как алгоритмы маршрутизации определяют, что один маршрут предпочтительнее других?

Для определения оптимального маршрута алгоритмы маршрутизации используют множество различных метрик. В сложных алгоритмах маршрутизации выбор маршрута осуществляется по нескольким метрикам, образующим составную (гибридную) метрику. Для определения наилучшего маршрута используются следующие метрики:

- длина маршрута;
- надежность;
- задержка;
- полоса пропускания;
- нагрузка;
- затраты на передачу.

Длина маршрута представляет собой наиболее часто используемую метрику маршрутизации. Некоторые протоколы маршрутизации позволяют сетевому администратору произвольным образом назначать каждому каналу значение, отражающее затраты на передачу. В этом случае длина маршрута представляет собой сумму затрат на всех пройденных участках. Другие протоколы маршрутизации вычисляют количество пройденных узлов — метрику, которая определяет, какое количество переходов между сетевыми устройствами, такими как маршрутизаторы, должен пройти пакет на пути от источника к получателю.

В контексте маршрутизации *надежность* алгоритма маршрутизации определяется надежностью канала связи (обычно выражаемой отношением количества переданных битов к количеству ошибок). В некоторых каналах сбои могут происходить чаще, чем в других. После сбоя одни каналы восстанавливаются быстрее и проще, другие — медленнее. При

назначении рейтингов надежности могут быть учтены любые относящиеся к этому факторы. Такие рейтинги представляют собой числовые оценки, обычно назначаемые линиям связи сетевыми администраторами.

Задержка при маршрутизации представляет собой время, требуемое для доставки пакета по сети от источника к получателю. Величина задержки зависит от многих факторов, таких как полоса пропускания промежуточных линий связи, длина очереди на порту каждого маршрутизатора, переполнения на промежуточных линиях связи, а также физическое расстояние, которое необходимо пройти. Поскольку задержка является комбинацией нескольких важных параметров, эта метрика получила широкое распространение.

Полоса пропускания характеризует пропускную способность канала. При прочих равных условиях 10-мегабитовый канал Ethernet предпочтительнее, чем выделенная линия с полосой пропускания 64 Кбит/с. Хотя полоса пропускания характеризует максимальную пропускную способность канала, маршруты, проходящие по каналам с большей полосой пропускания, не всегда оказываются лучше маршрутов, проходящих по более медленным линиям. Например, если быстрый канал загружен больше, то для передачи по нему пакета получателю может потребоваться больше времени, чем при использовании более медленного, но менее загруженного канала.

Нагрузка характеризует степень занятости сетевого ресурса, например маршрутизатора. Используются различные способы определения нагрузки, в том числе по интенсивности использования процессора и по количеству обрабатываемых в секунду пакетов. Однако сам по себе мониторинг этих параметров может поглощать значительные ресурсы.

Еще одной важной метрикой являются *затраты на передачу данных*, особенно потому, что некоторые компании заботятся не столько о производительности, сколько об эксплуатационных расходах. Во многих случаях эти компании предпочитают передавать данные по своим собственным каналам, хотя в них задержка больше, а не по общедоступным каналам, поскольку использование последних вызывает дополнительные расходы.

Сетевые протоколы

Данные маршрутизируемых протоколов передаются по объединенной сети с использованием протоколов маршрутизации. В этом контексте маршрутизируемые протоколы также называют сетевыми протоколами. Эти сетевые протоколы выполняют различные функции, необходимые для взаимодействия приложений пользователя на устройстве-источнике и на устройстве-получателе. Эти функции могут быть самыми разными, в зависимости от используемого стека (набора) протоколов. Сетевые протоколы работают на верхних пяти уровнях эталонной модели OSI: сетевом, транспортном, сеансовом, на уровнях представления и приложений.

Термины *маршрутизируемый протокол* (routed protocol) и *протокол маршрутизации* (routing protocol) часто ошибочно воспринимают как равноценные и взаимозаменяемые. Маршрутизируемыми являются протоколы, данные которых передаются по маршрутам объединенной сети, такие, например, как Internet Protocol (IP), DECnet, AppleTalk, Novell NetWare, OSI, Banyan VINES и Xerox Network System (XNS). Протоколы маршрутизации, напротив, представляет собой протоколы, реализующие алгоритмы маршрутизации. Иными словами, протоколы маршрутизации используются промежуточными системами для составления таблиц, по которым определяются маршруты маршрути-

зируемых протоколов. Протоколами маршрутизации являются такие протоколы, как Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (Enhanced IGRP), Open Shortest Path First (OSPF), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS) и Routing Information Protocol (RIP). Более подробно маршрутизируемые протоколы и протоколы маршрутизации будут рассмотрены в последующих главах.

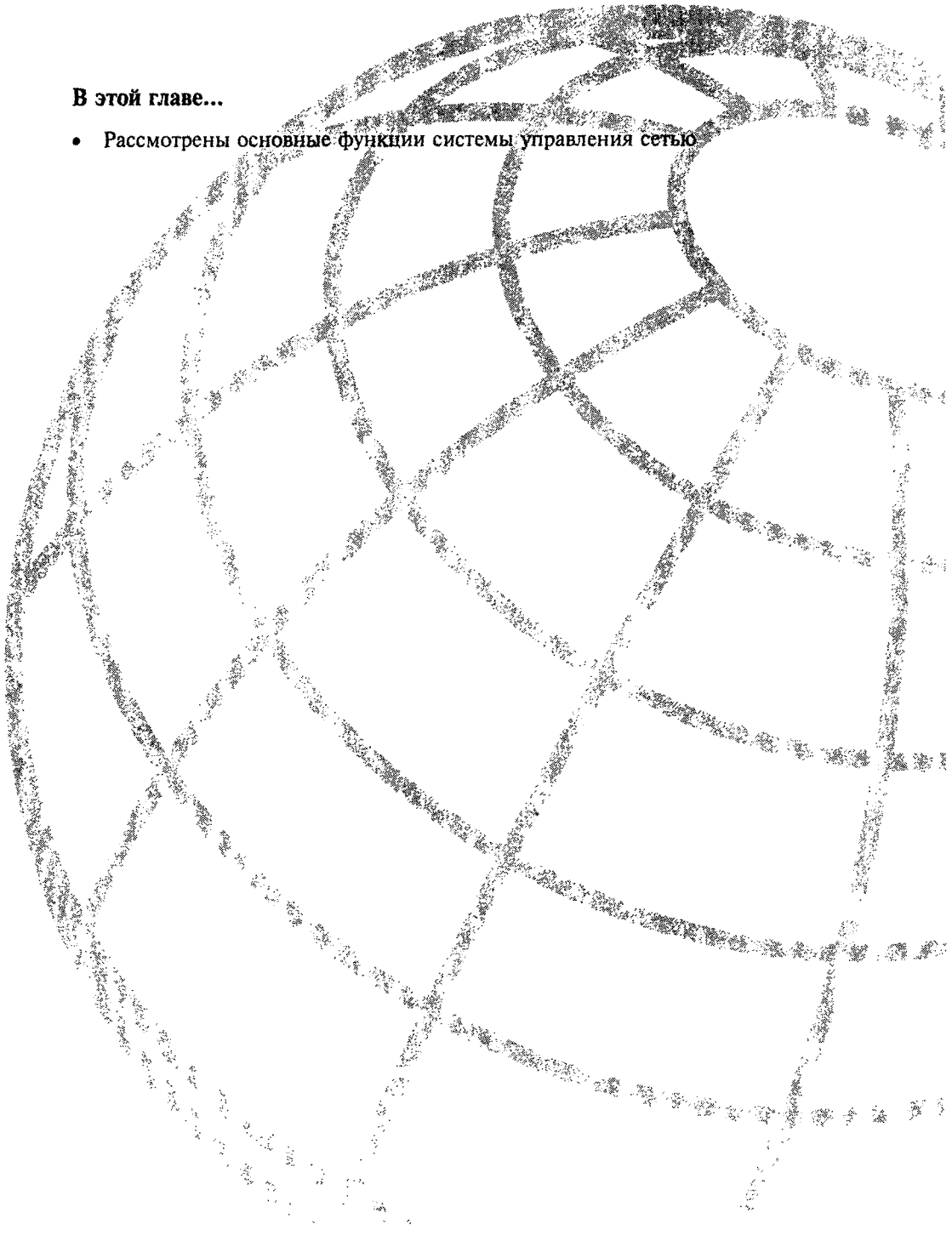
Контрольные вопросы

1. Что такое маршрутизация пакетов?
2. Назовите несколько типов алгоритмов маршрутизации.
3. Чем отличается статическая маршрутизация от динамической?

Назовите несколько метрик, используемых протоколами маршрутизации.

В этой главе...

- Рассмотрены основные функции системы управления сетью



Глава 7

Основные принципы управления сетями

Введение

В данной главе описаны функции, общие для большинства архитектур и протоколов управления сетью. Здесь также представлены пять концептуальных областей управления, определенных Международной организацией по стандартизации (International Organization for Standardization — ISO). Подробнее эти технологии, протоколы и платформы управления сетью рассматриваются в части VIII, "Управление сетями".

Что понимается под управлением сетью?

Под *управлением сетью* не всегда понимается одно и то же. В некоторых случаях речь идет о единственном сетевом консультанте, который следит за работой сети при помощи устаревшего анализатора протоколов. В других случаях для управления сетью используется распределенная база данных, автоопрос сетевых устройств и высокопроизводительные рабочие станции, составляющие в реальном времени графики изменений сетевой топологии и объема передаваемых данных. В общем смысле под управлением сетью понимают службу, использующую разнообразные средства, приложения и устройства, которые упрощают для сетевых менеджеров мониторинг и поддержку сетей.

Историческая справка

В начале 80-х годов прошлого века наблюдалось бурное развитие компьютерных сетей. Осознав экономическую выгоду и повышение производительности труда от применения сетевых технологий, компании стали создавать новые сети и расширять существующие почти с той же скоростью, с какой появлялись новые сетевые технологии и продукты. К середине 80-х годов XX века некоторые компании начали испытывать трудности от применения слишком большого количества различных (иногда несовместимых) сетевых технологий, и этих трудностей становилось все больше.

Проблемы, связанные с расширением сетей, влияют как на повседневное управление работой сети, так и на стратегическое планирование их развития. Каждая новая сетевая технология требует своих отдельных экспертов. В начале 80-х годов одна лишь потребность в обслуживающем персонале для управления большими разнородными сетями стала причиной кризиса во многих организациях. Возникла неотложная необходимость в средствах автоматизированного управления разнородными сетями (в том числе и в т.н. планировании пропускной способности сетей).

Архитектура системы управления сетью

В большинстве систем управления сетью используется одна и та же базовая структура и схема взаимодействия. На конечных станциях (управляемых устройствах), таких как компьютерные системы и другие сетевые устройства, работает программное обеспечение, позволяющее им посылать сообщения о возникающих проблемах (например, о превышении одного или нескольких граничных значений, определенных пользователем). Управляющие элементы запрограммированы таким образом, что они реагируют на получение этих сообщений одним или несколькими действиями, такими как оповещение оператора, запись в журнал событий, выключение системы или попытки ее автоматически восстановить.

Управляющие элементы также могут опрашивать конечные станции для того, чтобы проверить значения отдельных переменных. Агенты, работающие на управляемых устройствах, отвечают на все вопросы, независимо от того, являются ли они автоматическими или инициированы пользователем. *Агенты* представляют собой программные модули, которые сначала собирают информацию об управляемых устройствах, на которых они работают, затем сохраняют ее в специальной базе данных и предоставляют (самостоятельно или по запросу) управляющим элементам, принадлежащим системам управления сетью (Network Management Systems — NMS) по протоколу управления сетью, такому, например, как простой протокол управления сетью (Simple Network Management Protocol — SNMP) или информационный протокол общего управления (Common Management Information Protocol — CMIP). Управляющими прокси-серверами называются объекты, которые предоставляют управляющую информацию от имени других объектов. Типичная архитектура системы управления сетью показана на рис. 7.1.

Модель управления сетью ISO

Организация ISO внесла большой вклад в стандартизацию сетей. Ее модель управления сетью является основным средством для понимания важнейших функций систем управления сетями. Эта модель состоит из пяти концептуальных областей, описанных в следующих разделах.

Управление производительностью

Цель *управления производительностью* сети заключается в том, чтобы измерять производительность сети и предоставлять информацию о различных ее показателях, для поддержки производительности сети на приемлемом уровне. В качестве показателей производительности сети могут использоваться такие параметры, как пропускная способность сети, время реакции на запрос пользователя и степень загруженности канала.

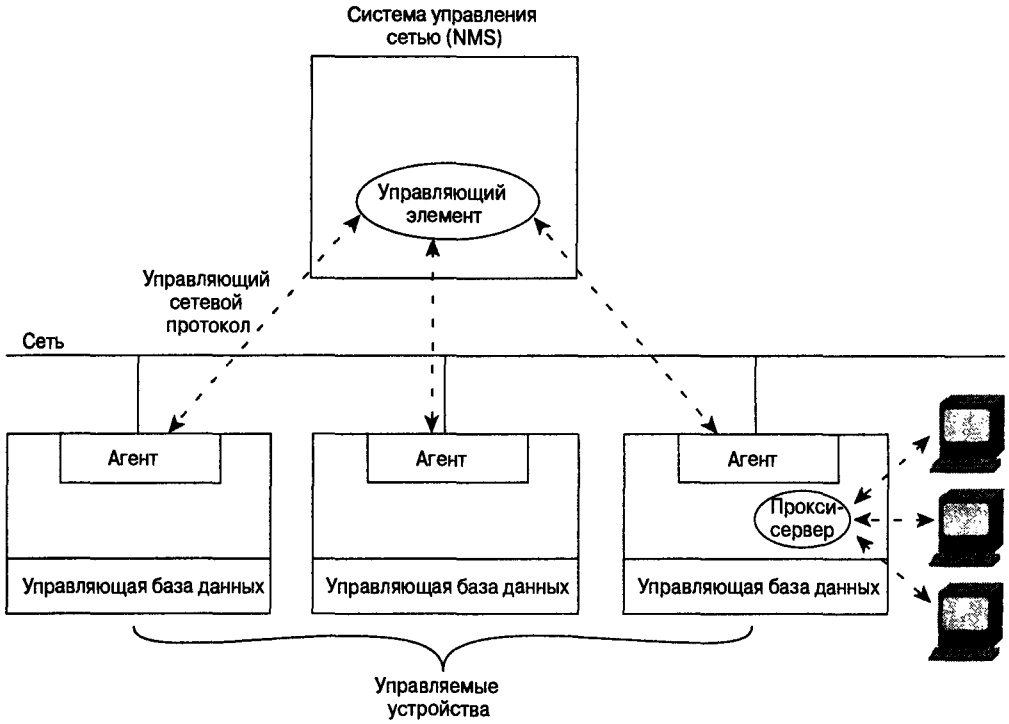


Рис. 7.1. Типичная архитектура системы управления сетью

Управление производительностью можно разделить на три основных этапа. Сначала производится сбор данных о производительности сети, которые отражаются в виде параметров, интересующих сетевых администраторов. Затем эти данные анализируются и определяются нормальные (эталонные) значения параметров. Кроме того, для каждой переменной определяются граничные значения производительности, превышение которых сигнализирует о проблеме в сети, требующей вмешательства.

Управляющие элементы постоянно следят за параметрами производительности сети. При превышении граничного значения какого-либо параметра в систему управления сетью отправляется предупреждение.

Каждая из описанных выше операций является частью процесса настройки интерактивной управляющей системы. Если производительность становится неприемлемой, поскольку превышается определенное пользователем граничное значение, то система реагирует на возникшую ситуацию отправкой сообщения. Управление производительностью сети также предусматривает профилактические меры. Например, для того чтобы предсказать влияние роста сети на параметры производительности, можно воспользоваться средствами моделирования сети. Такое моделирование предупредит администраторов о будущих проблемах и позволит вовремя предпринять контрмеры.

Управление конфигурацией

Цель *управления конфигурацией* состоит в сборе данных о конфигурации сети и системы, с тем чтобы можно было анализировать и корректировать работу различных аппаратных и программных сетевых элементов.

На каждом сетевом устройстве используются различные версии аппаратного и программного обеспечения. Например, рабочая станция инженера может иметь такую конфигурацию:

- операционная система — версия 3.2;
- интерфейс Ethernet — версия 5.4;
- программное обеспечение TCP/IP — версия 2.0;
- программное обеспечение NetWare — версия 4.1;
- программное обеспечение NFS — версия 5.1;
- контроллер последовательной передачи данных — версия 1.1;
- программное обеспечение X.25 — версия 1.0;
- программное обеспечение SNMP — версия 3.1.

Для облегчения доступа к информации подсистемы управления конфигурацией она хранится в базе данных, к которой можно обратиться в случае возникновения проблем.

Управление учетными записями

Цель *управления учетными записями (accounting)* состоит в измерении параметров использования сети одиночными пользователями и их группами для правильного регулирования этих параметров. Такое регулирование сводит к минимуму проблемы в сети, поскольку позволяет распределить сетевые ресурсы с учетом допустимой для них нагрузки, и максимально уравнивает условия доступа к сети для всех пользователей.

Как и в управлении производительностью, первым этапом управления учетными записями является измерение степени использования основных сетевых ресурсов. Анализ этих измерений позволяет определить характер использования ресурсов, на основании чего можно установить квоты их использования. Для достижения оптимальных условий доступа, как правило, требуется некоторая корректировка. С этого момента можно регулярно измерять степень загрузки ресурсов, а результаты использовать при выставлении счетов и абонентской платы, а также для того, чтобы добиться оптимального использования ресурсов.

Управление отказоустойчивостью

Цель *управления отказоустойчивостью* состоит в том, чтобы обнаруживать проблемы в сети, заносить их в журнал событий, уведомлять о них пользователей и (насколько это возможно) автоматически решать эти проблемы для поддержки эффективной работы сети. Поскольку сбои могут привести к простоям или к снижению производительности сети ниже допустимого уровня, управление отказоустойчивостью является, вероятно, самым распространенным элементом системы управления сетью ISO.

Прежде всего система управления отказоустойчивостью должна обнаруживать возникающие в сети проблемы и, по возможности, изолировать их. Затем возникшая проблема разрешается, а результат тестируется на самых важных подсистемах. После этого необходимо занести запись об обнаружении и решении проблемы в журнал событий.

Управление безопасностью

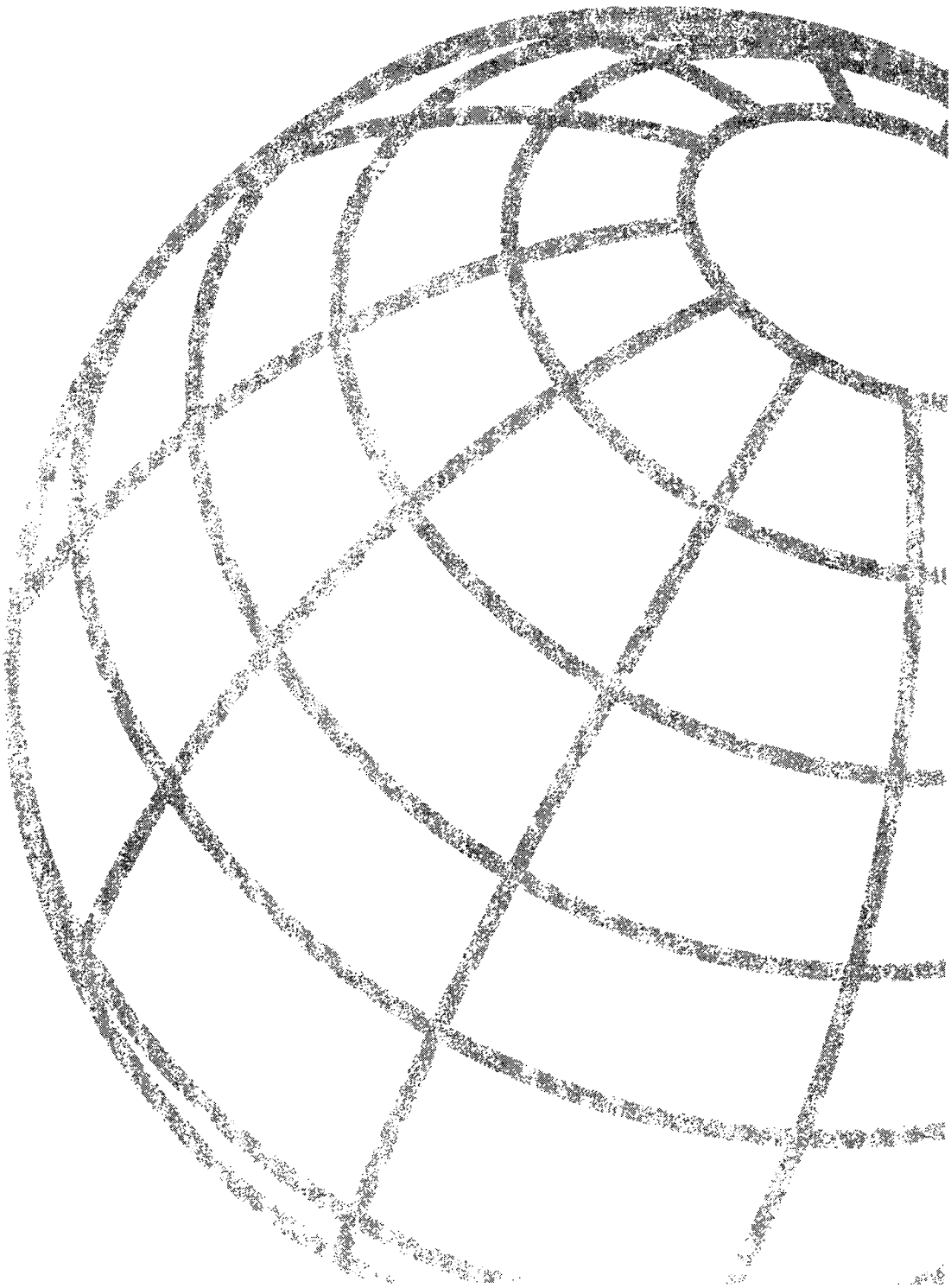
Целью *управления безопасностью в сети* является контроль доступа к сетевым ресурсам в соответствии с правилами, определяемыми конкретной ситуацией, во избежание нанесения сети ущерба (преднамеренного или непреднамеренного), а также для того, чтобы доступ к конфиденциальной информации имели только те, у кого есть соответствующие права. Например, подсистема управления безопасностью может следить за регистрацией пользователей при доступе к сетевым ресурсам и отказывать в доступе пользователю, который вводит некорректные идентификационные данные.

Подсистема управления безопасностью разделяет сетевые ресурсы на области, доступ к которым требует идентификации, и области, где этого не требуется. Некоторые пользователи — как правило, те, которые не являются сотрудниками компании, — должны иметь доступ не ко всем сетевым ресурсам. Другие сетевые пользователи (внутренние) не должны иметь доступ к информации определенного подразделения — например, отдела кадров.

Подсистема управления безопасностью выполняет несколько функций. Она определяет важные сетевые ресурсы (компьютеры, файлы и другие объекты) и устанавливает соответствие между ними и группами пользователей, которые имеют право доступа к отдельным ресурсам. Кроме того, эта подсистема следит за точками доступа к важным сетевым ресурсам и фиксирует попытки несанкционированного доступа к ним.

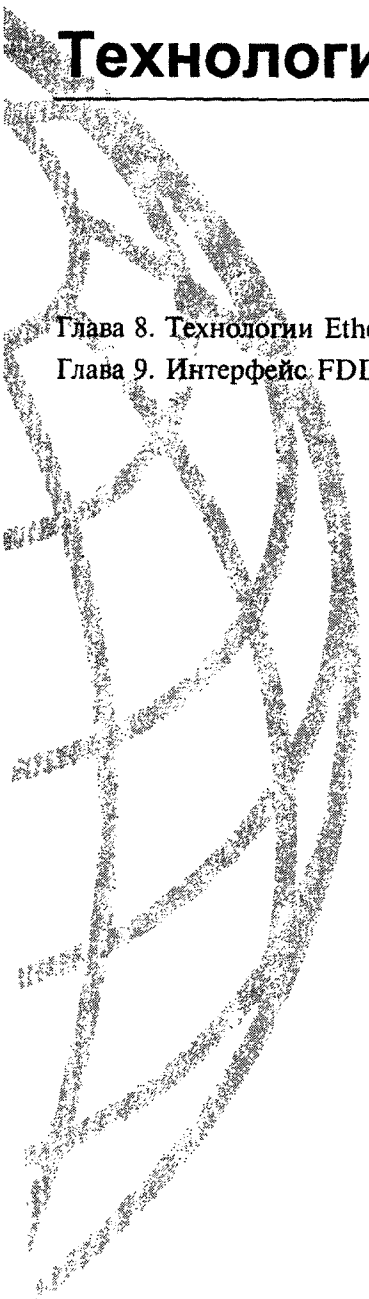
Контрольные вопросы

1. Назовите различные области управления сетью.
2. Каковы цели управления производительностью?
3. Каковы цели управления конфигурацией?
4. Каковы цели управления учетными записями?
5. Каковы цели управления отказоустойчивостью?
6. Каковы цели управления безопасностью?

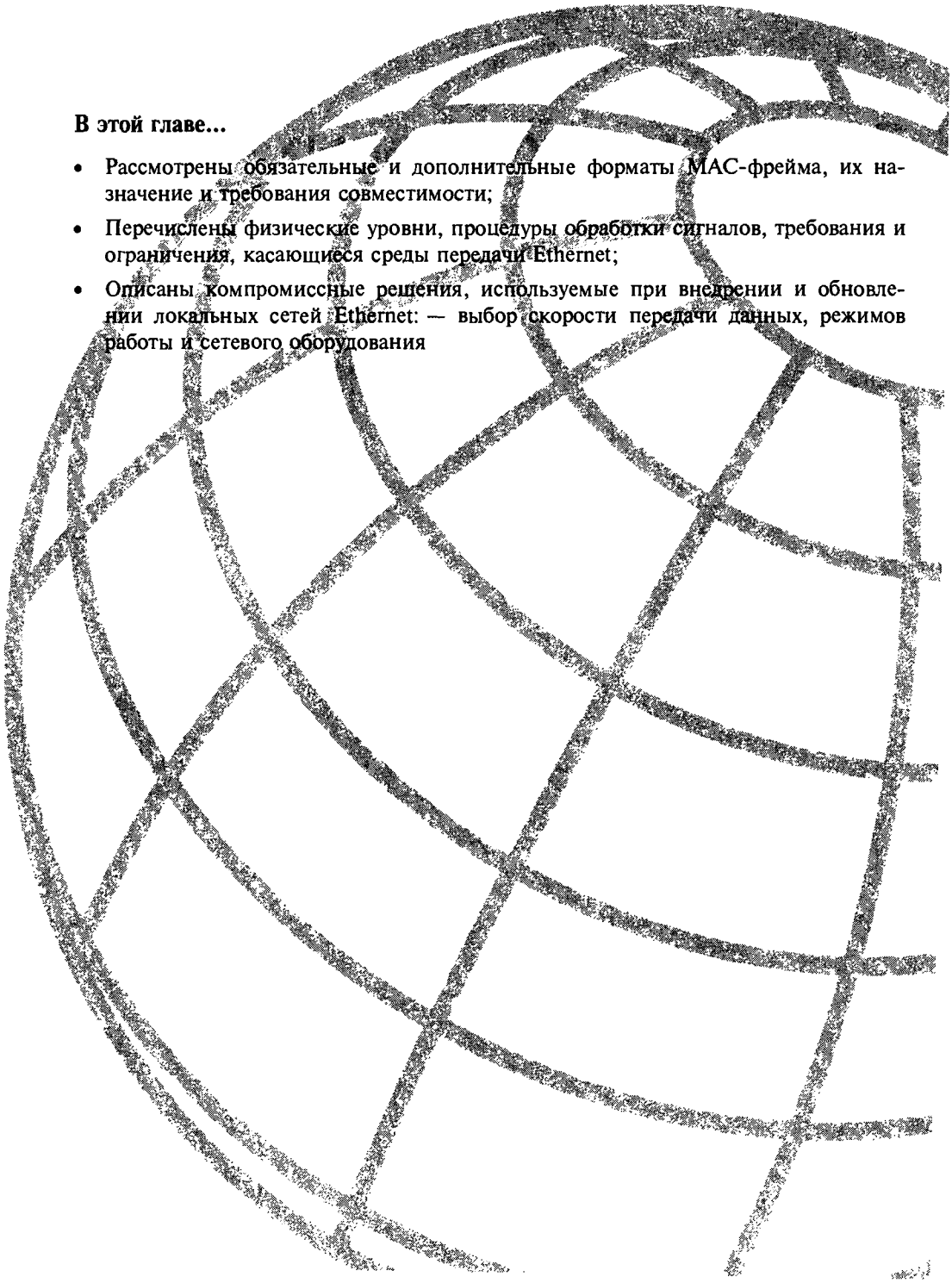


Часть II

Технологии локальных сетей



Глава 8. Технологии Ethernet
Глава 9. Интерфейс FDDI



В этой главе...

- Рассмотрены обязательные и дополнительные форматы MAC-фрейма, их назначение и требования совместимости;
- Перечислены физические уровни, процедуры обработки сигналов, требования и ограничения, касающиеся среды передачи Ethernet;
- Описаны компромиссные решения, используемые при внедрении и обновлении локальных сетей Ethernet: — выбор скорости передачи данных, режимов работы и сетевого оборудования

Глава 8

Технологии Ethernet

Введение

Термином *Ethernet* обозначают семейство аппаратных и программных продуктов для локальных сетей (local-area network — LAN), описываемых стандартом IEEE 802.3, который определяет протокол, известный под названием CSMA/CD. В настоящее время определены три стандартные скорости передачи данных по оптоволоконному кабелю и витой паре:

- 10 Мбит/с — 10BaseT;
- 100 Мбит/с — Fast Ethernet;
- 1000 Мбит/с — Gigabit Ethernet.

Стандарт 10-Gigabit Ethernet находится на стадии разработки и будет, вероятно, опубликован как дополнение IEEE 802.3ae к основному стандарту IEEE 802.3 в конце 2001 или в начале 2002 года.

В качестве возможной замены Ethernet предлагались и другие технологии и протоколы, но рынок сделал свой выбор. Технология Ethernet сохранилась в качестве основной технологии локальных сетей (в настоящее время она применяется примерно для 85 % персональных компьютеров и рабочих станций, подключенных к локальной сети) благодаря тому, что ее протокол обладает следующими характеристиками:

- простота, легкость реализации, управления и поддержки;
- возможность создать сеть с небольшими финансовыми затратами;
- значительная топологическая гибкость при реализации сетей;
- гарантия успешного взаимодействия между продуктами, соответствующими стандартам, независимо от производителя.

Краткая история сетей Ethernet

Первый вариант сети Ethernet был разработан корпорацией Xerox в 70-х годах XX века. Это была экспериментальная сеть на основе коаксиального кабеля, которая передавала данные со скоростью 3 Мбит/с с использованием протокола множественного доступа с контролем несущей и обнаружением конфликтов CSMA/CD (Carrier Sense

Multiple Access Collision Detect — CSMA/CD). Разработка предназначалась для локальных сетей со случайным, но иногда весьма интенсивным объемом передаваемых данных. Успех проекта сразу привлек к нему внимание, и в 1980 году консорциум трех компаний — Digital Equipment Corporation, Intel Corporation и Xerox Corporation — разработал спецификацию Ethernet 1.0 для передачи данных со скоростью 10 Мбит/с.

Первый стандарт IEEE 802.3 был основан на спецификации Ethernet 1.0 и был очень похож на нее. Проект стандарта был одобрен рабочей группой по стандарту 802.3 в 1983 году, а в 1985 году опубликован как официальный стандарт (ANSI/IEEE Std. 802.3-1985). С тех пор был принят ряд дополнений к стандарту, отражающих новые достижения в технологиях и позволяющих поддерживать дополнительные сетевые среды и более высокие скорости передачи, а также поддерживающих несколько новых дополнительных возможностей управления доступом к сети.

В настоящей главе термины *Ethernet* и *802.3* будут относиться исключительно к реализациям сетей, совместимых со стандартом IEEE 802.3.

Элементы сетей Ethernet

Локальная сеть Ethernet состоит из сетевых узлов и среды взаимодействия. Сетевые узлы делятся на следующие два класса.

- **Терминальное оборудование** (Data Terminal Equipment — DTE). Устройства, которые являются либо источниками, либо получателями фреймов данных. Обычно это персональные компьютеры, рабочие станции, файловые серверы или серверы печати. Устройства DTE часто называют также конечными станциями.
- **Оборудование передачи данных** (Data Communication Equipment — DCE). Промежуточные сетевые устройства, которые принимают и передают фреймы по сети. К устройствам DCE относятся не только самостоятельные устройства, такие как повторители, сетевые коммутаторы и маршрутизаторы, но и коммуникационные интерфейсы, такие как сетевые платы и модемы.

Далее в этой главе самостоятельные промежуточные сетевые устройства будут называться *промежуточными узлами*, или *DCE*, а сетевые платы будут обозначаться аббревиатурой *NIC* (network interface card — NIC).

В настоящий момент в качестве среды передачи Ethernet поддерживает: два основных типа электрических кабелей — неэкранированную витую пару (Unshielded Twisted-Pair — UTP) и экранированную витую пару (Shielded Twisted-Pair — STP), а также некоторые типы оптоволоконного кабеля.

Топологии и структуры сетей Ethernet

Существует много топологических конфигураций локальных сетей, но, независимо от их размера и сложности, все они состоят из трех основных структур взаимодействия или сетевых блоков.

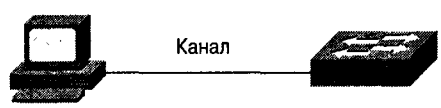


Рис. 8.1. Пример соединения типа "точка-точка"

Простейшей структурой является соединение типа "точка-точка", показанное на рис. 8.1. Оно состоит всего из двух сетевых модулей. При этом возможны соединения типа DTE-DTE, DTE-DCE или DCE-DCE. При соединении типа "точка-точка" кабель называют сетевой линией связи или сетевым каналом. Максимально допустимая длина линии связи зависит от типа кабеля и используемого метода передачи.

В первоначальных реализациях сетей Ethernet была использована шинная топология на основе коаксиального кабеля, показанная на рис. 8.2. Длина сегмента, к которому можно было подключить до 100 станций, была ограничена до 500 м. Отдельные сегменты соединялись между собой повторителями, при условии что между любыми двумя станциями в сети существует только один путь, а количество устройств DTE не превышает 1024. Общая длина пути между двумя наиболее удаленными станциями также не должна была превышать установленного значения.

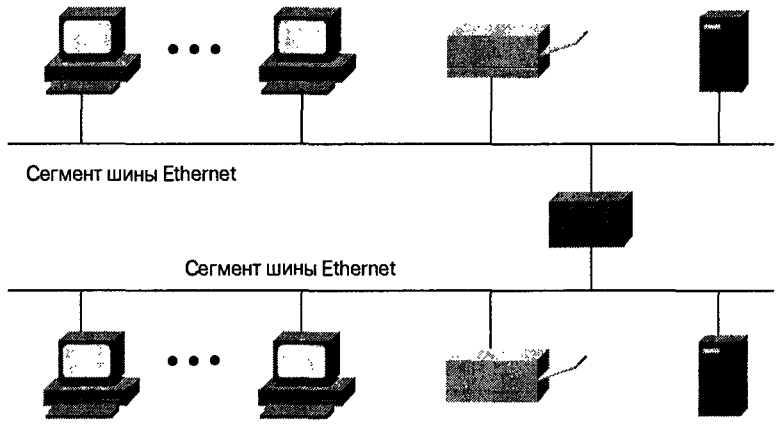


Рис. 8.2. Пример коаксиальной шинной топологии

В новых сетях шинная конфигурация, как правило, не используется, но в некоторых старых сетях она до сих пор небезуспешно применяется.

С начала 90-х годов XX века основной сетевой конфигурацией стала топология типа "звезда", показанная на рис. 8.3. Ее центральным сетевым элементом является либо многопортовый повторитель (также называемый концентратором), либо сетевой коммутатор. Все соединения в сети со звездообразной топологией представляют собой линии связи типа "точка-точка" на основе витой пары или оптоволоконного кабеля.

Связь стандарта IEEE 802.3 и эталонной модели OSI

На рис. 8.4 изображены логические уровни стандарта IEEE 802.3 и уровни эталонной модели OSI, которым они соответствуют. Как и во всех протоколах IEEE 802, канальный уровень модели OSI делится на два подуровня IEEE 802: подуровень управления доступом к среде (Media Access Control — MAC) и подуровень MAC-клиента. Физический уровень IEEE 802.3 соответствует физическому уровню модели OSI.

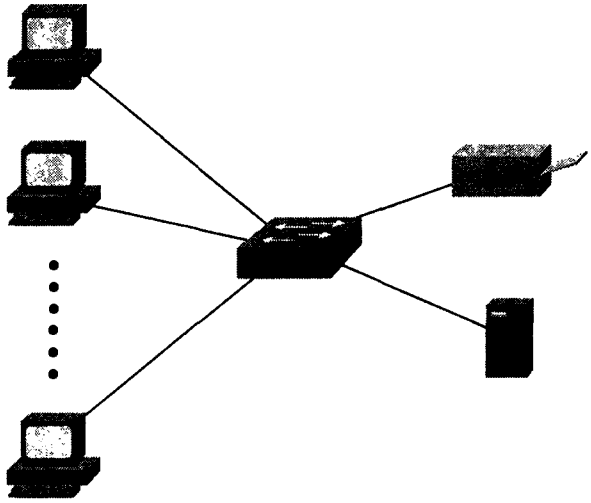


Рис. 8.3. Пример звездообразной топологии

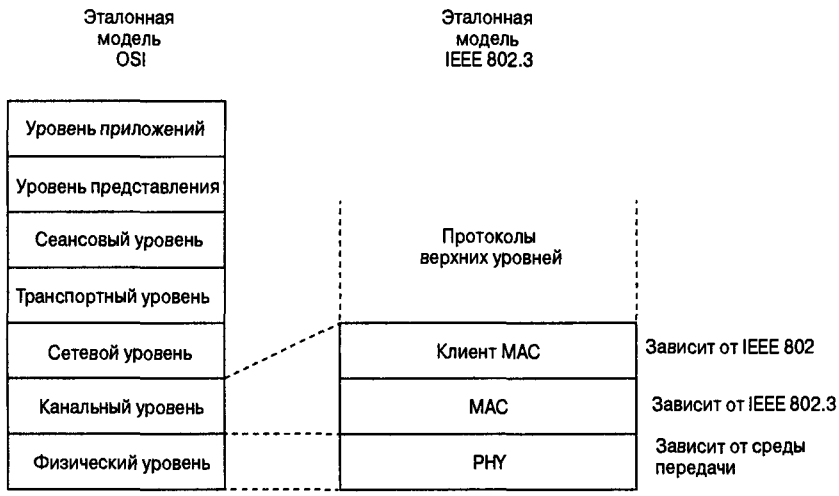


Рис. 8.4. Соответствие уровней спецификации Ethernet уровням эталонной модели OSI

Роль подуровня MAC-клиента может выполнять одно из следующих устройств.

- Подуровень LLC (Logical Link Control), если устройство принадлежит к типу DTE. Этот подуровень обеспечивает интерфейс между MAC-подуровнем Ethernet и верхними уровнями в протокольном стеке конечной станции. Подуровень LLC определяется стандартами IEEE 802.2.
- Мост, если устройство принадлежит к типу DCE. Мосты обеспечивают интерфейсы между локальными сетями как с одинаковыми протоколами (например, между сетями Ethernet), так и с различными протоколами (например, Ethernet и Token Ring). Мосты определяются стандартами IEEE 802.1.

Поскольку для всех протоколов локальных сетей IEEE 802 применяются одни и те же спецификации LLC и мостов, главной задачей каждого сетевого протокола становится со-

вместимость сетей. На рис. 8.5 показаны различные требования к совместимости, налагаемые подуровнем MAC и физическим уровнем при базовой передаче данных по каналу Ethernet.

MAC-уровень управляет доступом узла к сетевой среде передачи и зависит от конкретного протокола. Все MAC-уровни IEEE 802.3 должны удовлетворять одному и тому же набору основных логических требований, независимо от того, включают ли они в свой состав одно или несколько дополнительных расширений протоколов. Единственное требование к базовой передаче данных (не требующей дополнительных расширений протоколов) между двумя сетевыми узлами состоит в том, что оба MAC-уровня должны обеспечивать одинаковую скорость передачи.

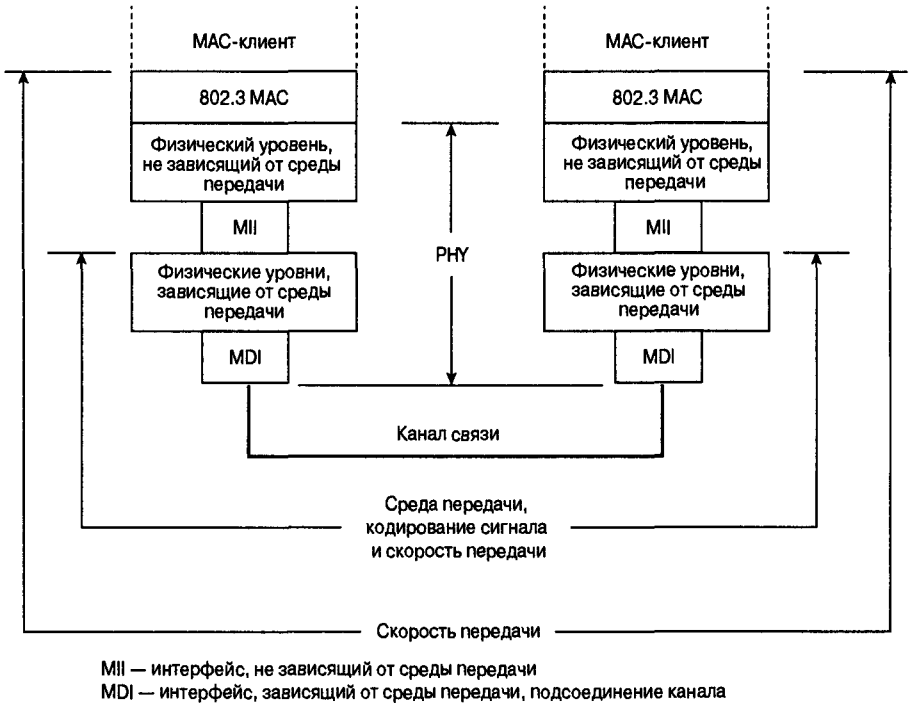


Рис. 8.5. Требования к совместимости, налагаемые подуровнем MAC и физическим уровнем при базовой передаче данных

Физический уровень 802.3 зависит от скорости передачи данных, кодирования сигнала и типа среды передачи между узлами. Например, Gigabit Ethernet предназначается для витой пары или оптоволоконного кабеля, но каждый тип кабеля и кодирования сигнала требует своей реализации физического уровня.

MAC-подуровень Ethernet

MAC-подуровень Ethernet должен выполнять две основные задачи:

- инкапсуляция данных, в том числе формирование фреймов перед передачей, а также синтаксический анализ фреймов и обнаружение ошибок во время и после приема данных;

- управление доступом к среде передачи, включая инициирование передачи фреймов и восстановление в случае сбоя при передаче.

Основной формат фрейма Ethernet

Стандарт IEEE 802.3 определяет базовый формат фрейма данных, обязательный для всех MAC-реализаций, а также несколько дополнительных форматов, применяемых для расширения базовых возможностей протокола. Основной формат фрейма данных содержит семь полей, показанных на рис. 8.6.

- **PRE (preamble, заголовок).** Длина — 7 байтов. Заголовок представляет собой набор чередующихся единиц и нулей, по которому принимающие станции узнают о поступающем фрейме. Он также служит для синхронизации принимающих физических уровней и входящего битового потока.
- **SOF (Start-of-Frame Delimiter, признак начала фрейма).** Длина — 1 байт. SOF представляет собой набор чередующихся единиц и нулей, заканчивающийся двумя единицами, что означает, что следующий бит является крайним левым битом в крайнем левом байте адреса получателя.
- **DA (Destination Address, адрес получателя).** Длина — 6 байтов. В поле адреса получателя указывается, какая станция (станции) должна получить этот фрейм. Крайний левый бит в поле адреса получателя показывает, является ли адрес индивидуальным (бит равен 0) или групповым (1), а следующий бит — является ли адрес глобально (0) или локально (1) административно управляемым. Оставшиеся 46 битов содержат уникальное значение, которое идентифицирует станцию, группу станций или все станции в сети.
- **SA (Source Address, адрес источника).** Длина — 6 байтов. Адрес источника идентифицирует отправляющую станцию. Этот адрес всегда является индивидуальным, а его крайний левый бит всегда равен 0.
- **Длина/тип.** Длина поля — 4 байта. В этом поле указывается количество байтов данных MAC-клиента, содержащихся в поле данных фрейма или идентификатор типа фрейма, если фрейм собран по дополнительному формату. Если значение этого поля меньше или равно 1500, то количество байтов LLC в поле данных равно значению поля длина/тип. Если значение поля длины/типа больше 1536, то это фрейм дополнительного типа, и значение поля длины/типа определяет тип посылаемого или получаемого фрейма.
- **Данные.** Последовательность из *n* байтов с любыми значениями, где *n* меньше или равно 1500. Если длина поля данных меньше 46, то его нужно дополнить до этого размера пустыми байтами-заполнителями.
- **Контрольная последовательность фрейма (Frame Check Sequence — FCS).** Длина — 4 байта. Эта последовательность содержит 32-битовое значение CRC (Cyclic Redundancy Check, циклическая проверка четности с избыточностью), которое вычисляется отправляющим и пересчитывается принимающим подуровнем MAC, чтобы проверить наличие поврежденных фреймов. Контрольная последовательность фрейма генерируется на основе полей DA, SA, длины/типа и поля данных.

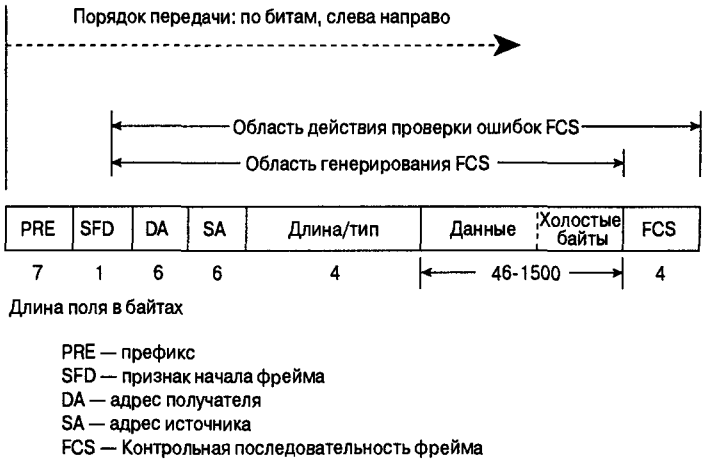


Рис. 8.6. Базовый формат фрейма данных MAC-уровня IEEE 802.3

Внимание!

Индивидуальные адреса называют также одиночными, поскольку они соответствуют единственному MAC-уровню и назначаются производителем NIC из блока адресов, выделенных IEEE. Групповые, или множественные, адреса идентифицируют конечные станции, принадлежащие рабочей группе, и назначаются сетевым администратором. Специальный групповой адрес (широковещательный адрес, состоящий только из единиц) соответствует всем станциям в сети.

Передача фрейма

Каждый раз, когда MAC-подуровень конечной станции принимает запрос о передаче фрейма, сопровождаемый адресом и информацией о данных от подуровня LLC, он начинает процедуру передачи, перенося информацию LLC в буфер MAC-фреймов.

- В поля PRE и SOF помещается заголовок и признак начала фрейма.
- В поля адресов помещаются адреса получателя и источника.
- Подсчитывается количество байтов данных подуровня LLC и это значение вставляется в поле длины/типа.
- В поле данных вставляются байты данных подуровня LLC. Если количество байтов данных LLC меньше 46, то в конец добавляется столько холостых байтов, чтобы длина поля данных составляла 46 байтов.
- По значениям полей DA, SA, длины/типа и данных вычисляется значение контрольной последовательности фрейма FCS и помещается после поля данных.

После того как фрейм собран, его фактическая передача зависит от того, в каком режиме работает MAC уровень: полудуплексном или дуплексном.

В настоящее время стандарт IEEE 802.3 требует, чтобы все MAC-уровни Ethernet поддерживали полудуплексный режим работы, в котором MAC-уровень может либо посылать, либо принимать фреймы, но не может делать то и другое одновременно. Поддержка дуплексного режима работы MAC-уровня, в котором возможен одновременный прием и передача данных, не является обязательной.

Полудуплексная передача — метод доступа CSMA/CD

Протокол CSMA/CD первоначально предназначался для того, чтобы несколько станций могли использовать общую среду передачи в некоммутируемой среде, где протокол не нуждается в центральном средстве разрешения конфликтов, маркерах доступа или назначаемых квантах времени, для указания на то, что станция имеет право передавать данные. В этом случае каждый MAC-уровень Ethernet сам определяет, когда он сможет послать фрейм.

Правила метода доступа CSMA/CD кратко выражены в названии этого протокола.

- **Контроль несущей.** Каждая станция непрерывно следит за потоками данных и отмечает вакантные промежутки времени между передачами фреймов.
- **Множественный доступ.** Станции могут начинать передачу в любой момент, когда они определят, что сеть свободна (передачи данных нет).
- **Обнаружение коллизий.** Если несколько станций в одной и той же сети CSMA/CD (коллизионный домен) начинают передачу примерно в одно и то же время, то потоки битов, поступающие от передающих станций, накладываются друг на друга (возникает коллизия — от англ. "collide" — сталкиваться), и их невозможно прочесть. В этом случае каждая из передающих станций должна быть способна обнаружить коллизию до того, как она закончит передавать свой фрейм. Обнаружив коллизию, станция должна сразу прекратить передачу. Попытаться повторить пересылку фрейма она сможет лишь по прошествии квазислучайного промежутка времени, определяемого алгоритмом блокировки.

Наихудшим является случай, когда двум наиболее удаленным друг от друга станциям сети требуется послать друг другу фреймы, и вторая станция не начинает передачу, пока не получит фрейм от первой. Вторая станция обнаружит коллизию сразу же, а первая — лишь после того, как искаженный сигнал проделает весь обратный путь. Максимальное время, которое потребуется, чтобы обнаружить коллизию (временной интервал, называемый "коллизионным окном"), оказывается примерно вдвое больше, чем время прохождения сигнала между двумя наиболее удаленными станциями сети.

Это означает, что как минимальная длина фрейма, так и максимальный диаметр коллизии прямо пропорциональны размеру "коллизионного окна". Чем длиннее фрейм, тем больше его "коллизионное окно", и следовательно, тем больше диаметр коллизий; напротив, более коротким фреймам соответствуют меньшие "коллизионные окна" и диаметры коллизий.

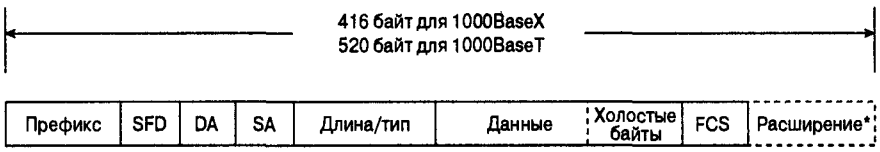
Таким образом, оптимальное решение требует нахождения компромисса между желанием минимизировать объем восстановительных работ после коллизий и потребностью в достаточно больших сетевых диаметрах, соответствующих размерам используемых сетей. В итоге было найдено компромиссное решение, которое заключалось в ограничении максимального сетевого диаметра расстоянием примерно 2500 м и в выборе такой минимальной длины фрейма, чтобы и в наихудшем варианте обеспечить обнаружение всех коллизий.

Этот компромисс был удачным решением при скорости передачи 10 Мбит/с, однако не подходил для разработчиков сетей Ethernet с более высокими скоростями передачи данных. От новой технологии Fast Ethernet требовалось, чтобы она обеспечивала обратную совместимость с ранее созданными сетями Ethernet, в том числе совместимость с существующим форматом фрейма IEEE 802.3 и с процедурами обнаружения ошибок, а также со всеми приложениями и сетевым программным обеспечением для 10-мегабитовых сетей Ethernet.

Хотя скорость распространения сигнала для всех скоростей передачи практически постоянна, время, требуемое для передачи фрейма, обратно пропорционально скорости передачи. При скорости 100 Мбит/с фрейм минимальной длины можно переслать примерно за одну десятую времени "коллизионного окна", и любая коллизия, которая может произойти при передаче, вряд ли будет обнаружена передающими станциями. Это, в свою очередь, означает, что максимальные сетевые диаметры, определенные для 10-мегабитовых сетей, не могут использоваться для сетей со скоростью передачи 100 Мбит/с. Решением этой проблемы для Fast Ethernet было уменьшение максимального сетевого диаметра приблизительно в десять раз (что составляет немногим более 200 м).

Та же проблема возникла и при разработке спецификации для Gigabit Ethernet, но уменьшать сетевой диаметр еще в десять раз (примерно до 20 м) для работы на скорости 1000 Мбит/с практически не имело смысла. На этот раз разработчики предпочли оставить максимальный диаметр коллизионного домена почти таким же, как и в 100-мегабитовых сетях, но увеличить фактический минимальный размер фрейма, добавив к фреймам, длина которых меньше минимальной, дополнительное неинформативное поле переменной длины (во время приема фрейма это поле удалялось).

На рис. 8.7 показан формат MAC-фрейма с дополнительным полем расширения для Gigabit Ethernet, а в табл. 8.1 продемонстрирован результат компромисса между скоростью передачи данных и минимальным размером фрейма для сетей Ethernet со скоростью передачи 10 Мбит/с, 100 Мбит/с и 1000 Мбит/с.



* При приеме фрейма поле расширения автоматически удаляется

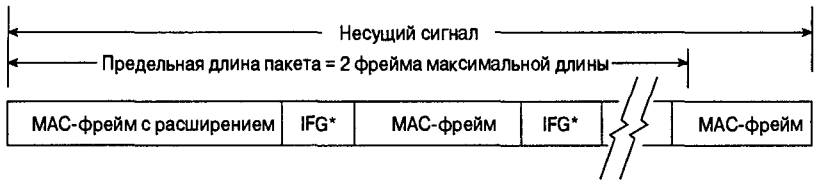
Рис. 8.7. MAC-фрейм с полем расширения для Gigabit Ethernet

Таблица 8.1. Ограничения полудуплексного режима

Параметр	10 Мбит/с	100 Мбит/с	1000 Мбит/с
Минимальный размер фрейма, байт	64	64	520[1] (с полем расширения)
Максимальный диаметр коллизии DTE-DTE	100 м для витой пары	100 м для витой пары, 412 м для оптоволоконного кабеля	100 м для витой пары, 316 м для оптоволоконного кабеля
максимальный диаметр коллизии при наличии повторителей, м	2500	205	200
Максимальное количество повторителей вдоль сетевого пути	5	21	1

[1]520 байтов — для 1000BaseT. Минимальный размер фрейма с полем расширения для 1000BaseX уменьшается до 416 байтов, так как 1000BaseX кодирует и передает по 10 битов на каждый байт.

Другим изменением спецификации передачи Ethernet CSMA/CD было добавление пакетной передачи фреймов для Gigabit Ethernet. Пакетный режим представляет собой функцию, позволяющую посылать на MAC-уровне короткую последовательность (пакет) фреймов, соответствующий приблизительно 5,4 фреймам максимальной длины, не переставая контролировать среду передачи. Интервалы между фреймами передающий MAC-подуровень заполняет битами расширения (рис. 8.8), чтобы другие станции сети видели, что сеть занята, и не пытались передавать данные, пока не закончится пакет.



* Для того чтобы обеспечить непрерывность несущего сигнала в течение передачи всей пакетной последовательности, промежутки между фреймами заполняются битами расширения

Рис. 8.8. Пакетная последовательность фреймов для Gigabit Ethernet

**Биты расширения посылаются в интервалах между фреймами для обеспечения непрерывности использования канала в течение всего времени передачи пакетной последовательности*

Если длина первого фрейма меньше минимальной длины фрейма, то к нему добавляется поле расширения, чтобы увеличить длину фрейма до величины, указанной в табл. 8.1. Остальным фреймам пакетной последовательности поля расширения не нужны, и последующие фреймы могут заноситься в пакет до тех пор, пока не будет достигнута предельная длина пакета. Если она достигнута после того, как началась передача фрейма, то передача может продолжаться до тех пор, пока не будет передан весь фрейм.

Для скоростей передачи 10 Мбит/с и 100 Мбит/с поля расширения и пакетный режим не используются.

Повышение эффективности путем дуплексной передачи

Дуплексный режим представляет собой дополнительную возможность одновременной двусторонней передачи по линии связи типа "точка-точка" на MAC-уровне. Функционально дуплексная передача намного проще полудуплексной, так как она не вызывает в среде передачи конфликтов и коллизий, не требует составления расписания повторных передач и добавления битов расширения в конце коротких фреймов. В результате не только увеличивается время, доступное для передачи данных, но и удваивается полезная полоса пропускания канала, поскольку каждый канал обеспечивает полноскоростную одновременную и двустороннюю передачу.

Обычно передача может начинаться сразу же, как только фреймы будут готовы к отправке. Единственным ограничением является то, что интервал между последовательными фреймами не должен быть меньше определенной минимальной длины (рис. 8.9), а формат фреймов должен соответствовать стандартам Ethernet.

Управление потоком

Дуплексный режим требует установки еще одной дополнительной функции — управления потоком. Она позволяет принимающему узлу (например, порту сетевого

коммутатора) в случае переполнения дать команду узлу-источнику (например, файловому серверу) приостановить передачу фреймов на некоторый короткий промежуток времени. Управление потоком осуществляется MAC-уровнями отправителя и получателя с помощью фрейма-паузы, который автоматически формируется принимающим MAC-уровнем. Если переполнение будет ликвидировано до истечения периода ожидания, то для восстановления передачи, отправляется второй фрейм-пауза с нулевым значением времени ожидания. Общая схема управления потоком показана на рис. 8.10.

Рис. 8.9. Дуплексный режим обеспечивает одновременную двустороннюю передачу по одной и той же линии связи

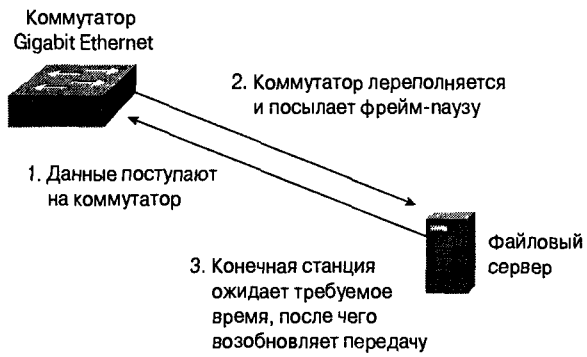


Рис. 8.10. Последовательность действий для управления потоком IEEE 802.3

Дуплексный режим и сопутствующее ему управление потоком являются дополнительными режимами для всех MAC-уровней Ethernet независимо от скорости передачи. Обе эти функции могут быть реализованы на отдельных каналах в том случае, если соответствующие физические уровни также поддерживают дуплексный режим.

Фреймы-паузы распознаются как управляющие MAC-фреймы по индивидуальным (зарезервированным) значениям поля "длина/тип". Им также назначается зарезервированное значение адреса получателя, для того чтобы исключить возможность передачи входящего фрейма-паузы протоколам верхних уровней или на другие порты коммутатора.

Получение фреймов

Процедура получения фреймов в полудуплексном и дуплексном режимах почти одинакова, за исключением того, что дуплексные MAC-станции для одновременной передачи и приема фреймов нуждаются в отдельных буферах фреймов и в отдельных маршрутах для приема и передачи данных.

Получение фреймов является процедурой, обратной их передаче. Адрес получателя поступившего фрейма (MAC-адрес, групповой или широковещательный) сверяется со списком адресов станции и определяется, предназначен ли данный фрейм для данной станции. Если адрес получателя соответствует адресу принимающей станции, то проверяется длина фрейма, а содержащееся во фрейме значение контрольной последовательности FCS сравнивается с соответствующим значением, вычисленным при приеме фрейма. Если длина фрейма соответствует требуемой и значения FSC совпадают, то по содержанию поля "длина/тип" определяется тип фрейма. Затем фрейм анализируется и передается на соответствующий верхний уровень.

Использование дескрипторов виртуальных сетей VLAN

Использование дескрипторов виртуальных сетей VLAN представляет собой дополнительную функцию MAC-уровня, которая обеспечивает пользователям Ethernet и сетевым администраторам три ранее недоступные важные возможности, которые описаны ниже.

- Ускорение прохождения по сети срочных данныхпутем назначения исходящим фреймам приоритетов при передаче.
- Объединение станций в логические группы, что позволяет нескольким локальным сетям осуществлять обмен данными так же, как если бы они находились в одной общей локальной сети. Мосты и коммутаторы фильтруют адреса получателей и передают фреймы VLAN только портам, принадлежащим той виртуальной локальной сети, для которой предназначены эти данные.
- Упрощение управления сетью, а также значительное уменьшение объема работ для администратора сети при добавлении, перемещении и замене устройств.

Фрейм с дескриптором виртуальной сети VLAN представляет собой обычный фрейм данных MAC-уровня, у которого между полем SA и полем "длина/тип" помещен 4-байтовый заголовок VLAN (рис. 8.11).

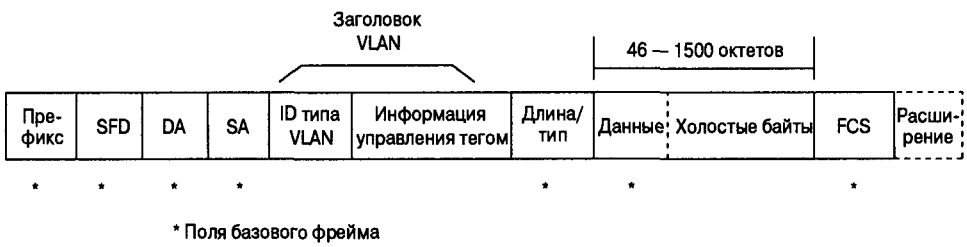


Рис. 8.11. Фреймы с дескриптором виртуальной сети VLAN распознаются MAC-уровнем благодаря тому, что на месте обычного поля "длина/тип" в этих фреймах содержится тип локальной сети

Заголовок виртуальной сети VLAN состоит из следующих двух полей:

- зарезервированное 2-байтовое значение типа, указывающее на то, что это фрейм виртуальной сети VLAN;
- 2-байтовое поле управления дескриптором (Tag-Control), в котором содержится приоритет передачи (число в диапазоне от 0 до 7, при этом значению 7 соответст-

вует наивысший приоритет) и идентификатор VLAN, указывающий, для какой виртуальной сети VLAN предназначен данный фрейм.

Принимающая MAC-станция считывает зарезервированное значение типа, которое находится там, где обычно расположено поле "длин/тип", и интерпретирует полученный фрейм как фрейм VLAN. После этого выполняются описанные ниже действия.

- Если MAC-уровень принадлежит порту коммутатора, то фрейм передается в соответствии с приоритетом всем портам, связанным с данным идентификатором VLAN.
- Если MAC- уровень принадлежит конечной станции, то 4-байтовый заголовок виртуальной сети VLAN удаляется, и фрейм обрабатывается так же, как обычный фрейм данных.

Для использования дескрипторов виртуальных сетей VLAN необходимо, чтобы все сетевые узлы, входящие в группу VLAN, поддерживали эту функцию.

Физические уровни Ethernet

Поскольку устройства Ethernet работают только на двух нижних уровнях стека протоколов OSI, они обычно реализуются как платы сетевого интерфейса (Network Interface Card — NIC), устанавливаемые на материнской плате компьютера. Платы NIC идентифицируются именем, состоящим из трех частей и основанному на атрибутах физического уровня.

Имя состоит из трех частей, указывающих скорость и метод передачи, а также типы среды и кодирования сигнала, например:

- 10BaseT — 10 Мбит/с, немодулированная передача по двум кабелям витой пары;
- 100BaseT2 — 100 Мбит/с, немодулированная передача по двум кабелям витой пары;
- 100BaseT4 — 100 Мбит/с, немодулированная передача по четырем кабелям витой пары;
- 1000BaseLX — 100 Мбит/с, немодулированная низкочастотная передача по оптоволоконному кабелю.

Иногда возникает вопрос о том, почему в обозначении всегда присутствует слово "Base". Первые версии протокола допускали также широкополосную передачу (например 10Broad), но они не имели успеха на рынке. Все современные реализации Ethernet предусматривают немодулированную передачу.

Кодирование передаваемого сигнала

При немодулированной передаче информация фрейма передается прямо по каналу связи в виде последовательности импульсов, которые обычно ослабляются (уменьшается амплитуда) и искажаются (изменяют форму), прежде чем достигают другого конца линии. Задача получателя заключается в том, чтобы распознать каждый поступающий импульс и правильно определить его значение, перед тем как передать восстановленную информацию принимающему MAC-устройству.

Хотя для восстановления размера и формы полученного сигнала применяются фильтры и цепи формирования импульсов, однако для того, чтобы обеспечить правильную выборку полученных сигналов в соответствии с периодом импульсов и с

той же скоростью, с какой они передаются, требуются описанные ниже дополнительные меры.

- Синхросигнал получателя должен быть восстановлен на основе входного потока данных, для того чтобы принимающий физический уровень мог синхронизироваться с входными импульсами.
- Необходимо принять меры по компенсации эффекта передачи, известного как блуждание базовой линии.

Восстановление синхросигнала требует анализа переходов уровня во входном сигнале идентификации и синхронизации границ импульсов. Чередующиеся единицы и нули заголовка фрейма не только сообщают о поступлении фрейма, но и помогают восстановить синхросигнал. Однако восстановленные синхросигналы могут смещаться и терять синхронизацию, если уровень импульсов не изменяется и переходы обнаружить не удается (например, при передаче длинной цепочки нулей).

Блуждание базовой линии является следствием того, что каналы Ethernet связаны по переменному току с трансиверами и эта связь может обеспечить стабильный уровень напряжения только на короткое время. В результате переданные импульсы искажаются, появляются спады наподобие тех, которые (в увеличенном масштабе) показаны на рис. 8.12. В длинных цепочках единиц или нулей спад может быть настолько сильным, что уровень напряжения превышает пороговый, приводя к ошибочному распознаванию искаженных импульсов.

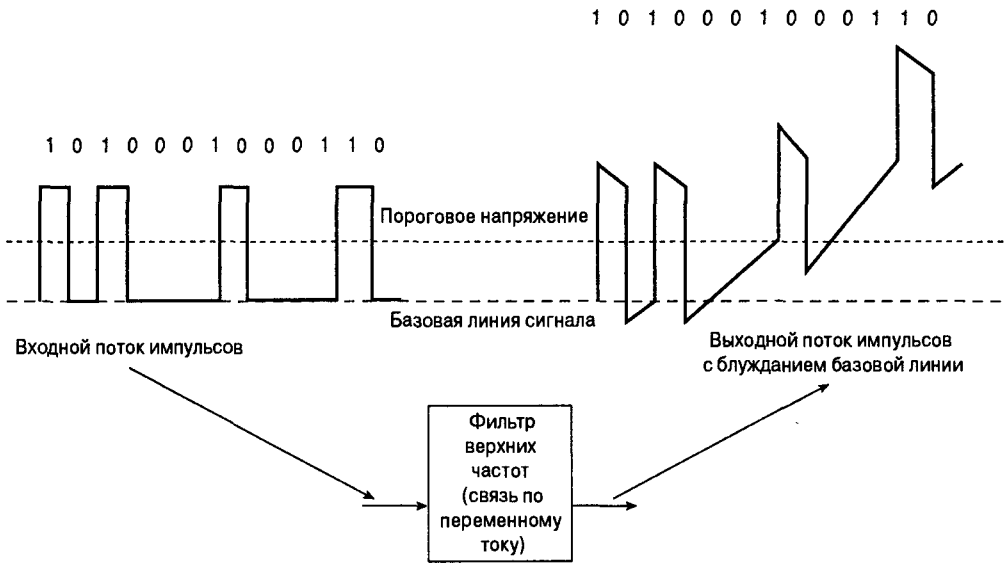


Рис. 8.12. Схематический пример блуждания базовой линии

К счастью, кодирование выходного сигнала перед передачей может существенно ослабить влияние этих неблагоприятных факторов, а также снизить вероятность ошибок при передаче. В первых версиях Ethernet, в том числе в версии 10BaseT, использовался т.н. манчестерский код (рис. 8.13), где каждый импульс явно идентифицировался по направлениям перехода среднего импульса, а не выбранным значениям уровня.

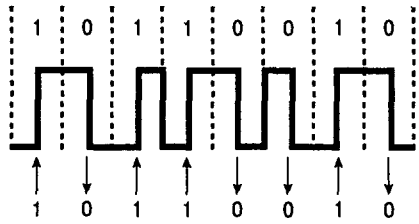


Рис. 8.13. Манчестерскае двоичное кодирование, основанное на направлении перехода

Однако при манчестерском кодировании возникает ряд сложных проблем, связанных с частотой, что делает его непригодным для более высоких скоростей передачи данных. В версиях Ethernet после 10BaseT используются иные процедуры кодирования, основанные на некоторых или на всех из перечисленных ниже методов.

- **Перестановка данных.** Упорядоченная (и обратимая) перестановка битов в каждом байте. Некоторые нули заменяются единицами, а единицы — нулями, при этом другие биты не изменяются. В результате уменьшается длина серий одинаковых битов, увеличивается плотность передачи и упрощается восстановление синхронизации.
- **Расширение кодового пространства.** Методика, которая позволяет назначать символам данных и символам управления различные коды (такие, как признаки начала и конца потока, биты расширения и т.п.), что помогает обнаруживать ошибки передачи.
- **Прямое исправление ошибок.** Кодирование, при котором к пересылаемому потоку данных добавляется избыточная информация, благодаря которой некоторые типы ошибок передачи можно исправить при приеме фреймов.

Внимание!

В версии 1000BaseT коды прямого исправления позволяют значительно снизить частоту битовых ошибок. Обработка ошибок в протоколе Ethernet ограничивается обнаружением битовых ошибок в полученном фрейме. Восстановление фреймов, полученных с неисправленными ошибками, или отсутствующих фреймов производится на более высоких уровнях используемого стека протоколов.

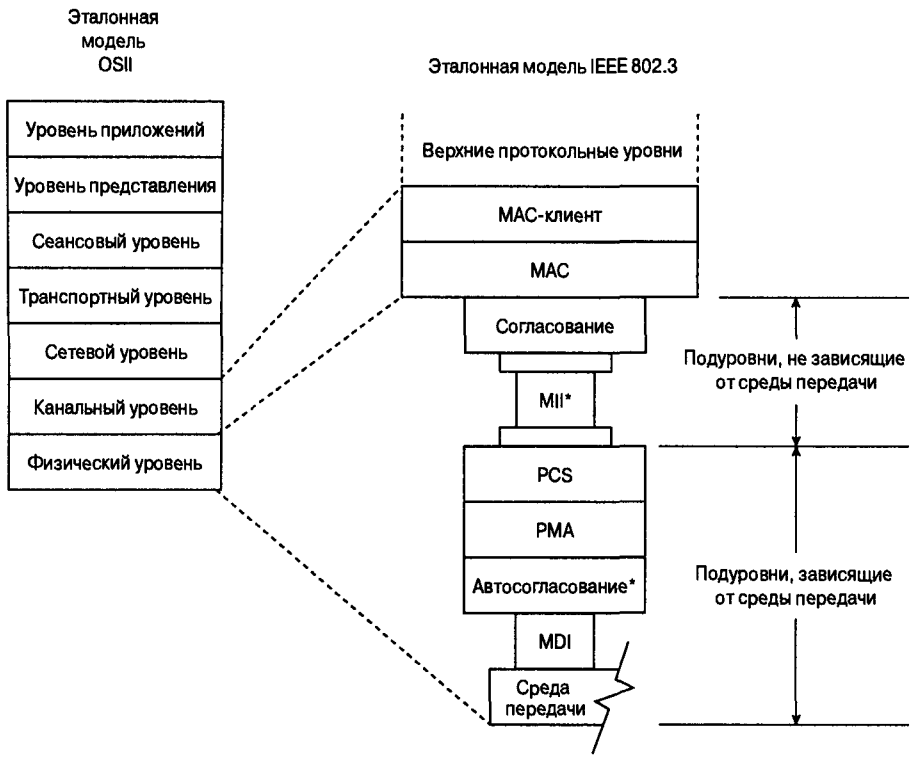
Взаимосвязь между физическим уровнем 802.3 и эталонной моделью OSI

Несмотря на то, что конкретная логическая модель физического уровня зависит от версии, все платы NIC Ethernet, как правило, соответствуют общей модели, показанной на рис. 8.14.

Физический уровень, соответствующий определенной скорости передачи, делится на подуровни, не зависящие от типа среды передачи, и те, которые зависят от типа среды передачи и кодирования сигнала.

- Подуровень согласования и дополнительный интерфейс, не зависящий от среды передачи (MII для версий Ethernet 10 Мбит/с и 100 Мбит/с, GMII для

Gigabit Ethernet), обеспечивают логическую связь между MAC-уровнем и различными группами уровней, зависящих от среды передачи. Типы согласования MII и GMII характеризуются раздельными маршрутами для приема и передачи данных, побитовыми для версии Ethernet 10 Мбит/с, послоговыми (по 4 бита) для 100 Мбит/с и побайтовыми (по 8 битов) для 1000 Мбит/с. Интерфейсы, не зависящие от среды передачи, и подуровень согласования являются общими для соответствующих скоростей передачи и конфигурируются для дуплексных операций в версии 10BaseT и во всех последующих версиях Ethernet.



MDI — интерфейс, зависящий от среды передачи
MII — интерфейс, не зависящий от среды передачи
PCS — подуровень физического кодирования
PMA — дополнение физической среды передачи
* Дополнительные необязательные уровни

Рис. 8.14. Общая эталонная модель физического уровня Ethernet

- Зависящий от среды передачи подуровень физического кодирования (Physical Coding Sublayer — PCS), обеспечивает логическую схему кодирования, мультиплексирования и синхронизации исходящих символьных потоков, а также выравнивание символьного кода, демультиплексирование и декодирование входящих данных.
- Подуровень подсоединения к физической среде передачи (Physical Medium Attachment — PMA) содержит устройства приема и передачи сигналов, (иногда

называемые трансиверами), а также схему восстановления синхронизации получаемых потоков данных.

- Интерфейс, зависящий от среды передачи (Medium-Dependent Interface — MDI), представляет собой кабельное соединение между устройствами приема/передачи сигналов и линией связи.
- Подуровень автосогласования позволяет сетевым адаптерам, расположенным на концах линии связи, обмениваться информацией о своих возможностях и выбирать из поддерживаемых обоими устройствами режимов работы наиболее подходящий. В первых версиях Ethernet автосогласование было дополнительной функцией, но в более поздних стало обязательным.
- Возможность поддержки дуплексных операций подуровнями PCS и PMA зависит от типа кодирования сигнала и от конфигурации канала.

Спецификация Ethernet 10BaseT (скорость передачи 10 Мбит/с)

Спецификация 10BaseT обеспечивает последовательную передачу данных с манчестерским кодированием и скоростью 10 Мбит/с по двойной неэкранированной витой паре. Хотя изначально стандарт был рассчитан на обычный телефонный кабель, чаще используются две пары четырехпарной витой пары кадескрипторий 3 или 5, на каждом конце которой установлен сетевой адаптер с 8-контактным разъемом RJ-45 (MDI), как показано на рис. 8.15. Поскольку каждая активная пара сконфигурирована для полудуплексного, однонаправленного режима передачи, физические уровни 10BaseT поддерживают как полудуплексный, так и дуплексный режим работы.

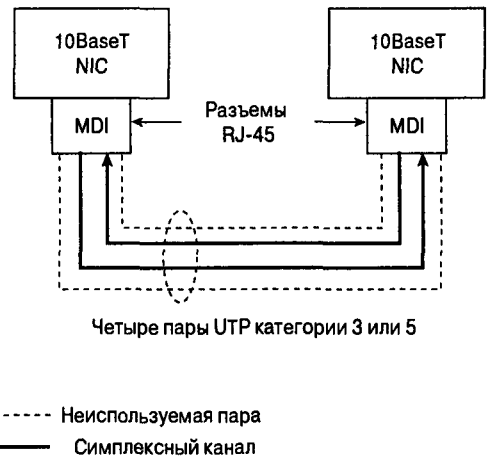


Рис. 8.15. Типичная линия связи 10BaseT представляет собой четырехпарный кабель UTP, где две пары не используются

Хотя в некоторых кругах стандарт 10BaseT считается устаревшим, он все же рассматривается в настоящей книге, поскольку во многих сетях он до сих пор используется, а дуплексный режим дал ему вторую жизнь.

Спецификация 10BaseT также является первой версией Ethernet с проверкой целостности канала для определения его работоспособности. Сразу же после включения питания подуровень PMA передает обычный канальный импульс (Normal Link Pulse — NLP), чтобы сообщить сетевому адаптеру на другом конце линии о своем намерении установить активное соединение.

- Если сетевой адаптер на другом конце линии включен, то он посылает в ответ свой собственный импульс NLP.
- Если он не включен, то первый сетевой адаптер продолжает посылать импульсы NLP каждые 16 мс, пока не получит ответ.
- Линия связи активизируется только после того, как сетевые адаптеры успешно обменяются импульсами NLP.

Спецификация Fast Ethernet (скорость передачи 100 Мбит/с)

Увеличить скорости передачи Ethernet в десять раз по сравнению с 10BaseT было непросто, однако результатом усилий в этом направлении стало появление трех стандартов физического уровня для передачи данных со скоростью 100 Мбит/с по неэкранированной витой паре: 100BaseTX и 100BaseT4 в 1995 году и 100BaseT2 в 1997 году. Несмотря на то, что некоторые общие параметры кабеля у них совпадают, каждый из этих стандартов предъявляет свои требования к кодированию и имеет зависящие от среды передачи подуровни. В табл.8.2 приводится сравнение характеристик физического уровня версии 10BaseT с различными версиями 100Base.

Таблица 8.2. Характеристики физического уровня 100BaseT

Версия Ethernet	Скорость передачи символов[1]	Кодирование	Кабель	Дуплексный режим
10BaseT	10 Мбод	Манчестерский	Два UTP категории не ниже -3	Да
100BaseTX	125 Мбод	4B/5B	Два UTP категории не ниже — 5 или STP, тип 1	Да
100BaseT4	33 Мбод	8B/6T	Четыре UTP категории не ниже —3	Нет
100BaseT2	25 Мбод	PAM5x5	Два UTP категории не ниже —3	Да

[1] Один бод равен одному символу в секунду. Символ может состоять из одного или нескольких двоичных разрядов.

Несмотря на то, что не все 100-мегабитовые версии имели успех на рынке, они описаны в литературе и оказали воздействие на последующие разработки. Поэтому ниже рассматриваются все три версии.

Спецификация 100BaseX

Стандарт 100BaseX описывает передачу данных по двойной неэкранированной витой паре или двойному оптоволоконному кабелю. Кодирование, декодирование и вос-

становление синхронизации в обоих случаях одинаковы, но природа передаваемых сигналов различна: в первом случае это электрический импульс, а во втором — световой. Приемопередатчики сигналов, которые в общей логической модели, изображенной на рис. 8.14, являются частью функции PMA, здесь определены как самостоятельные подуровни, зависящие от среды передачи (Рис. 8.16).

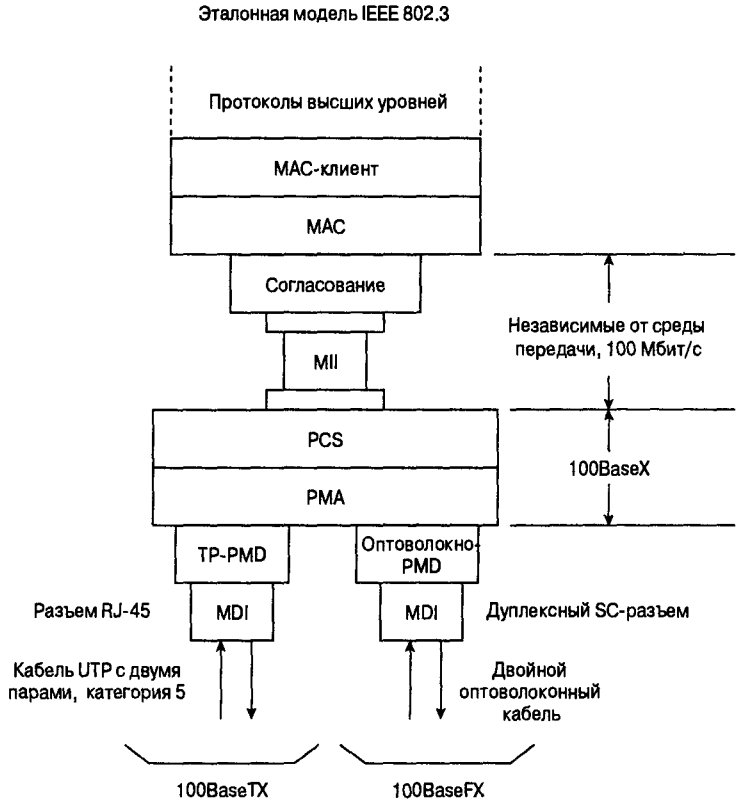


Рис. 8.16. Логическая модель 100BaseX

Кодирование 100BaseX основано на первых сигнальных стандартах физического подуровня, разработанных ISO и ANSI и зависящих от среды передачи: FDDI — для оптоволоконного кабеля и FDDI/CDDI — для витой пары. Для полупроводниковых приемопередатчиков CDDI и разъема RJ-45 был использован зависящий от среды передачи физический подуровень 100BaseTX (TP-PMD), а для оптических приемопередатчиков FDDI и разъема Low Cost Fibre Interface Connector (разъем экономичного оптоволоконного интерфейса, часто называемый дуплексным SC-разъемом) — оптоволоконный PMD.

Декодирование 4B/5B выполняется так же, как и кодирование, используемое в FDDI, однако с меньшей адаптацией к применяемому Ethernet управлению фреймами. Каждый слог (4 бита) данных (половина байта данных) преобразуется в 5-битовую двоичную кодовую группу, которая передается побитово по линии связи. В расширенном кодовом пространстве, обеспечиваемом тридцатью двумя 5-битовыми кодовыми группами, все значения делятся на следующие кадескрипторории.

- 16 возможных значений в 4-битовом слоге (16 кодовых групп).
- 4 управляющие кодовые группы, передаваемые попарно и служащие признаками начала (Start-Of-Stream Delimiter — SSD) и конца (End-Of-Stream Delimiter — ESD) потока. Каждый MAC-фрейм заключен между признаками начала и конца фрейма. Первый байт префикса заменяется кодовой парой SSD, точно идентифицирующей кодовые границы фрейма. Кодовая пара ESD добавляется после поля фрейма FCA.
- Специальная кодовая группа IDLE, которая постоянно посылается в течение межфреймовых интервалов для сохранения синхронизации между сетевыми адаптерами на концах линии связи. Получение сигнала IDLE интерпретируется как сообщение о том, что линия свободна.
- 11 недействительных кодовых групп, передаваемых сетевым адаптером непреднамеренно (хотя одна из них используется повторителем для распространения сообщения об ошибке приема). При получении любой такой кодовой группы весь входящий фрейм рассматривается как ошибочный.

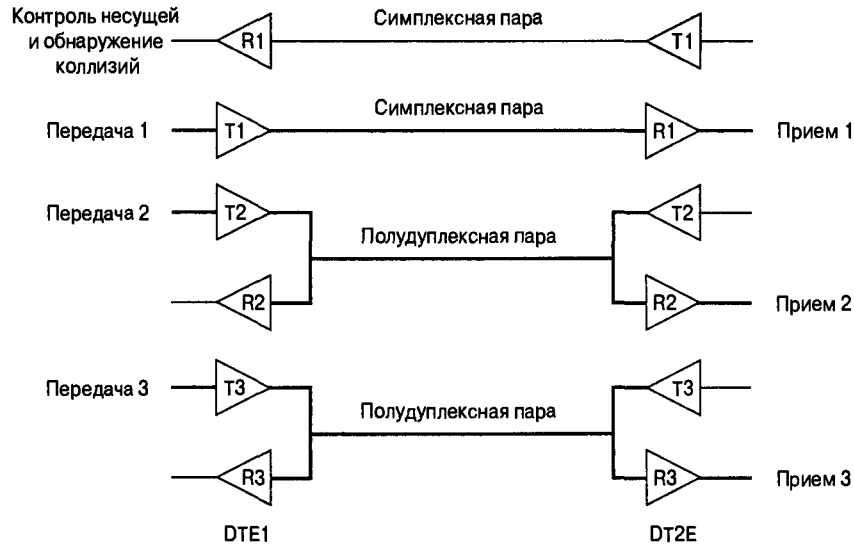
На рис. 8.17 показано, как MAC-фрейм перед передачей инкапсулируется в поток кодовых групп 100BaseX.

Рис. 8.17. Инкапсуляция фрейма в поток кодовых групп 100BaseX

В 100BaseTX прием и передача происходит по такой же паре каналов и с таким же назначением контактов, что и в MDI стандарта 10BaseT. И 100BaseTX, и 100BaseFX поддерживают полудуплексную и дуплексную передачу.

Стандарт 100BaseT4

Стандарт 100BaseT4 был разработан с целью обеспечить возможность передачи данных со скоростью 100 Мбит/с по сетям 10BaseT без замены четырех кабелей UTP кадескриптории 3 новыми кабелями кадескриптории 5. Две из четырех пар настроены на полудуплексную передачу в любом направлении, но не в обоих направлениях сразу. Другие две пары настроены на симплексный режим передачи только в одном направлении. При передаче фреймов используются обе полудуплексные пары, а также симплексная, в соответствии с направлением передачи (рис. 8.18). По симплексной паре информация передается в обратном направлении, что обеспечивает контроль несущей и обнаружение коллизий. 100BaseT4 не поддерживает дуплексный режим.



Жирным выделены маршруты передачи DTE1

Рис. 8.18. Передача фреймов по витой паре по стандарту 100BaseT4

В спецификации 100BaseT4 используется схема кодирования 8B6T, в которой каждый 8-битовый двоичный байт преобразуется в последовательность из шести троичных (трехуровневых: +1; 0; −1) символов, известных как кодовая группа 6T. Некоторые группы 6T используются как сигналы IDLE и управляющие кодовые группы, необходимые для передачи фреймов. Получение сигнала IDLE по выделенной принимающей паре означает, что линия свободна.

Во время передачи фреймов кодированные данные 6T передаются в циклической последовательности с задержками по трем передающим витым парам (рис. 8.19). Каждый фрейм инкапсулирован между кодовыми группами 6T, служащими признаками начала и конца кодированного фрейма, а также начала и конца кодированного потока на каждой витой паре. Прием по выделенной витой паре кодовых групп, отличных от IDLE, в любой момент до того, как будет превышено время "коллизионного окна", означает, что произошла коллизия.

Спецификация 100BaseT2

Спецификация 100BaseT2 была разработана в качестве альтернативы обновлению сетей с кабелями кадескриптororии 3 по стандарту 100BaseT4. 100BaseT2 была призвана решить две новые важные задачи:

- обеспечить взаимосвязь между двумя витыми парами кадескриптororии 3 или выше;
- поддерживать как полудуплексный, так и дуплексный режим.

В 100BaseT2 используется процедура передачи сигналов, отличная от предыдущих реализаций Ethernet для витой пары. Вместо двух симплексных каналов, образующих один дуплексный, в 100BaseT2 используется метод двойной дуплексной немодулированной передачи кодированных символов одновременно в обоих направлениях по

обеим витым парам (Рис. 8.20). Термин "TDX<3:2>" означает 2 самых значимых бита в слоге перед кодированием и передачей, а "RDX<3:2>" — те же два бита после приема и декодирования.

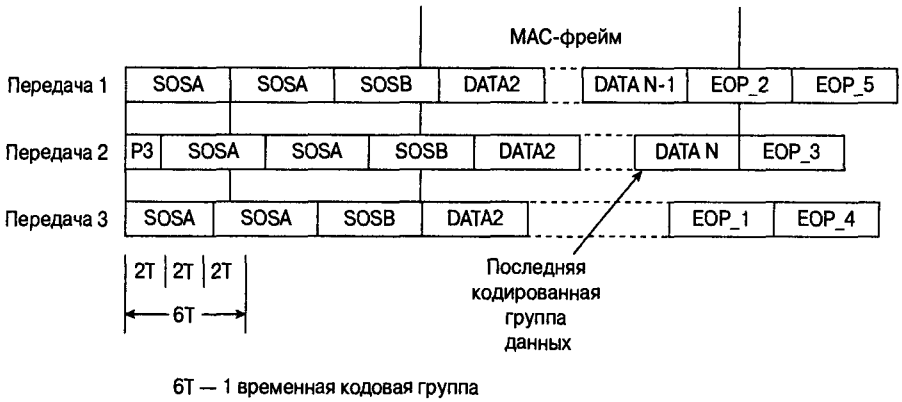
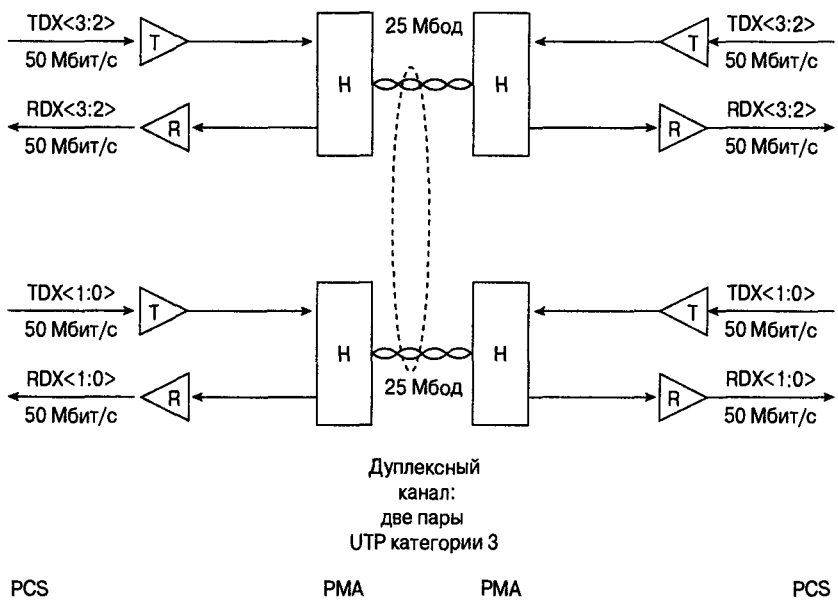


Рис. 8.19. Последовательность передачи фрейма 100BaseT4



H — гибридный подавляющий приемопередатчик
T — передающее кодирующее устройство
R — приемное декодирующее устройство
Два кодированных символа PAM5 = один слог

Рис. 8.20. Топология канала 100BaseT2

Двойная дуплексная немодулированная передача требует наличия на обоих концах линии связи сетевых адаптеров, работающих в режиме временных циклов "ведущий/

ведомый". Какой адаптер когда является ведущим, а когда ведомым — определяется во время автосогласования при инициировании линии. Когда линия находится в рабочем режиме, синхронизация определяется внутренним генератором частоты синхронизации ведущего сетевого адаптера. Ведомый сетевой адаптер использует для получения и передачи восстановленную частоту синхронизации (Рис. 8.21). Каждый переданный фрейм инкапсулирован, а во время межфреймовых интервалов синхронизация линии связи поддерживается непрерывным потоком символов IDLE.

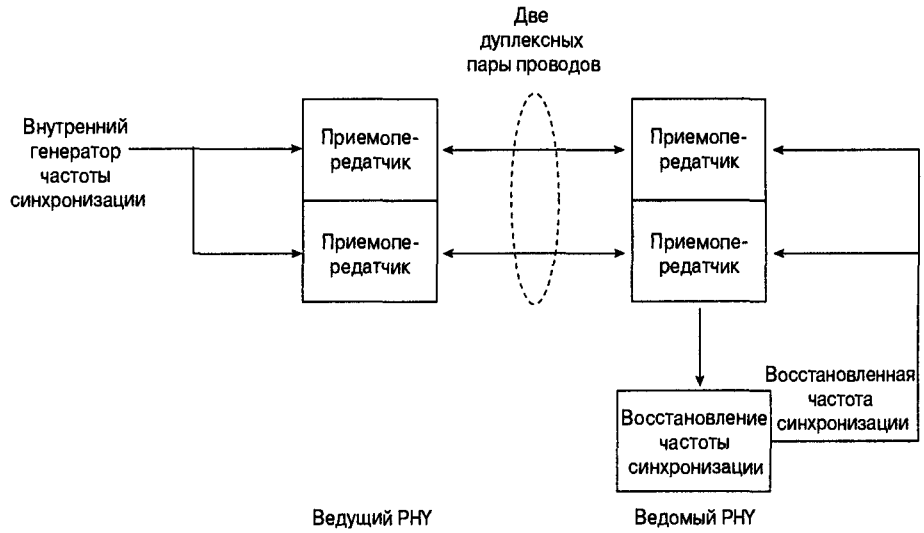


Рис. 8.21. Конфигурация временных циклов 100BaseT2

В процессе кодирования 100BaseT2 в первую очередь шифруются слоги фреймов данных для нарушения последовательности одинаковых битов. Затем два верхних и два нижних бита каждого слога преобразуются в два пятиуровневых (+2, +1, 0, −1, −2) импульсных амплитудно-модулированных (Pulse Amplitude-Modulated — PAM5) символа, которые передаются одновременно по двум витым парам (PAM5x5). Различные процедуры шифрования для ведущей и ведомой передачи обеспечивают рассогласование потоков данных, движущихся в противоположных направлениях по одной витой паре.

Процедура получения сигнала, в сущности, обратна процедуре передачи. Поскольку сигнал, поступивший на MDI по каждой витой паре, является результатом наложения передаваемого и принимаемого сигналов, каждый получатель вычитает из сигнала, полученного MDI, переданные символы и получает символы входного потока данных. Затем входящая символьная пара декодируется, упорядочивается и восстанавливается в виде слога данных для передачи MAC.

Спецификация Gigabit Ethernet — 1000 Мбит/с

Вследствие разработки стандартов Gigabit Ethernet появились две основные спецификации: 1000BaseT — для неэкранированной витой пары и 1000BaseX — для экранированной витой пары, а также для одно- и многомодового оптоволоконного кабеля (Рис. 8.22).

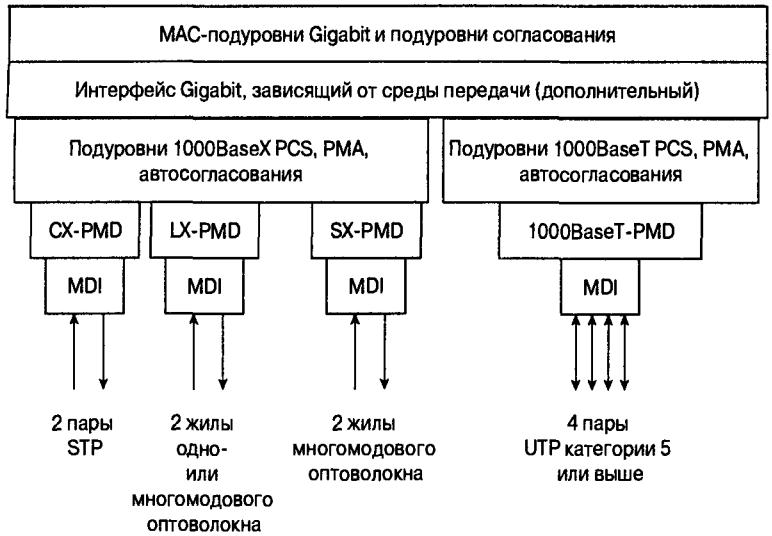


Рис. 8.22. Разновидности Gigabit Ethernet

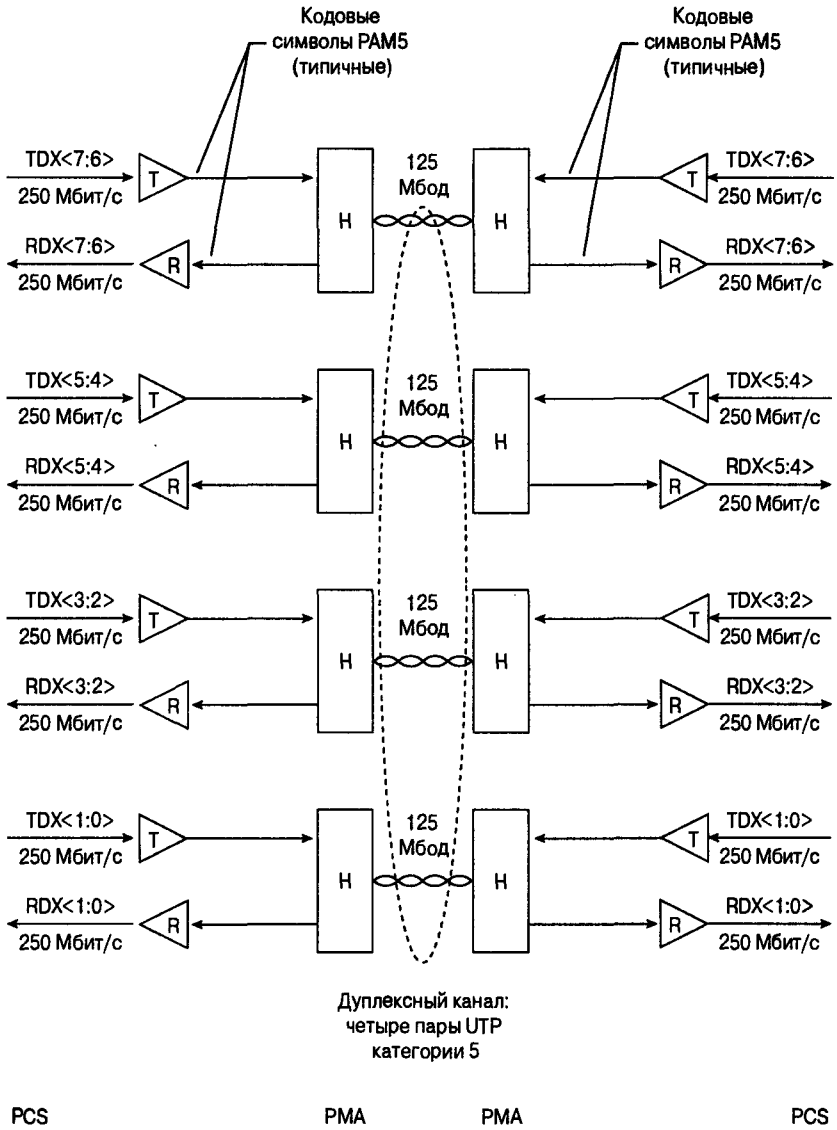
1000BaseT

1000BaseT Ethernet обеспечивает дуплексную передачу по четырехпарной витой паре кадескриптopории 5 или выше. 1000BaseT широко использует результаты исследований и разработки, которые дали толчок развитию реализации физического уровня Fast Ethernet.

- В спецификации 1000BaseTX доказана возможность успешной передачи потоков двоичных символов по UTP кадескриптopории 5 со скоростью 125 Мбод.
- В 1000BaseT4 содержится описание основных принципов передачи многоуровневых сигналов по четырем витым парам.
- В спецификации 1000BaseT2 доказано, что при кодировании PAM5 и цифровой обработке сигналов возможна одновременная передача двунаправленных потоков данных и решение потенциальных проблем, вызванных наводками из-за сигналов, передаваемых по смежным парам проводов.

В 1000BaseT шифруется каждый байт MAC-фрейма во избежание образования цепочек одинаковых битов, а результат кодируется методом 4-D, 8-State Trellis Forward Error Correction (FEC), где по четырем парам проводов отправляются одновременно четыре символа PAM5. Четыре из пяти уровней в каждом символе PAM5 представляют два бита в байте данных. Пятый уровень используется для кодирования FEC, которое улучшает восстановление символов в случае наложения шумов и перекрестных помех. Отдельные устройства шифрования для ведущего и ведомого PHY создают существенно некоррелированные потоки данных между двумя встречными символьными потоками в каждой паре проводов.

Топология линий 1000BaseT показана на рис. 8.23. Термин "TDX<7:6>" обозначает два наиболее значимых бита в байте данных перед кодированием и передачей, а "RDX<7:6>" — те же два бита после приема и декодирования.



H — гибридный подавляющий приемопередатчик
T — передающее кодирующее устройство
R — приемное декодирующее устройство
Четыре кодовых символа PAM5 = одна кодовая группа 4D-PAM5

Рис. 8.23. Топология линий 1000BaseT

Восстановление частоты синхронизации и временных циклов "ведущий/ведомый" в сущности не отличается от 1000BaseT2 (Рис. 8.24). То, какой из сетевых адаптеров будет ведущим (обычно это сетевой адаптер в многопортовом промежуточном сетевом узле), а какой — ведомым, определяется в процессе автосогласования.

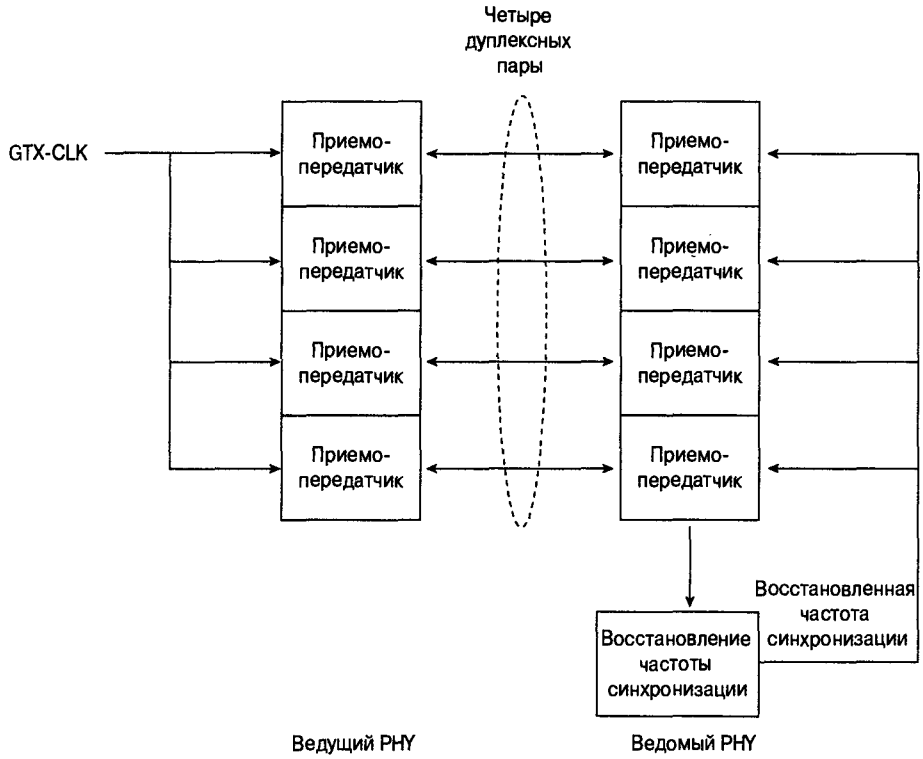


Рис. 8.24. Настройка временных циклов "ведущий/ведомый" в 1000BaseT

Каждый переданный фрейм помещен между признаками начала и конца потока. В межфреймовых промежутках временной цикл сохраняется посредством непрерывной передачи IDLE символов по каждой паре проводов. 1000BaseT поддерживает как полудуплексный, так и дуплексный режимы.

1000BaseX

Все три версии 1000BaseX поддерживают дуплексную двоичную передачу на скорости 1250 Мбит/с по двойному оптоволоконному кабелю или двум парам STP (Рис. 8.25). Кодирование передаваемых сигналов осуществляется по схеме ANSI Fibre Channel 8B/10B. Каждый 8-битовый байт данных преобразуется в 10-битовую кодовую группу для побитовой передачи. Подобно ранним версиям Ethernet, каждый фрейм данных инкапсулируется на физическом уровне перед передачей, а в межфреймовых интервалах синхронизация канала поддерживается путем постоянной передачи кодовых групп IDLE. Все физические уровни 1000BaseX поддерживают как полудуплексный, так и дуплексный режимы.

Принципиальные различия между версиями 1000BaseX касаются в среды передачи и разъемов, поддерживаемых отдельными версиями и, при использовании оптоволоконного кабеля, длины волны оптического сигнала (табл. 8.3).

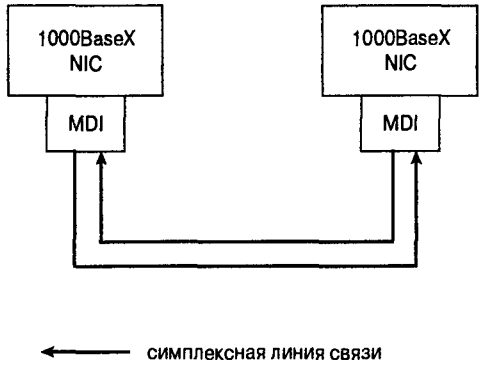


Рис. 8.25. Конфигурация канала 1000BaseX

Таблица 8.3. Конфигурации канала, поддерживаемые спецификациями 1000BaseX

Конфигурация канала	1000BaseCX	1000BaseSX (длина волны 850 нм)	1000BaseLX (длина волны 1300 нм)
150 Ом, STP	Да	Нет	Нет
многомодовый оптоволоконний кабель 125/62,5 мкм[1]	Нвт	Да	Дв
многомодовый оптоволоконний кабель 125/50 мкм	Нет	Да	Дв
одномодовый оптоволоконний кабвль 125/10 мкм	Нет	Нет	Да
Разъемы	IEC style 1 или Fibrв Channel style 2	SFF MT-RJ или Duplex SC	SFF MT-RJ или Duplex SC

[1] 125/62,5 мкм относится к плакированному диаметру и диаметру жилы оптоволоконного кабеля.

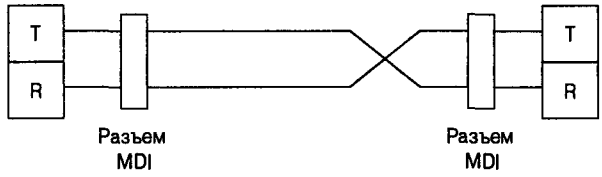
Требования к пересечениям сетевых кабелей

Совместимость линий связи требует, чтобы передатчики на каждом конце канала были соединены с получателями на другом ее конце. Однако поскольку кабельные разъемы на обоих концах канала настроены одинаково, проводники должны пересекаться в некоторой точке, чтобы выход передатчика всегда был подключен ко входу получателя.

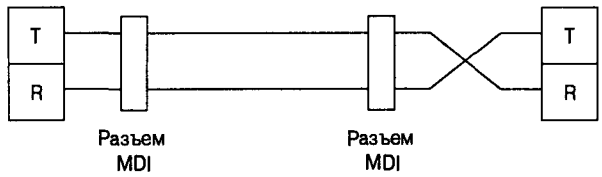
К сожалению, когда это требование впервые предъявили к разработчикам 10BaseT, в IEEE 802.3 не было внесено четких правил относительно того, где должно располагаться пересечение проводов: внутри кабеля (Рис. 8.26, а) или в середине устройства (Рис. 8.26, б).

Вместо этого в IEEE 802.3 определены следующие два правила и две рекомендации.

- Количество пересечений во всех многожильных кабелях должно быть нечетным.
- Если PHY имеет внутреннее пересечение, то его MDI должен быть явно помечен символом "X".



(а) Пересечение внутри кабеля



(б) Внутреннее пересечение

Рис. 8.26. Варианты пересечения проводов

- Реализация всех пересечений внутри устройств необязательна.
- Если DTE соединено с портом повторителя или коммутатора, то рекомендуется поместить пересечение внутри порта DCE.

В результате порты большинства DCE были оборудованы PMD со схемами внутреннего пересечения, а устройства DTE имели PMD без внутренних пересечений. Вследствие этого появилось следующее неписаное "правило установки".

- DTE к DCE подключается прямым кабелем, а DTE к DTE и DCE к DCE — кабелем с пересечением.

Однако данное правило применимо не ко всем версиям Ethernet, разработанным после 10BaseT. В настоящее время правила подключения сформулированы следующим образом.

- Во всех оптоволоконных системах применяются кабели с внутренними пересечениями.
- Во всех системах 100Base используется витая пара по тем же правилам и рекомендациям, что и для 10BaseT.
- В некоторых сетевых адаптерах 1000BaseT есть внутренние пересечения, которые могут быть включены в ходе автосогласования. Если же таковых нет, то действуют правила и рекомендации для 10BaseT.

Системные требования

При таком разнообразии вариантов может показаться, что обновить существующую сеть или спланировать новую не составляет труда. Но это ложное впечатление. Не все варианты подходят для любой сети и не все версии и функции Ethernet доступны на рынке, даже если они описаны в стандартах.

Выбор компонентов и категории среды передачи для неэкранированной витой пары

Из сказанного выше очевидно, что сетевые адаптеры для неэкранированной витой пары обеспечивают скорости передачи 10 Мбит/с, 100 Мбит/с и 1000 Мбит/с. Для 10 Мбит/с и 1000 Мбит/с выбор сравнительно невелик: 10BaseT и 1000BaseT.

Хотя для передачи на скорости 100 Мбит/с описаны три типа сетевых UTP-адаптеров, рынок сузил этот выбор до одного — 100BaseTX, который получил широкое распространение в первой половине 1995 года.

- К моменту появления на рынке продуктов 100BaseT4 спецификация 100BaseTX уже прочно заняла на нем свое место, а дуплексный режим 100BaseT4 находился только в процессе разработки.
- Стандарт 100BaseT2 был утвержден только весной 1997 года, что в современных условиях рынка было слишком поздно. В результате продукты 100BaseT2 так и не были выпущены.

Для UTP было разработано также несколько вариантов среды передачи: категории 3, 4, 5 и 5E. Различия между ними заключаются в стоимости кабеля и скорости передачи, которые тем больше, чем выше категория. Однако скорость передачи и стоимость не должны быть решающими факторами при выборе категории прокладываемого кабеля. С учетом будущих потребностей относительно скорости передачи не следует выбирать кабель ниже категории 5, а если речь идет о гигабитовых скоростях, то, возможно, и 5E.

- Стоимость прокладки, как правило, для всех типов четырехпарного UTP-кабеля одинакова.
- Стоимость замены имеющегося кабеля (удаление старого и прокладки нового) обычно выше, чем стоимость прокладки.
- UTP-кабели обладают обратной совместимостью. Кабель высшей категории поддерживает сетевые адаптеры низшей категории, но не наоборот.
- Срок физического износа UTP-кабеля (десятки лет) намного больше, чем срок морального износа подключенного к нему оборудования.

Автосогласование — дополнительный метод автоматической настройки режимов работы канала

Назначение автосогласования состоит прежде всего в том, чтобы найти способ обмена данными между двумя сетевыми адаптерами, подключенными к одному UTP-каналу, независимо от того, принадлежат ли они к одной версии Ethernet и работают ли в одном режиме.

Автосогласование выполняется полностью на физическом уровне во время инициации линии связи без дополнительного привлечения протоколов MAC или высших уровней. Автосогласование позволяет сетевым UTP-адаптерам выполнить следующие операции.

- Сообщить другому сетевому адаптеру о своей версии Ethernet и дополнительных возможностях.
- Подтвердить прием и определить общие режимы работы у этих сетевых адаптеров.
- Отказаться от режимов работы, не поддерживаемых вторым адаптером.
- Настроить каждый адаптер на режим работы наивысшего уровня, поддерживаемый обоими устройствами.

Автосогласование является дополнительной функцией 10BaseT, 100BaseTX и 100BaseT4 и обязательной для 100BaseT2 и 1000BaseT. В табл. 8.4 перечислены стандартные уровни приоритета (высший уровень — высший приоритет) для сетевых UTP-адаптеров Ethernet.

Таблица 8.4. Стандартные уровни выбора для автосогласования сетевых UTP-адаптеров

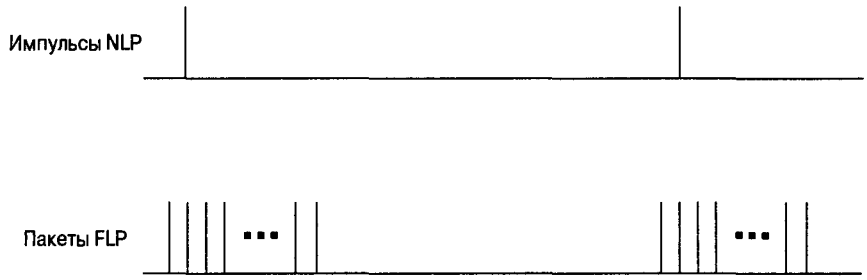
Уровень	Режим работы	Максимальная скорость передачи, Мбит/с[1]
9	1000BaseT, дуплексный	2000
8	1000BaseT, полудуплексный	1000
7	100BaseT2, дуплексный	200
6	100BaseTX, дуплексный	200
5	100BaseT2, полудуплексный	100
4	100BaseT4, полудуплексный	100
3	100BaseTX, полудуплексный	100
2	10BaseT, дуплексный	20
1	10BaseT, полудуплексный	10

[1] Поскольку дуплексный режим обеспечивает одновременную двунаправленную передачу, максимальная скорость передачи для этого режима вдвое превышает скорость полудуплексной передачи.

Функция автосогласования сетевых UTP-адаптеров использует модифицированную импульсную последовательность 10BaseT для проверки целостности линии, в которой обычные канальные импульсы заменяются пакетами скоростных канальных импульсов (Fast Link Pulses — FLP), как показано на рис. 8.27. Каждый пакет импульсов является перемежающейся последовательностью синхронизационных сигналов и сигналов данных, где биты данных определяют режимы работы, поддерживаемые передающим сетевым адаптером, а также несут информацию, используемую механизмом установления связи при автосогласовании. Если второй сетевой адаптер совместим с первым, то но не имеет функции автосогласования и он опознается при помощи функции параллельного распознавания. Сетевой адаптер, не отвечающий на пакеты скоростных канальных импульсов и возвращающий только нормальные импульсы, считается полудуплексным адаптером 10BaseT.

На первый взгляд может показаться, что при автосогласовании всегда выбирается узел, поддерживаемый сетевым адаптером с более ограниченными функциями. Это действительно может иметь место, если оба сетевых адаптера используют одинаковую процедуру кодирования и настройки канала. Например, если оба сетевых адаптера от-

носится к 100BaseTX, но только один из них поддерживает дуплексные операции, то будет выбран полудуплексный режим 100BaseTX. К сожалению, различные версии 100Base не совместимы друг с другом на скорости 100 Мбит/с, и сетевой адаптер 100BaseTX с дуплексным режимом будет после автосогласования с сетевым адаптером 100BaseT4 работать в полудуплексном режиме 10BaseT.



NLP — нормальный канальный импульс
FLP — скоростной канальный импульс

Рис. 8.27. При инициации линии связи нормальные канальные импульсы заменяются пакетами скоростных канальных импульсов автосогласования

Автосогласование сетевых адаптеров 1000BaseX подобно аналогичной процедуре для UTP-устройств, за исключением того, что оно применяется только к устройствам, совместимым с 1000BaseX, и в настоящее время ограничивается полудуплексным или дуплексным режимом и направлением сигналов управления потоком.

Возможная альтернатива высокоскоростных каналов в модернизированных сетях CSMA/CD — сетевые коммутаторы

Сетевые коммутаторы по доступной цене появились на рынке во второй половине 90-х годов прошлого века и потеснили повторители в крупных сетях. Повторители могут принимать фреймы только по очереди, пересылая их затем всем активным портам (кроме того, из которого фрейм был получен), а коммутаторы имеют следующие возможности.

- MAC-порты с буферами ввода/вывода фреймов, надежно изолирующие порт от других данных, посылаемых одновременно или с других портов коммутатора.
- Несколько внутренних маршрутов данных, что позволяет передавать сразу несколько фреймов между разными портами.

Эти отличия могут показаться незначительными, но они имеют решающее значение в работе сети. Поскольку каждый порт обеспечивает доступ к высокоскоростному сетевому мосту (коммутатору), коллизионный домен разбивается на несколько небольших доменов, состоящих всего из двух устройств — порта коммутатора и подключенного к нему сетевого адаптера (рис. 8.28). Более того, поскольку все устройства теперь принадлежат изолированным коллизионным доменам, доступная им полоса пропускания значительно увеличивается, к тому же без изменения скорости передачи.

Рассмотрим, например, рабочую группу из 48 станций с парой крупных файловых серверов и несколькими сетевыми принтерами, которая принадлежит сети CSMA/CD, а ее скорость передачи 100 Мбит/с. Средняя возможная полоса пропускания, не считая межфреймовых интервалов и восстановления после коллизий, составляет 100/50 = 2 Мбит/с (серверы печати не увеличивают объем передаваемых данных). Если та же рабочая группа находится в той же сети 10BaseT, но повторители в ней заменены коммутаторами, то пропускная способность, доступная для каждого пользователя, составит 10 Мбит/с.

Отсюда становится ясно, что чистая скорость передачи определяется конфигурацией сети.

Внимание!

Для того чтобы каждая конечная станция могла обмениваться данными на полной скорости, сетевые коммутаторы должны быть ненасыщенными (принимать и передавать данные на полной скорости из всех портов одновременно).

Многоскоростные сетевые адаптеры

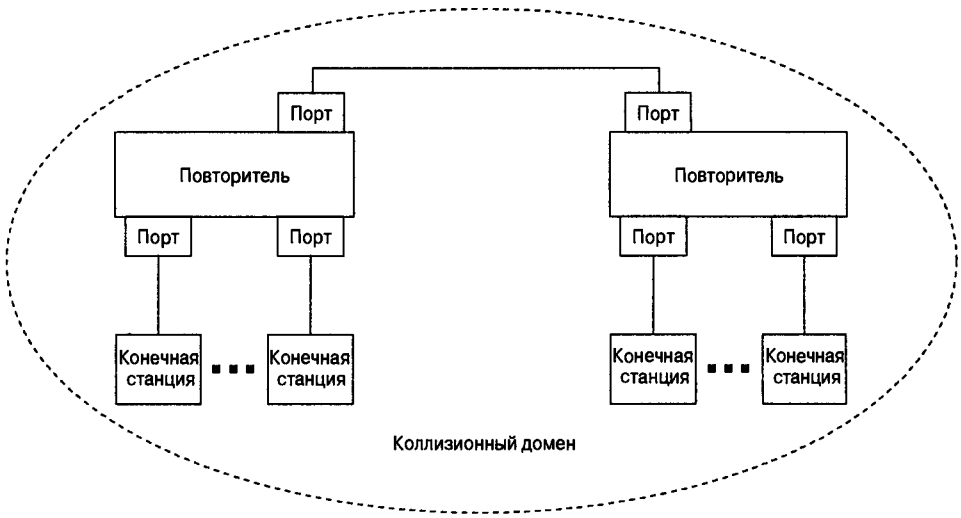
Автосогласование дало толчок к разработке недорогих многоскоростных сетевых адаптеров, поддерживающих, например, полу- и полнодуплексный режимы для 100BaseTX и 10BaseT. Благодаря многоскоростным сетевым адаптерам стала возможна поэтапная модернизация сети, в ходе которой полудуплексные конечные станции 10BaseT могут подключаться к дуплексным портам коммутаторов 100BaseTX без замены плат сетевых адаптеров в компьютере. Если же некоторым компьютерам потребуется бо́льшая пропускная способность, то их сетевые адаптеры можно заменить на такие, которые поддерживают дуплексный режим 100BaseTX.

Выбор компонентов и среды передачи для сети 1000BaseX

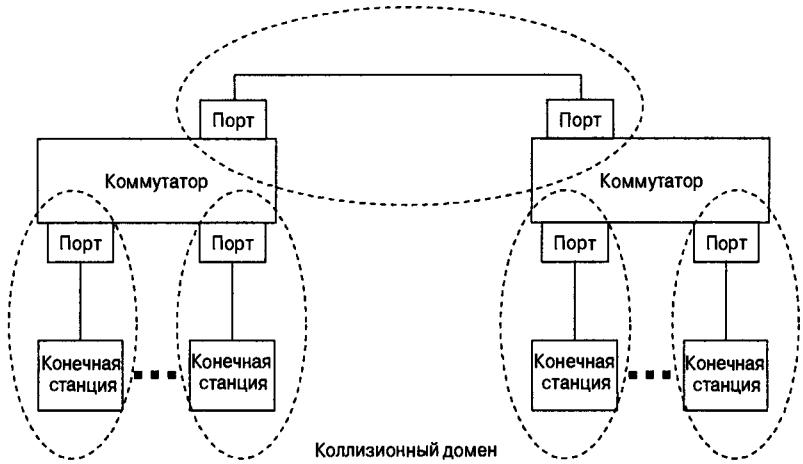
Хотя, согласно табл. 8.3, вариантов среды передачи для 1000BaseX весьма много, не все они равноправны. Рекомендуется придерживаться следующих правил.

- Сетевые адаптеры на обоих концах линии связи должны быть одинаковой версии 1000BaseX (CX, LX или SX), а разъемы линии связи — соответствовать разъемам сетевых адаптеров.
- Спецификация 1000BaseCX допускает разъемы стиля 1 и 2, однако стиль 2 предпочтительнее, поскольку некоторые разъемы стиля 1 не подходят для скорости 1250 Мбит/с. Линии связи 1000BaseCX предназначены для небольших сетей с использованием коммутационного шнура и ограничиваются 25 метрами.
- Спецификации 1000BaseLX и 1000BaseSX допускают как разъем SFF MT-RJ с малым форм-фактором, так и бо́льшие дуплексные SC-разъемы. Поскольку разъемы SFF MT-RJ примерно вдвое меньше дуплексных SC-разъемов, а пространство ограничено, то, вероятно, разъемы SFF MT-RJ получат бо́льшее распространение.
- Трансиверы 1000BaseLX, как правило, дороже трансиверов 1000BaseSX.

- Максимальная длина оптоволоконного кабеля зависит от длины передаваемой волны и модальной пропускной способности (МГц/км), зависящей от вида волокна (табл. 8.5).



(а) Сеть CSMA/CD с повторителями



(б) Сеть CSMA/CD с коммутаторами

Рис. 8.28. Если заменить повторители коммутаторами, то в коллизионных доменах останется лишь по два сетевых адаптера

Таблица 8.5. Максимальная длина часто применяемых оптоволоконных кабелей

Диаметр жилы/модальная полоса пропускания	1000BaseSX (длина волны 850 нм)	1000BaseLX (длина волны 1300 нм)
Многомодовое оптоволокно, 62,5 мкм (200/500) МГц/км	275 м	550 м[1]
Многомодовое оптоволокно, 50 мкм (400/400) МГц/км	500 м	550 м[1]
Многомодовое оптоволокно, 50 мкм (500/500) МГц/км	550 м	550 м[1]
Одномодовое оптоволокно, 10 мкм	Не поддерживается	5000[1]

[1] Для соединения трансиверов 1000BaseSX с некоторыми многомодовыми оптоволоконными кабелями иногда требуется коммутационный шнур с возможностью переключения режимов.

Длины кабелей, указанные в табл. 8.5, соответствуют стандарту IEEE 802.3. Однако на практике максимальная длина многомодового оптоволоконного кабеля диаметром свыше 62,5 мкм для LX-трансиверов составляет приблизительно 700 м, а некоторые LX-трансиверы могут работать с одномодовыми оптоволоконными кабелями длиной 10000 м.

Многоскоростные сети Ethernet

Учитывая возможности, проиллюстрированные примером в предыдущем разделе, неудивительно, что большинство крупных сетей Ethernet являются комбинированными, как в отношении скорости передачи, так и в отношении используемых сред передачи. Кабельная модель такой сети показана на рис. 8.29.

Кабельная модель ISO/IEC 11801 представляет собой сетевую модель, на которой основаны стандарты IEEE 802.3.

- **Распределитель сети кампуса. Сетью Кампуса** называют сеть, которая находится в группе из нескольких зданий, расположенных на сравнительно небольшой территории. Распределитель кампуса представляет собой центральную точку его опорной сети и является точкой его телекоммуникационной связи с внешним миром. В локальных сетях Ethernet распределитель кампуса обычно представляет собой гигабитовый коммутатор с телекоммуникационным интерфейсом.
- **Распределитель здания.** Точка связи сети, расположенной в здании, с опорной сетью кампуса. В сетях Ethernet распределитель здания обычно представляет собой коммутатор со скоростями передачи 1000/100 Мбит/с или 1000/100/10 Мбит/с.
- **Этажный распределитель.** Точка связи сети, расположенной на этаже, с распределителем здания. Стандарт ISO/IEC 11801 рекомендует устанавливать как минимум один распределитель на каждые 1000 м^2 офисной площади и, если возможно, дополнительный распределитель для каждого этажа. Этажный распределитель Ethernet, как правило, представляет собой коммутатор со скоростью передачи 1000/100/10 Мбит/с или 100/10 Мбит/с.

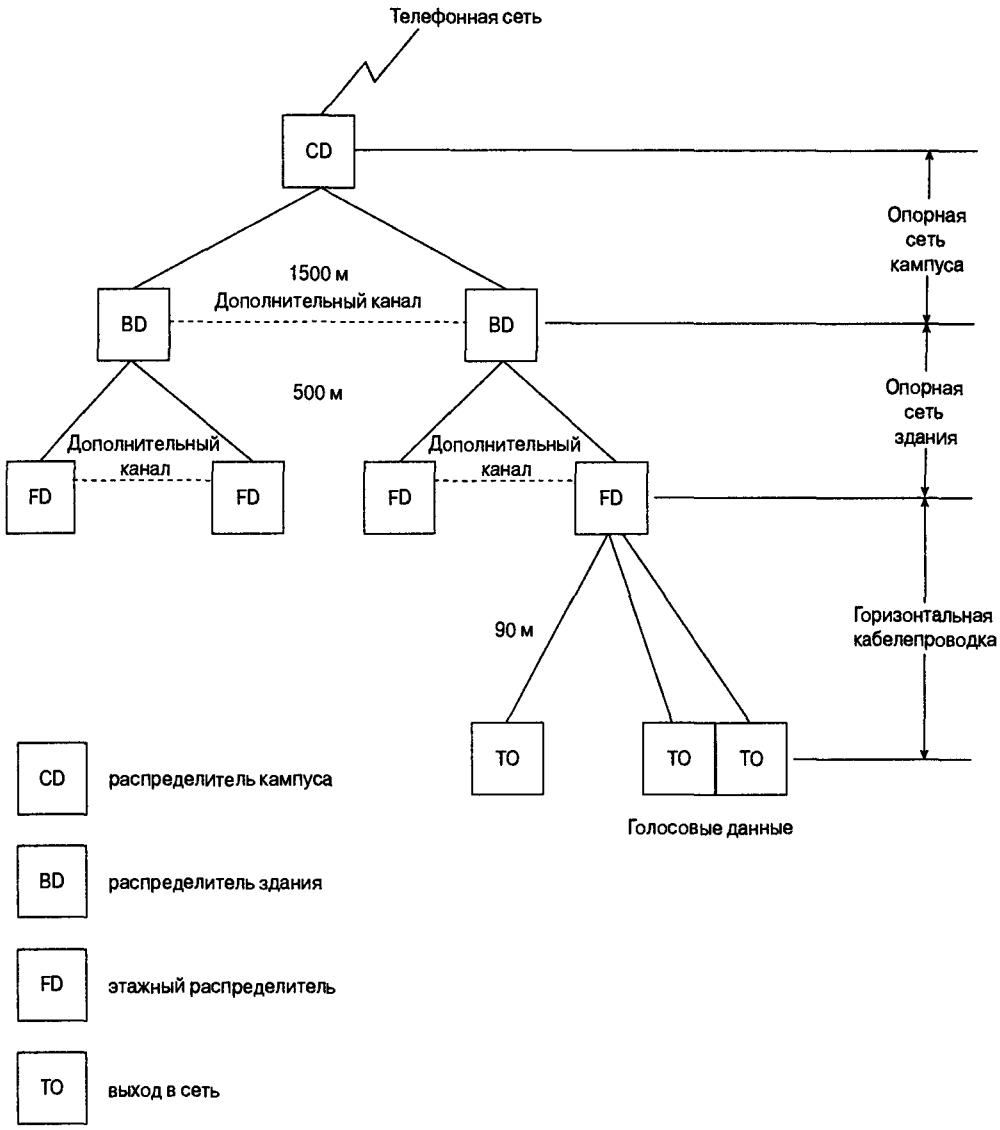


Рис. 8.29. Пример многоскоростной сетевой топологии — кабельная модель ISO/IEC 11801

- **Выход в сеть.** Точка связи персональных компьютеров, рабочих станций и серверов печати с сетью. Файловые серверы обычно расположены компактно и напрямую подключены к распределителю кампуса, здания или этажа, в зависимости от их назначения.
- **Кабель опорной сети кампуса.** Обычно это одно- или многомодовый оптоволоконный кабель, соединяющий распределители зданий с распределителем кампуса.
- **Кабель опорной сети здания.** Обычно это неэкранированная витая пара кадескриптории 5 или выше, либо многомодовый оптоволоконный кабель, соединяющий этажные распределители с распределителем здания.

- **Горизонтальная кабельная проводка.** Преимущественно неэкранированная витая пара кадескрипторории 5 или выше, хотя иногда используется оптоволоконный кабель.

Как и в случае выбора типа неэкранированной витой пары, выбор среды передачи и межсетевых узлов должен осуществляться с учетом скоростей передачи, которые потребуются в будущем, и темпов устаревания сетевых элементов, хотя предсказать их достаточно сложно. За 90-е годы XX века скорость передачи данных в локальных сетях возросла в 100 раз.

Это, однако, не означает, что все или даже некоторые конечные станции и линии связи между ними обязательно потребуют гигабитовой пропускной способности. Однако это означает, что сетевым узлам, расположенным ближе к центральной точке сети (в частности, большинству распределителей кампуса и здания), такая пропускная способность все же потребуется, а все этажные распределители должны работать со скоростью не менее 100 Мбит/с. Это также означает, что ни один сетевой коммутатор не должен блокироваться, все порты должны поддерживать дуплексный режим, а все новые опорные сети кампуса должны создаваться на основе одномодового оптоволоконного кабеля.

Объединение каналов и создание высокоскоростных сетевых магистралей

Объединение каналов (link aggregation) представляет собой недавно появившуюся дополнительную функцию MAC-подуровня и позволяющую объединить несколько физических каналов связи в одну логическую высокоскоростную магистраль. Это дает возможность более чем на порядок повысить действительную скорость передачи данных между двумя сетевыми узлами путем объединения нескольких линий передачи данных.

Объединение каналов может оказаться весьма экономным способом обеспечить высокоскоростное соединение в локальных сетях Ethernet, достигших предельных размеров при скорости 100 Мбит/с, но не требующих гигабитовой пропускной способности, по крайней мере, в ближайшее время. Предположим, например, что максимальная протяженность линии связи на базе многомодового оптоволоконного кабеля диаметром 62,5 мкм равна 2000 м при скорости передачи 100 Мбит/с, а для многих опорных сетей кампуса был использован оптоволоконный кабель. Казалось бы, весьма логично использовать эти же линии и для работы на скорости 1000 Мбит/с, однако максимальная длина многомодового оптоволоконного кабеля составляет всего 700 м, и только при использовании спецификации 1000BaseLX. Если имеющиеся линии длиннее 700 м, то объединение n таких каналов обеспечит эффективную скорость передачи в $100n$ Мбит/с.

Объединение каналов следует рассматривать как вариант конфигурирования сети, используемый преимущественно для таких немногочисленных соединений, как "коммутатор-коммутатор" или "коммутатор-файловый сервер", которым требуются более высокие скорости передачи, чем те, которые обеспечиваются одиночными каналами. Эту функцию также можно применять для повышения надежности критически важных линий. В случае повреждения линии связи объединенный канал быстро перенастраивается (обычно не более чем за 1 секунду), а риск дублирования или изменения порядка фреймов незначителен.

Объединение каналов не влияет ни на формат фреймов данных IEEE 802.3, ни на форматы высших уровней в стеке протоколов. Оно сохраняет обратную совместимость с устройствами, не поддерживающими такого объединения и может применяться не-

зависимо от скорости Ethernet (впрочем, для 10 Мбит/с объединение каналов не имеет смысла, поскольку установка пары сетевых адаптеров 100 Мбит/с обходится дешевле). Объединение каналов возможно только для параллельных линий связи "точка-точка", поддерживающих дуплексный режим на одной и той же скорости.

Управление сетью

Все высокоскоростные спецификации Ethernet содержат определения управляемых объектов и агентов управления, совместимые с простым протоколом сетевого управления (Simple Network Management Protocol — SNMP). Их можно использовать для сбора статистической информации о работе сетевых узлов и для выполнения функций управления сетью. Поскольку информация о пользователях в лучшем случае эпизодическая и всегда поступает с большими задержками, во всех крупных сетях должны быть сконфигурированы, как минимум, управляемые коммутаторы и сетевые серверы. Это позволяет обнаруживать потенциальные проблемы и "узкие места" еще до того, как они вызовут серьезные ухудшения работы сети.

Переход на высокоскоростные сети

Как следует из сказанного выше, после проведения модернизации существующих сетей обычно не требуется полностью заменять оборудование или среду передачи. Однако для осуществления такого процесса необходимо знание существующей конфигурации сети и готовность к потенциальным проблемам. Это означает, что должна функционировать система управления сетью, а схема расположения кабелей должна быть точной и доступной. Определение типа и доступности линии связи после того, как кабели проложены под землей, в стене или по кабелепроводу, весьма непросто и требует значительного количества времени .

Линии связи часто являются сдерживающим фактором при модернизации сети. Существующие кабельные линии кадескриптории 5 должны поддерживать все скорости Ethernet от 10 Мбит/с до 1000 Мбит/с, хотя поддержка гигабитовых скоростей нуждается в тестировании. Если же в сети используется только кабель кадескриптории 3, то перед переходом на скорость передачи 1000 Мбит/с некоторые линии потребуется заменить. Аналогичная ситуация возникает с одно- и многомодовым оптоволоконным кабелем. Не следует применять многомодовое для всех опорных сетей. С другой стороны, одномодовый оптоволоконный кабель не только позволяет создавать линии длиной до 10000 м со скоростью передачи 1000 Мбит/с, но и сможет в будущем поддерживать использование магистралей со скоростью передачи в десятки гигабит.

Замену коммутаторов можно начинать сразу же, как только будут проложены все необходимые линии связи. Имеющиеся коммутаторы, служащие распределителями кампуса и здания, часто можно повторно использовать в качестве, соответственно, распределителей здания и этажа. Чтобы продлить срок использования конечных станций, обычно заменяют сетевые адаптеры. Аналогичные соображения используются и для других элементов сети.

Резюме

В начале этой главы был приведен обзор технологии Ethernet, элементов сетей и взаимосвязи Ethernet с семиуровневой эталонной моделью OSI. Кроме того, были

описаны требования совместимости между уровнями MAC и PHY (MAC-уровнем и физическим уровнем).

Ниже приведены основные функции MAC-уровня.

- **Инкапсуляция данных.** Сборка фрейма в соответствии со стандартным форматом перед началом передачи и обратное преобразование фрейма после получения и проверки на наличие ошибок передачи.
- **Управление доступом к среде передачи.** Эта функция выполняется в обязательном полудуплексном и в дополнительном дуплексном режимах CSMA/CD.

Выше были рассмотрены две дополнительные функции MAC-уровня и соответствующие им форматы фреймов. Использование дескрипторов виртуальных сетей VLAN позволяет задавать сетевым узлам как логические, так и физические адреса, и назначать фреймам приоритеты при передаче. Специальный формат фрейма-паузы, используемый для краткосрочного контроля потока, предусмотрен стандартом, однако в настоящей книге не описан, поскольку он использование фрейма-паузы является автоматической функцией MAC-уровня, вызываемой при необходимости во избежание переполнения входного буфера.

При обсуждении уровня PHY были описаны сигнальные процедуры, а также требования и ограничения среды передачи для следующих спецификаций:

- 10BaseT;
- 100BaseTX, 100BaseT4 и 100BaseT2;
- 1000BaseT, 1000BaseCX, 1000BaseLX и 1000BaseSX.

Хотя спецификация 100BaseFX отдельно не рассматривалась, она использует те же сигнальные процедуры, что и 100BaseTX, с той лишь разницей, что вместо неэкранированной витой пары применяется оптоволоконный кабель.

Остальные разделы главы были посвящены описанным ниже особенностям построения локальной сети на основе витой пары и на базе оптоволоконного кабеля.

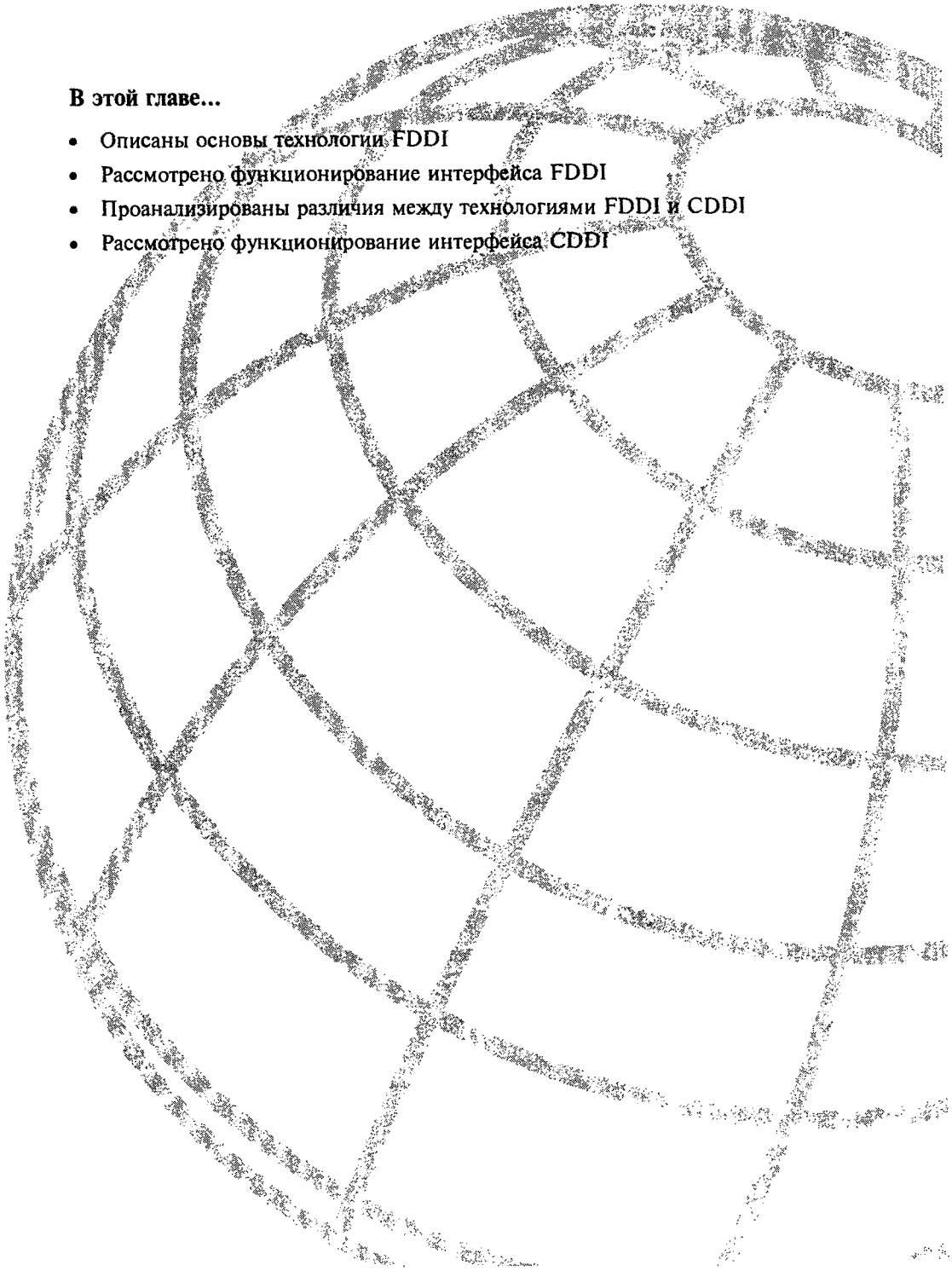
- Пересечение линий связи в сетях на базе неэкранированной витой пары.
- Соответствие подуровня PMD и среды передачи для получения требуемой скорости передачи.
- Создание высокоскоростных логических магистралей путем объединения каналов.
- Применение сетей с несколькими скоростями передачи.

Контрольные вопросы

1. Следует ли модернизировать все сети 10BaseT до 100 Мбит/с? Почему?
2. Какая версия (версии) 100Base предпочтительнее? Почему?
3. Какая версия (версии) 1000Base предпочтительнее? Где их следует применять?
4. Какой тип кабеля следует использовать для создания новой сети и для модернизации уже существующей? Почему?
5. Как определить, нуждается ли сеть в модернизации? С чего начать?

В этой главе...

- Описаны основы технологии FDDI
- Рассмотрено функционирование интерфейса FDDI
- Проанализированы различия между технологиями FDDI и CDDI
- Рассмотрено функционирование интерфейса CDDI



Глава 9

Интерфейс FDDI

Введение

Распределенный интерфейс передачи данных по оптоволоконным каналам (Fiber Distributed Data Interface — FDDI) определяет передачу данных в локальной сети с двойным кольцом и передачу маркера по оптоволоконному кабелю при скорости 100 Мбит/с. Благодаря большей пропускной способности и поддержке больших, чем электрические провода, расстояний, интерфейс FDDI часто используется в скоростных магистралях. Следует отметить, что сравнительно недавно появилась аналогичная технология, позволяющая передавать данные со скоростью 100 Мбит/с по электрическим проводам — т.н. распределенный проводной интерфейс передачи данных (Copper Distributed Data Interface — CDDI). Интерфейс CDDI является реализацией протокола FDDI для витой пары. В настоящей главе основное внимание уделяется подробному описанию и принципам работы протокола FDDI, однако в ней также представлен обзор протокола CDDI.

В FDDI используется архитектура двойного кольца, в которой фреймы перемещаются по кольцам в противоположных направлениях (так называемая контрциркуляция). Двойное кольцо состоит из первичного и вторичного колец. В нормальном режиме данные передаются по первичному кольцу, а вторичное не используется. Как будет описано далее в этой главе, основное назначение двойного кольца состоит в обеспечении высокой надежности и безопасности. На рис. 9.1 показана контрциркуляция данных по первичному и вторичному кольцам FDDI.

Стандарты

Интерфейс FDDI был разработан в середине 80-х годов прошлого века комитетом по стандартизации X3T9.5 при Американском национальном институте стандартов (ANSI). В то время высокоскоростные инженерные рабочие станции локальных сетей, основанных на технологиях Ethernet и Token Ring стали испытывать недостаток в пропускной способности. Требовалась новая среда передачи данных по локальной сети, которая бы смогла поддерживать такие рабочие станции и их новые распределенные приложения. Одновременно значительно возросло значение надежности сетей, так как системные администраторы стали перемещать в сети важные приложения с больших компьютеров. Для удовлетворения этих потребностей был разработан протокол

FDDI. Институт ANSI предложил протокол FDDI Международной организации по стандартизации (ISO), которая создала международный вариант FDDI, полностью совместимый со стандартной версией ANSI.

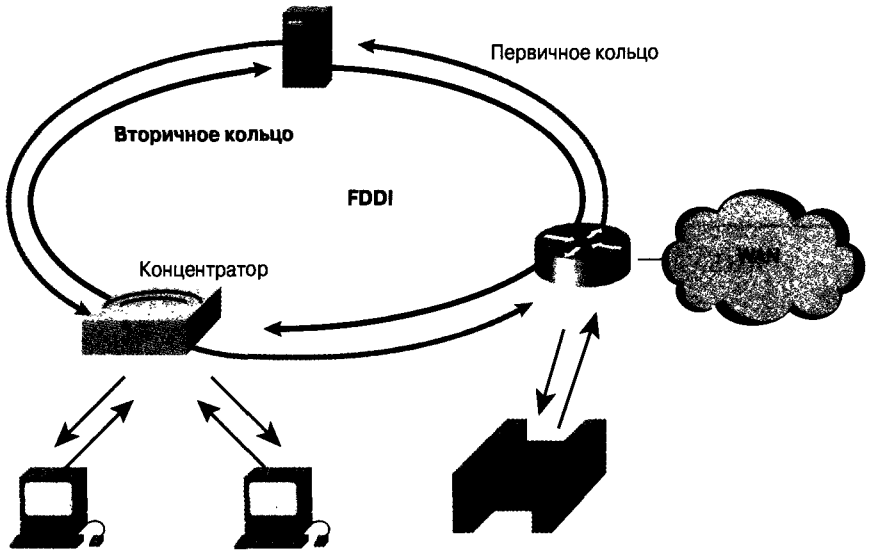


Рис. 9.1. В протоколе FDDI используется и первичное, и вторичное кольцо, и данные по ним передаются в противоположных направлениях

Среда передачи интерфейса FDDI

В качестве основной среды передачи интерфейс FDDI использует оптоволоконный кабель, но он может работать и с электрическим кабелем. Как уже отмечалось, в последнем случае FDDI называется распределенным проводным интерфейсом передачи данных (Copper Distributed Data Interface — CDDI). По сравнению с электрическим, у оптоволоконного кабеля есть несколько преимуществ. В особенности это касается безопасности, надежности и скорости: у оптоволоконной среды эти параметры лучше, поскольку оптоволокно не излучает электромагнитных волн. Если физическая среда (электрический кабель) излучает такие сигналы, то их можно записать, и, следовательно, существует опасность несанкционированного доступа к передаваемым данным. Кроме того, оптоволоконный кабель невосприимчив к радио- и электромагнитным помехам. Исторически сложилось так, что оптоволоконные линии связи обеспечивали более высокую пропускную способность, чем электрические кабели, хотя последние технологические достижения сделали возможной передачу данных по проводам со скоростью 100 Мбит/с. Кроме того, интерфейс FDDI позволяет располагать станции, соединенные многомодовым оптоволоконным кабелем, на расстоянии до 2 км друг от друга, а при использовании одномодового кабеля — на еще больших расстояниях.

Протокол FDDI допускает использование двух видов оптоволоконного кабеля: одно- и многомодовый. *Мода* представляет собой луч света, который входит в волокно под определенным углом. В *многомодовом* волокне источниками света служат светодиоды, а в *одномодовом* используются лазеры.

Многомодовый оптоволоконный кабель позволяет передавать сразу несколько мод света. Поскольку эти моды входят в волокно под разными углами, они достигают конца кабеля в разное время. Эта особенность называется *модовой дисперсией.* Модовая дисперсия ограничивает пропускную способность и расстояние, на которое можно передавать сигналы по многомодовому кабелю. По этой причине многомодовое волокно используется, как правило, для сетей, расположенных в пределах одного здания или на ограниченной территории.

Одномодовое волокно позволяет передавать только одну моду света, так что модовая дисперсия в этом случае отсутствует. Поэтому одномодовый кабель обеспечивает значительно более высокую скорость передачи на гораздо большие расстояния. Это позволяет использовать его для связи между зданиями и на больших территориях.

На рис. 9.2 показан одномодовый кабель, использующий в качестве источника света лазер, и многомодовый кабель, использующий светодиод.

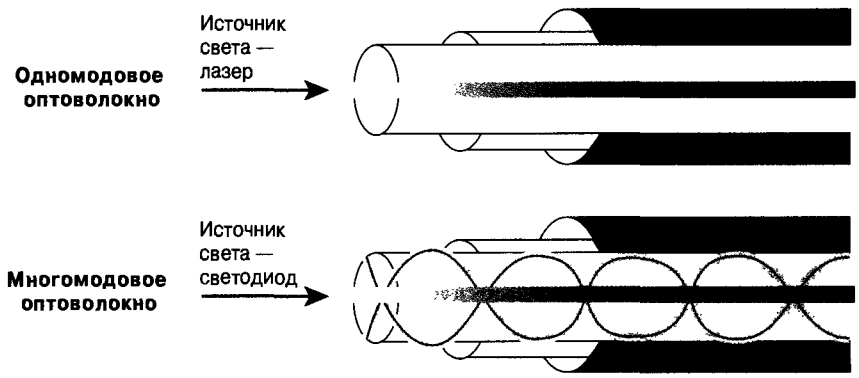


Рис. 9.2. В одно- и многомодовых кабелях используются разные источники света

Спецификации интерфейса FDDI

Протокол FDDI определяет физический уровень эталонной модели OSI и ту ее часть, которая касается доступа к среде передачи. На самом деле FDDI не является единой спецификацией, а представляет собой четыре отдельные спецификации, каждая из которых имеет свое назначение. Вместе они обеспечивают возможность высокоскоростной передачи данных протоколов более высокого уровня, таких как TCP/IP и IPX, по оптоволоконному кабелю.

В состав FDDI входят следующие четыре спецификации: MAC, PHY, PMD и SMT. *MAC*-спецификация *(Media Access Control — MAC)* определяет доступ к среде передачи, включая формат фрейма, обработку маркеров, адресацию, алгоритмы расчета избыточного циклического кода (Cyclic Redundancy Check — CRC) и механизмы исправления ошибок. Спецификация PHY *(PHYsical layer protocol)* описывает процедуры кодирования и декодирования данных, требования синхронизации, формирование фрейма и другие функции. Спецификация *физической среды передачи (Physical-Medium Dependent — PMD)* определяет характеристики среды передачи, включая оптоволоконные линии связи, уровни мощности, частоту ошибок по битам, оптические компоненты и соединители. Спецификация *управления станцией (Station ManagemenT* — SMT*)* определяет конфигурацию станций протокола FDDI, конфигурацию кольца и средства управления им, включая добавление, удаление,

инициализацию станций и изоляцию сбойных станций, а также восстановление после сбоев, составление расписания и сбор статистических данных.

Связь интерфейса FDDI с эталонной моделью OSI аналогична описываемой в спецификациях IEEE 802.3 Ethernet и IEEE 802.5 Token Ring. Основное назначение интерфейса FDDI состоит в обеспечении взаимодействия между протоколами верхних уровней OSI и средой передачи, связывающей сетевые устройства. На рис. 9.3 показаны четыре спецификации FDDI, их отношения между собой и связь с определенным IEEE подуровнем управления логическим соединением (Logical Link Control — LLC). Подуровень LLC является компонентом 2-го (MAC) уровня эталонной модели OSI.

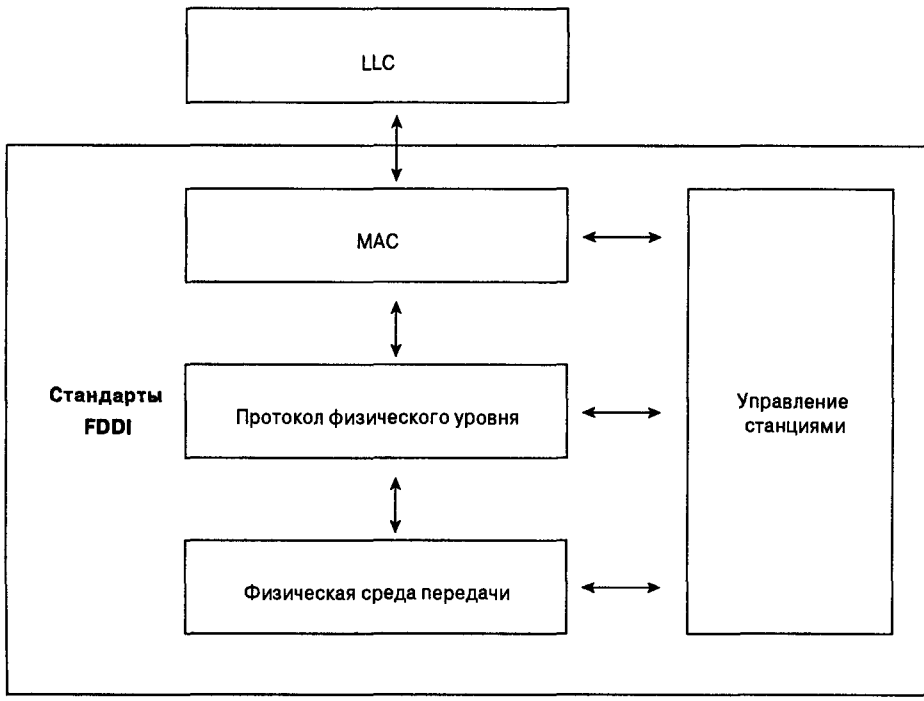


Рис. 9.3. Взаимовязь между спецификациями FDDI и иерархической моделью OSI

Типы подключения станций в протоколе FDDI

Одним из уникальных свойств интерфейса FDDI является возможность подключения FDDI-устройств несколькими способами. Спецификация FDDI определяет четыре типа устройств: однопортовая станция (Single-Attachment Station — SAS), двухпортовая станция (Dual-Attachment Station — DAS), однопортовый концентратор (Single-Attached Concentrator — SAC) и двухпортовый концентратор (Dual-Attached Concentrator — DAC).

Однопортовая станция SAS подключается через концентратор только к одному кольцу (первичному). Одним из основных преимуществ подключения устройств по схеме SAS является то, что отсоединение или выключение таких устройств не влияет на кольцо FDDI. Концентраторы будут более подробно рассмотрены ниже.

У каждой двухпортовой станции DAS в FDDI есть два порта, обозначаемые A и B. Через эти порты станция DAS подключается к кольцу FDDI. Таким образом, каждый порт обеспечивает подключение как к первичному, так и ко вторичному кольцу. Как будет показано в следующем разделе, устройства, подключенные по схеме DAS, в случае отсоединения или выключения оказывают влияние на кольца. На рис. 9.4 показаны порты A и B DAS-устройства FDDI, подключенные к первичному и вторичному кольцам.

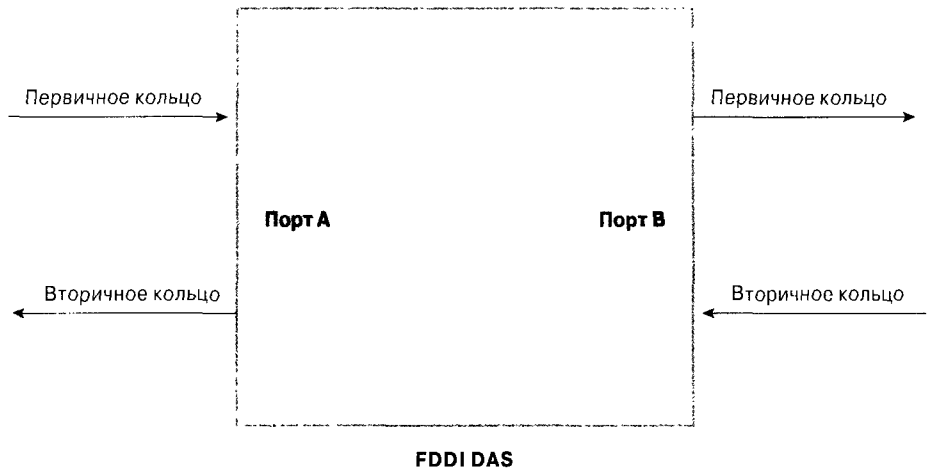


Рис. 9.4. Порты DAS-устройства FDDI соединены с первичным и вторичным кольцами

Концентратор FDDI (также называемый *двухпортовым концентратором — DAC*) представляет собой один из компонентов сети FDDI. Он непосредственно подключается к первичному и вторичному кольцам и гарантирует, что сбой или отключение одного из SAS-устройств не повлечет за собой сбой всего кольца. Это особенно важно в тех случаях, когда к кольцу подключены персональные компьютеры или другие часто отключаемые устройства. На рис. 9.5 показаны подключенные к кольцу FDDI станции SAS, DAS и концентратор.

Отказоустойчивость FDDI

Интерфейс FDDI обеспечивает несколько способов защиты от сбоев. Это, в частности, использование двойного кольца FDDI, оптического обходного переключателя и поддержка двойного подключения.

Двойное кольцо

Основным средством защиты от сбоев в FDDI является *двойное кольцо*. Если станция, подключенная к двойному кольцу, выходит из строя, отключается или повреждается кабель, то двойное кольцо автоматически сворачивается в одиночное (дублирует само себя). Когда кольцо сворачивается, топология двойного кольца превращается в топологию одиночного кольца. В этом состоянии данные продолжают передаваться по кольцу FDDI без снижения производительности. Эффект от сворачивания кольца FDDI показан на рис. 9.6 и 9.7.

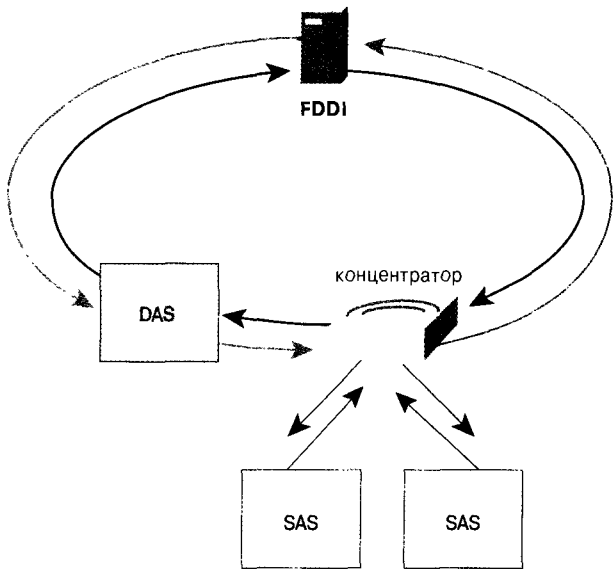


Рис. 9.5. Концентратор подключается как к первичному, так и ко вторичному кольцам

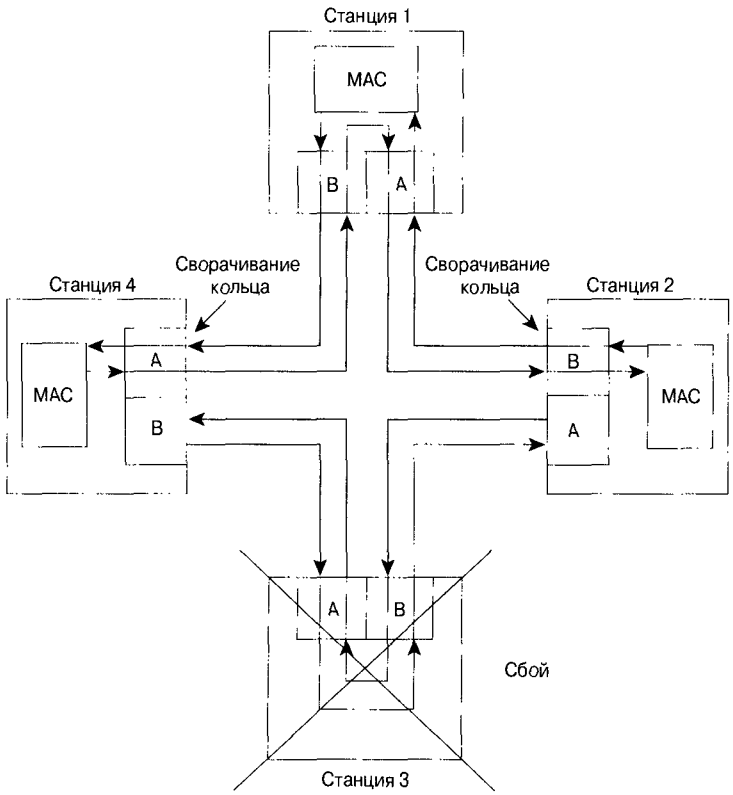


Рис. 9.6. Сворачивание кольца при сбое станции

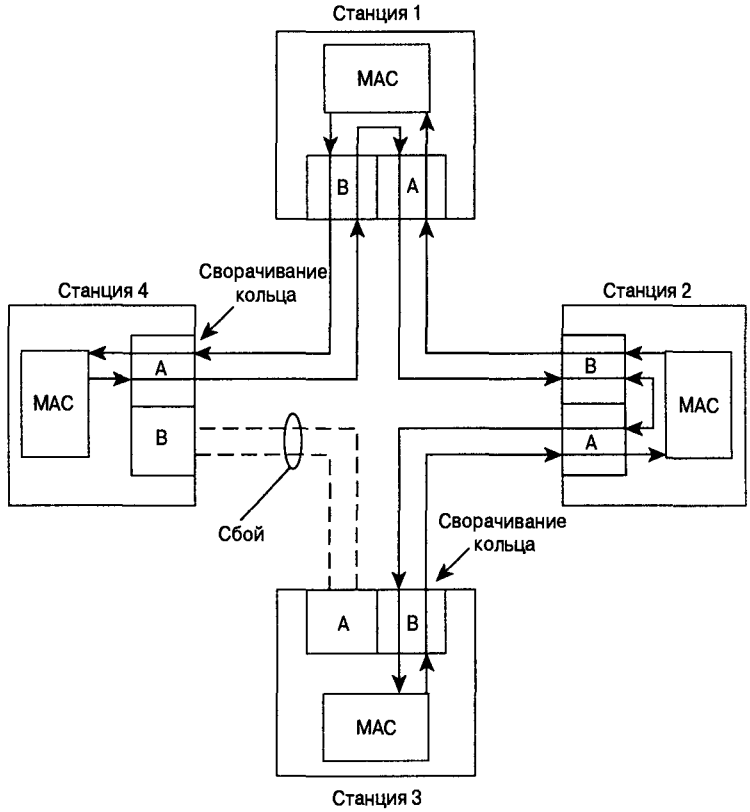


Рис. 9.7. Сворачивание кольца при повреждении кабеля

Если одна из станций выйдет из строя (рис. 9.6), устройства по обе ее стороны сворачивают кольцо, и оно превращается в одиночное. Для остальных станций в кольце сеть продолжает работать. При повреждении кабеля (рис. 9.7) сворачивание кольца происходит на устройствах по обеим сторонам поврежденного участка и сеть продолжает работать для всех станций.

Оптический обходной переключатель

Оптический обходной переключатель обеспечивает работу двойного кольца в случае выхода из строя одного из устройств. Он применяется для предотвращения сегментации кольца с одновременным исключением из него поврежденных станций. Оптический обходной переключатель выполняет эту функцию при помощи оптических зеркал, которые в нормальном режиме работы передают свет из кольца напрямую к DAC-устройству. Если на DAC-устройстве происходит сбой, например, выключение питания, то оптический обходной переключатель будет передавать свет через себя с помощью внутренних зеркал, сохраняя таким образом целостность кольца.

Преимуществом такого подхода является то, что в случае выхода устройства из строя кольцо не сворачивается. Работа оптического обходного переключателя в сети FDDI проиллюстрирована на рис. 9.8. Прохождение сетевых пакетов через оптический переключатель значительно отличается от обычной работы сети.

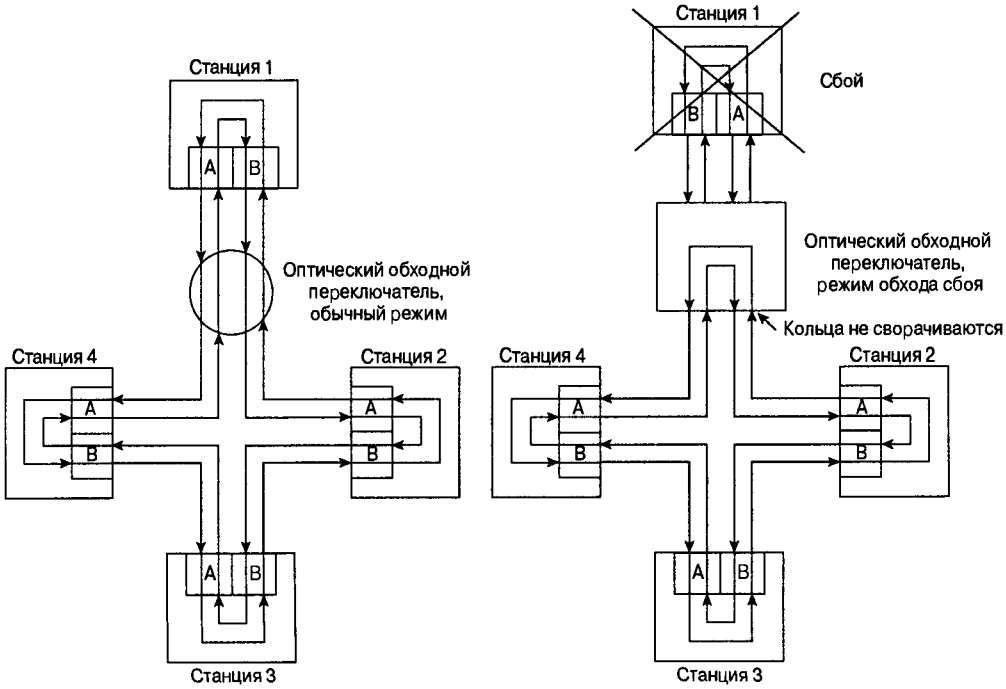


Рис. 9.8. Для поддержки работоспособности сети в оптическом обходном переключателе используются внутренние зеркала

Двойное подключение

Для критически важных устройств, таких как маршрутизаторы или мэйнфреймы, может использоваться метод защиты от сбоев, называемый *двойным* подключением *(dual homing)*, который обеспечивает работоспособность за счет избыточности. При двойном подключении критическое устройство подключается сразу к двум концентраторам. На рис. 9.9 показана конфигурация двойного подключения для таких устройств, как файловые серверы и маршрутизаторы.

Одна пара подключений к концентратору объявляется активной, другая — пассивной. Пассивное подключение находится в резерве на тот случай, если основное подключение (или концентратор) выйдет из строя. В этой ситуации пассивный канал автоматически активизируется.

Формат фрейма FDDI

Формат фреймов FDDI аналогичен формату фреймов в сети Token Ring. В этой области, как и во многих других, FDDI многое позаимствовал из более ранних технологий локальных сетей, таких как Token Ring. Максимальный размер фрейма FDDI составляет 4500 байтов. На рис. 9.10 показаны форматы фрейма данных и маркера.

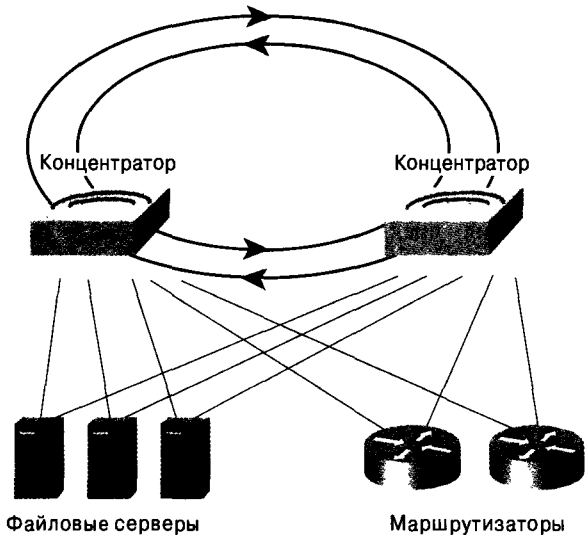


Рис. 9.9. Конфигурация двойного подключения гарантирует работоспособность устройств

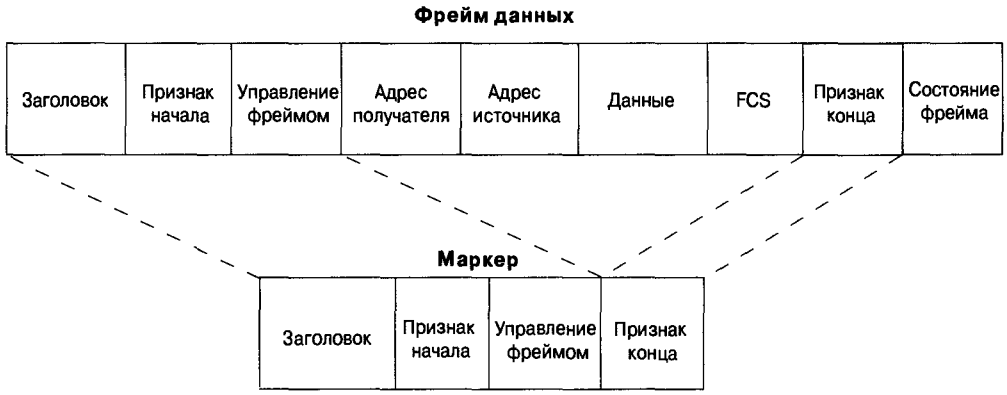


Рис. 9.10. Формат фрейма FDDI аналогичен формату фрейма Token Ring

Поля фрейма FDDI

Ниже приводится описание полей фрейма данных FDDI и Token Ring, показанных на рис. 9.10.

- **Заголовок.** Уникальная последовательность, сообщающая станции о поступлении фрейма.
- **Признак начала фрейма.** Указывает начало фрейма при помощи последовательности сигналов, отличной от остальной части фрейма.
- **Управление фреймом.** Управляющая информация, в том числе размер адресных полей и тип данных (асинхронные или синхронные).

- **Адрес получателя.** Одноадресатный, многоадресатный или широковещательный адрес. Как и во фреймах Ethernet и Token Ring, в FDDI длина адреса получателя составляет 6 байтов.
- **Адрес источника.** Определяет станцию, отправившую фрейм. Как и в сетях Ethernet и Token Ring, в протоколе FDDI длина адреса источника данных составляет 6 байтов.
- **Данные.** Информация, предназначенная для протокола высшего уровня, либо управляющая информация.
- **Контрольная последовательность фрейма** (Frame Check Sequence — FCS). Вычисляется на станции-источнике. В это поле заносится вычисленное значение циклического избыточного кода, которое зависит от содержимого фрейма (как и в сетях Token Ring и Ethernet). На устройстве-получателе это значение пересчитывается, чтобы определить, был ли поврежден фрейм во время передачи. Поврежденные фреймы отбрасываются.
- **Признак конца фрейма.** Содержит уникальные символы, обозначающие конец фрейма. В качестве таких символов не могут использоваться символы данных.
- **Состояние фрейма.** Позволяет станции-источнику определить, были ли допущены ошибки при передаче, и был ли фрейм распознан и скопирован станцией-получателем.

Интерфейс CDDI

Распределенный проводной интерфейс передачи данных (Copper Distributed Data Interface — CDDI) является реализацией протокола FDDI для витой пары. Как и интерфейс FDDI, CDDI обеспечивает передачу данных со скоростью 100 Мбит/с и использует архитектуру двойного кольца для обеспечения надежности. Интерфейс CDDI допускает установку рабочей станции и концентратора на расстоянии до 100 м.

Стандарт CDDI определен комитетом X3T9.5 Национального института стандартизации США. Официальное название CDDI — TP-PMD (Twisted-Pair Physical Medium-Dependent — TP-PMD). Его также называют TP-DDI (Twisted-Pair Distributed Data Interface — TP-DDI), что больше согласуется с термином "распределенный интерфейс передачи данных по оптоволоконным каналам" — FDDI. Интерфейс CDDI согласуется с физическим уровнем и подуровнем управления доступом, определенными стандартом ANSI.

Стандарт ANSI предусматривает для интерфейса CDDI всего два типа кабелей: экранированная витая пара (Shielded Twisted Pair — STP) и неэкранированная витая пара (Unshielded Twisted Pair — UTP). Кабель STP имеет сопротивление 150 Ом и соответствует спецификациям EIA/TIA 568 (IBM Type 1). UTP представляет собой кабель для передачи данных (категория 5), состоящий из четырех неэкранированных витых пар и специально разработанных изолирующих полимеров в пластиковой оболочке, соответствующих спецификациям IEA/TIA 568B.

На рис. 9.11 показаны отличия спецификации CDDI TP-PMD от других спецификаций FDDI.

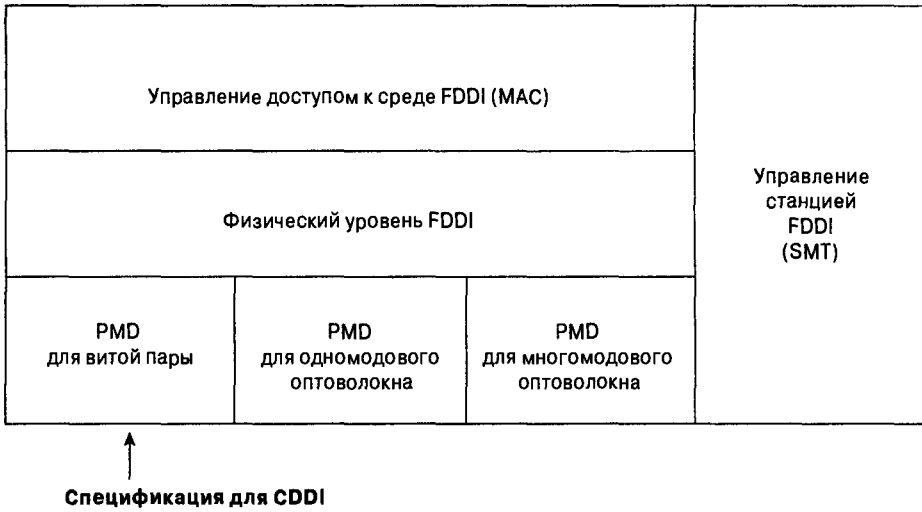


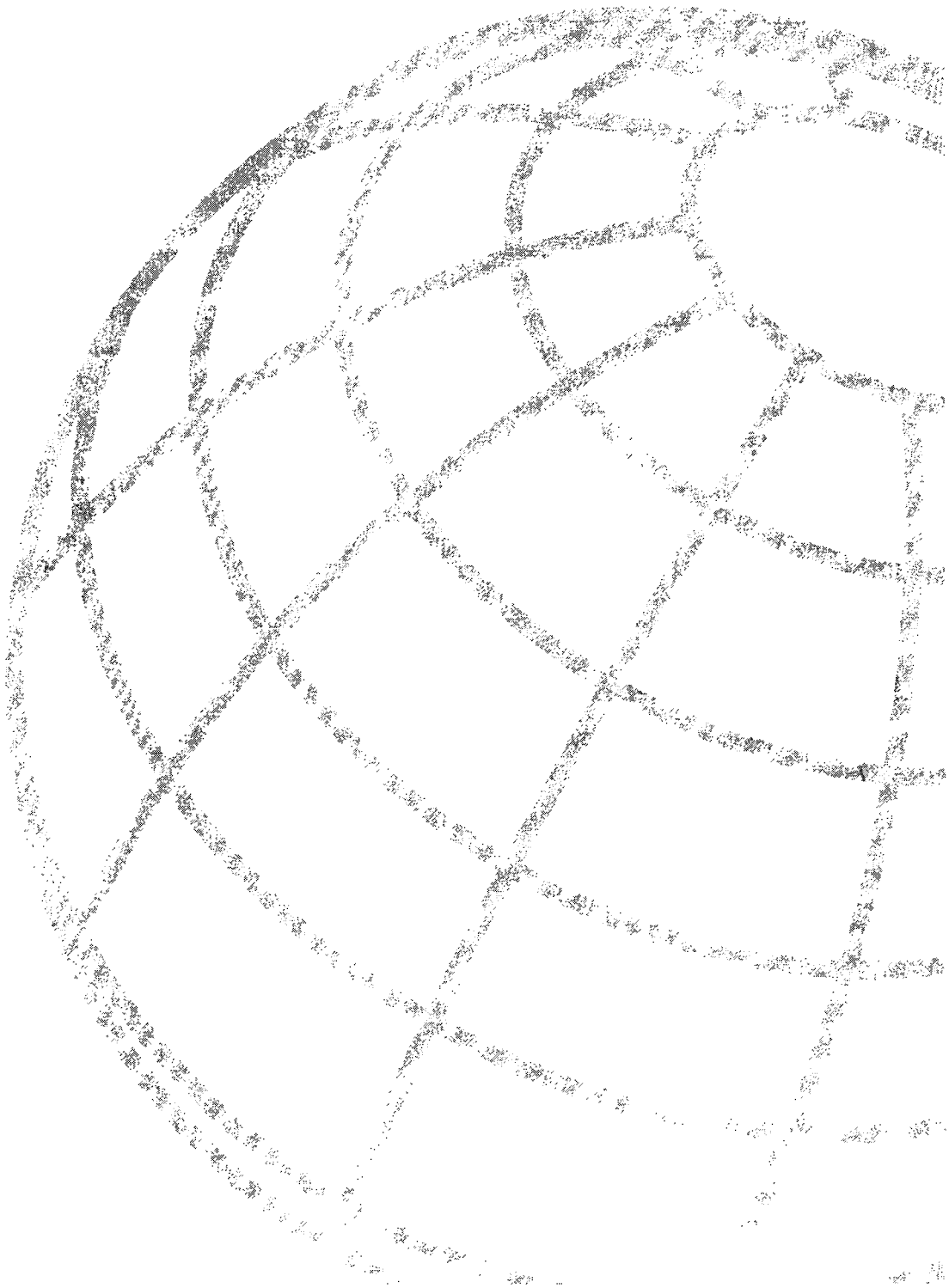
Рис. 9.11. Спецификации TP-PMD протоколов CDDI и FDDI соответствуют различным стандартам

Резюме

Распределенный интерфейс передачи данных по оптоволоконным каналам FDDI (Fiber Distributed Data Interface — FDDI) определяет архитектуру локальной сети в виде двойного кольца на основе оптоволоконного кабеля со скоростью передачи 100 Мбит/с. Благодаря высокой пропускной способности и возможности передачи данных на большие расстояния, чем при использовании электрического провода, протокол FDDI часто применяется на высокоскоростных магистралях.

Контрольные вопросы

1. Каковы преимущества интерфейса FDDI по сравнению с интерфейсом CDDI?
2. Какова роль DAC-устройств в сети FDDI?



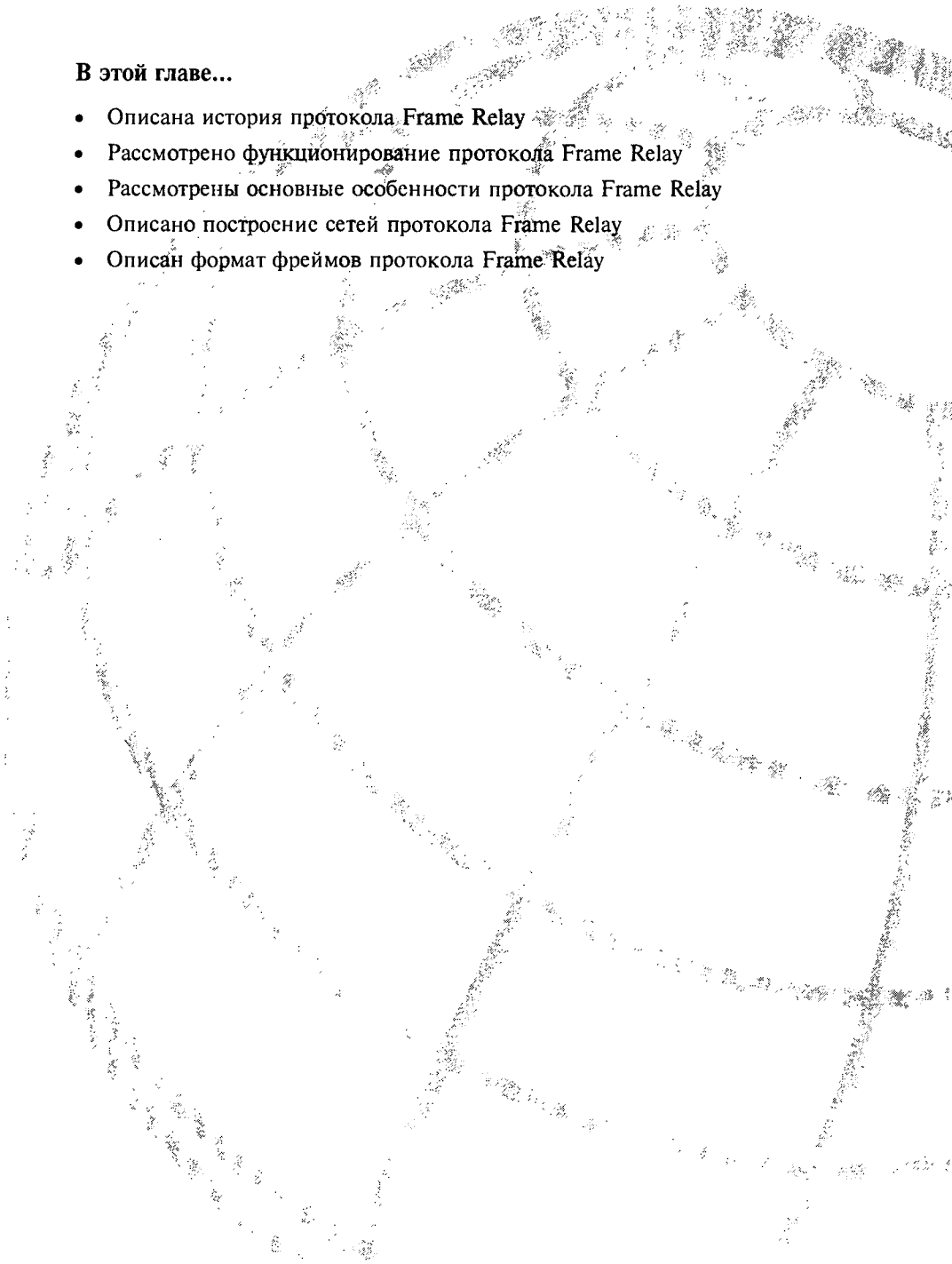
Часть III

Технологии распределенных сетей

Глава 10. Протокол Frame Relay
Глава 11. Интерфейс HSSI
Глава 12. Технология ISDN
Глава 13. Протокол PPP
Глава 14. Служба SMDS
Глава 15. Коммутируемые соединения
Глава 16. Протокол SDLC и его производные
Глава 17. Протокол X.25
Глава 18. Виртуальные частные сети

В этой главе...

- Описана история протокола Frame Relay
- Рассмотрено функционирование протокола Frame Relay
- Рассмотрены основные особенности протокола Frame Relay
- Описано построение сетей протокола Frame Relay
- Описан формат фреймов протокола Frame Relay



Глава 10

Протокол Frame Relay

Введение

Frame Relay представляет собой высокопроизводительный протокол распределенных сетей WAN, работающий на физическом и канальном уровнях эталонной модели OSI. Первоначально протокол Frame Relay был разработан для использования с интерфейсами цифровых сетей интегрированных служб (Integrated Services Digital Network — ISDN). В настоящее время он используется также со многими другими сетевыми интерфейсами. В этой главе основное внимание будет уделено спецификациям и применению Frame Relay для служб распределенных сетей WAN.

Протокол Frame Relay является примером технологии коммутации пакетов. Сети с коммутацией пакетов позволяют конечным станциям динамически распределять между собой среду передачи и доступную полосу пропускания. В технологии коммутации пакетов используются следующие два метода:

- применение пакетов переменной длины;
- статическое мультиплексирование.

Пакеты переменной длины используются для более эффективной и гибкой передачи данных. Эти пакеты коммутируются между различными сегментами сети, пока не достигают места назначения.

Методы статического мультиплексирования управляют доступом к сети с коммутацией пакетов. Их преимущество заключается в том, что они обеспечивают большую гибкость и эффективнее используют полосу пропускания. Большинство из распространенных в настоящее время локальных сетей, таких как Ethernet и Token Ring, являются сетями с коммутацией пакетов.

Часто Frame Relay называют упрощенным вариантом X.25, поскольку в нем отсутствуют такие функции повышения надежности, как управление окнами и повторная передача утерянных данных. Причина их отсутствия состоит в том, что протокол Frame Relay обычно работает в распределенных сетях с более надежными службами соединений и более высокой степенью надежности, чем у платформ WAN, распространенных в конце 70-х — начале 80-х годов прошлого века, на которых использовался протокол X.25. Как уже отмечалось, протокол Frame Relay относится к протоколам 2-го уровня, а протокол X.25, кроме того, предоставляет услуги и на 3-м (сетевом) уровне. Благодаря этому протокол Frame Relay обеспечивает более высокую производительность и эффек-

тивность передачи данных, чем протокол X.25, что делает Frame Relay пригодным для современных WAN-приложений.

Стандартизация Frame Relay

Первые предложения по стандартизации протокола Frame Relay были представлены Международному консультационному комитету по телеграфии и телефонии (Consultative Committee on International Telephone and Telegraph — CCITT) в 1984 году. Однако тогда, в конце 1980-х годов, из-за недостаточных возможностей взаимодействия с другими протоколами и неполной стандартизации протокол Frame Relay не получил значительного распространения.

Крутой поворот в истории протокола Frame Relay произошел в 1990 году, когда компании Cisco, Digital Equipment Corporation (DEC), Northern Telecom и StrataCom образовали консорциум, направленный на развитие технологии Frame Relay. Этот консорциум разработал спецификацию, которая соответствовала базовому протоколу Frame Relay, обсуждавшемуся CCITT, но дополняла его функциями, обеспечивающими новые возможности для сложных сред объединенных сетей. В целом эти дополнения базового протокола Frame Relay называются интерфейсом локального управления (Local Management Interface — LMI).

С тех пор как спецификация консорциума была разработана и опубликована, многие производители объявили о своей поддержке расширенного определения протокола Frame Relay. Впоследствии ANSI и CCITT стандартизировали собственные варианты первоначальной спецификации LMI, и эти стандартизированные спецификации в настоящее время более распространены, чем исходная версия.

На международном уровне протокол Frame Relay был стандартизирован секцией телекоммуникационных стандартов Международного союза электросвязи (International Telecommunication Union — Telecommunications Standards Section — ITU-T). В США протокол Frame Relay является стандартом Американского Национального института стандартов (American National Standards Institute — ANSI).

Устройства сетей протокола Frame Relay

Устройства, подключаемые к распределенным сетям Frame Relay, делятся на следующие две основные категории:

- терминальное оборудование (Data Terminal Equipment — DTE);
- оборудование передачи данных (Data Circuit-Terminating Equipment — DCE).

Обычно под DTE понимают терминальное оборудование отдельной сети, которое, как правило, находится у потребителя. Эти устройства могут также принадлежать потребителю. Примерами устройств DTE являются терминалы, персональные компьютеры, маршрутизаторы и мосты.

Под оборудованием DCE понимаются устройства объединенных сетей, принадлежащие провайдеру. Назначение устройств DCE состоит в обеспечении служб синхронизации и коммутации, а также непосредственной передаче данных по распределенным сетям. В большинстве случаев эти устройства представляют собой пакетные коммутаторы. На рис. 10.1 показаны взаимосвязи между этими двумя категориями устройств.

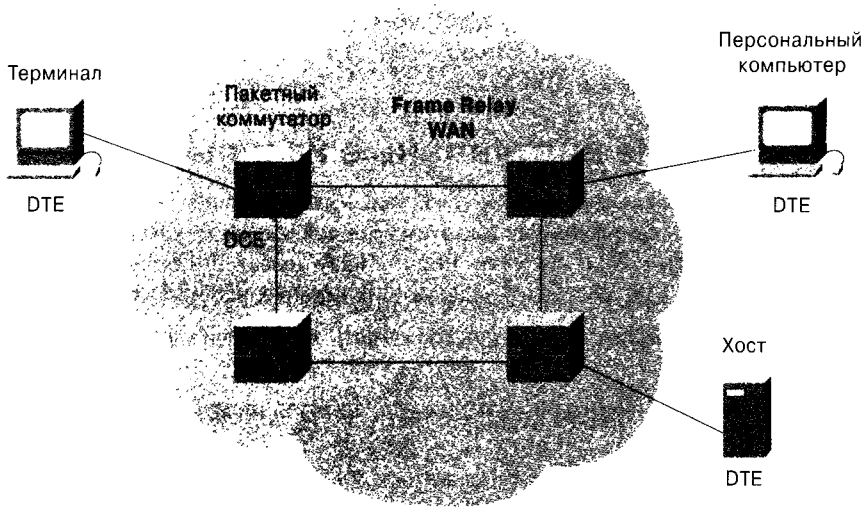


Рис. 10.1. Устройства DCE обычно находятся в распределенной сети, управляемой провайдером

Соединения между устройствами DTE и DCE обеспечиваются компонентами как физического, так и канального уровней. Физический компонент определяет механические, электрические, функциональные и процедурные параметры соединения между устройствами. Одной из наиболее распространенных спецификаций интерфейса физического уровня является спецификация стандарта RS-232. Канальный компонент задает протокол, устанавливающий соединение между устройством DTE, например маршрутизатором, и устройством DCE, например, коммутатором. В настоящей главе будет рассмотрена наиболее широко используемая спецификация протокола для распределенных сетей — протокол Frame Relay.

Виртуальные каналы протокола Frame Relay

Frame Relay обеспечивает ориентированный на соединение обмен данными на канальном уровне. Это означает, что между каждой парой устройств происходит обмен данными и этим соединениям соответствуют идентификаторы соединений. Такая служба реализуется с помощью виртуальных каналов протокола Frame Relay. Виртуальный канал Frame Relay представляет собой логическое соединение между двумя терминальными устройствами (DTE) по сети Frame Relay с коммутацией пакетов (Packet-Switched Network — PSN).

Виртуальный канал обеспечивает двунаправленный маршрут обмена данными между двумя устройствами DTE и однозначно определяется идентификатором канального соединения (Data-Link Connection Identifier — DLCI). Для передачи данных по сети несколько виртуальных каналов можно объединить в один физический канал. Эта возможность часто позволяет упростить сеть и уменьшить количество оборудования, требуемого для соединения нескольких устройств DTE.

Виртуальный канал может проходить через любое количество промежуточных DCE-устройств (коммутаторов), расположенных в PSN-сети Frame Relay.

Виртуальные каналы Frame Relay делятся на две категории: коммутируемые виртуальные каналы (Switched Virtual Circuit — SVC) и постоянные виртуальные каналы (Permanent Virtual Circuit — PVC).

Коммутируемые виртуальные каналы

Коммутируемые виртуальные каналы (Switched Virtual Circuits — SVC) представляют собой временные соединения, используемые в тех случаях, когда пересылка данных между устройствами DTE по сети Frame Relay имеет эпизодический характер. Сеанс связи по каналу SVC состоит из следующих четырех рабочих состояний.

- **Соединение.** Установка виртуального канала между двумя DTE-устройствами Frame Relay.
- **Передача данных.** Передача данных по виртуальному каналу между DTE-устройствами.
- **Холостой ход или простой.** Соединение между DTE устройствами по-прежнему активно, но данные не передаются. Если канал SVC находится в состоянии простоя в течение определенного времени, то соединение может быть ликвидировано.
- **Разъединение.** Ликвидация виртуального канала между DTE-устройствами.

Если после ликвидации виртуального канала возникает потребность в отправке дополнительных данных, то устройства DTE должны установить новый канал SVC. Предполагается, что каналы SVC устанавливаются, поддерживаются и ликвидируются с помощью тех же протоколов сигнализации, которые используются в сетях ISDN.

Раньше лишь немногие производители оборудования DCE для сетей Frame Relay обеспечивали возможность создания коммутируемых виртуальных каналов. Поэтому до недавнего времени в сетях Frame Relay такие каналы не имели большого распространения. Однако в настоящее время каналы SVC поддерживаются оборудованием Frame Relay, и их использование стало нормой. Компании обнаружили, что в конечном счете каналы SVC экономят средства, поскольку не требуется их постоянной поддержки в открытом состоянии.

Постоянные виртуальные каналы

Постоянные виртуальные каналы (Permanent Virtual Circuits — PVC) представляют собой постоянно поддерживаемые соединения, используемые для частой или постоянной передачи данных между DTE-устройствами по сети Frame Relay. Связь по PVC-каналам, в отличие от каналов SVC, не требует соединения и разъединения. PVC-каналы всегда находятся в одном из указанных ниже двух рабочих состояний.

- **Передача данных.** Передача данных по виртуальному каналу между устройствами DTE.
- **Холостой ход или простой.** Соединение между DTE-устройствами по-прежнему активно, но данные не передаются. В отличие от каналов SVC, связь по PVC-каналам не прерывается ни при каких обстоятельствах, в том числе и в режиме холостого хода.

Поскольку канал действует постоянно, устройства DTE могут начинать передачу данных в любое время, по мере необходимости.

Идентификатор канального соединения

Виртуальные каналы Frame Relay идентифицируются при помощи *идентификаторов канального соединения (Data-Link Connection Identifiers — DLCI)*. Обычно значения DLCI назначаются провайдером службы Frame Relay (например телефонной компанией).

Идентификаторы DLCI Frame Relay имеют локальное значение. Это означает, что их значения уникальны в пределах локальной сети, но не обязательно уникальны во всей распределенной сети Frame Relay.

На рис. 10.2 показано, что два различных DTE-устройства в сети Frame Relay могут иметь одинаковые значения DLCI.

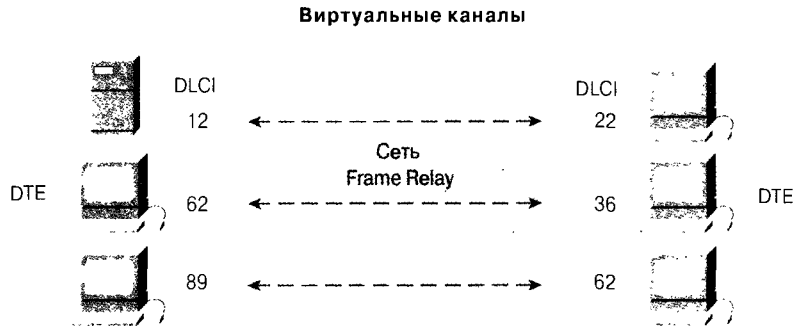


Рис. 10.2. Два различных DTE-устройства в распределенной сети Frame Relay могут иметь одинаковые значения идентификаторов DLCI

Механизмы управления переполнением

Frame Relay позволяет снизить нагрузку на сеть благодаря простым механизмам оповещения о переполнении, используемым вместо явного управления потоком каждого виртуального канала. Обычно сети Frame Relay реализуются в надежной среде передачи и контроль за целостностью данных не ослабляется, поскольку управление потоком можно предоставить протоколам более высоких уровней. В сетях Frame Relay используются следующие два механизма оповещения о переполнении:

- прямое явное уведомление о переполнении (Forward-Explicit Congestion Notification — FECN);
- обратное явное уведомление о переполнении (Backward-Explicit Congestion Notification — BECN).

Каждый из механизмов FECN и BECN управляется одним битом в заголовке фрейма Frame Relay. В этом заголовке также содержится бит допустимости отбрасывания (discard eligibility bit — DE), используемый для идентификации менее важных данных, которые в случае переполнения можно отбросить.

Бит FECN является частью поля адреса в заголовке фрейма Frame Relay. Механизм FECN инициируется при отправке DTE-устройством фреймов Frame Relay в сеть. Если в сети произошло переполнение, то устройства DCE (коммутаторы) устанавливают значение бита FECN во фреймах равным 1. Когда фреймы достигают устройства DTE, являющегося получателем, поле адреса (с установленным битом FECN)

указывает, что на пути от источника к получателю фрейм прошел через переполнение. Устройство DTE может передать эту информацию для обработки протоколу более высокого уровня. В зависимости от типа реализации сети может быть запущен процесс управления потоком или же это сообщение может быть проигнорировано.

Бит BECN также является частью поля адреса в заголовке фрейма Frame Relay. Устройства DCE устанавливают значение бита BECN равным 1 в тех фреймах, которые передаются навстречу фреймам с установленным битом FECN. Этот установленный бит уведомляет устройство DTE о переполнении на некотором участке сети. Затем устройство DTE может передать эту информацию для обработки протоколу более высокого уровня. В зависимости от типа реализации, может быть запущен процесс управления потоком или же это сообщение может быть проигнорировано.

Бит допустимости отбрасывания во фреймах Frame Relay

Бит допустимости отбрасывания (Discard Eligibility bit — DE) используется для указания на то, что данный фрейм имеет меньшую важность, чем другие фреймы. Бит DE является частью поля адреса в заголовке фрейма Frame Relay.

Устройства DTE могут устанавливать значение DE бита фрейма равным 1 для указания на то, что этот фрейм имеет меньшую важность, чем другие фреймы. В случае переполнения в сети устройства DCE в первую очередь отбрасывают фреймы с установленным DE-битом и лишь после этого отбрасывают фреймы, в которых он равен 0. Это уменьшает вероятность потери DCE-устройствами сети Frame Relay критически важных данных при возникновении в сети переполнения.

Контроль ошибок в сетях Frame Relay

В сетях Frame Relay используется обычный механизм контроля ошибок, известный как *циклическая проверка четности с избыточностью (Cyclic Redundancy Check — CRC)*. Проверка CRC путем сравнения двух вычисляемых значений позволяет определить, возникли ли ошибки при передаче данных от источника к получателю. В сетях Frame Relay нагрузка на сеть сокращается за счет того, что ошибки контролируются, но не исправляются. Обычно сети Frame Relay реализуются в надежной среде передачи и контроль за целостностью данных не ослабляется, поскольку управление потоком можно предоставить протоколам более высоких уровней.

Интерфейс локального управления Frame Relay

Интерфейс локального управления LMI (Local Management Interface — LMI) представляет собой ряд дополнений к базовой спецификации Frame Relay. Интерфейс LMI был разработан в 1990 году корпорациями Cisco Systems, StrataCom, Northern Telecom и Digital Equipment Corporation. Он предлагает ряд функций (называемых расширениями) для управления сложными объединенными сетями. Главными расширениями LMI-интерфейса Frame Relay являются глобальная адресация, сообщения о состоянии виртуального канала и многоадресатная рассылка.

Глобальная адресация делает идентификаторы канального соединения (DLCI) Frame Relay не локальными, а глобальными. Значения DLCI становятся адресами DTE, которые являются уникальными во всей распределенной сети Frame Relay. Благодаря глобальной адресации объединенные сети Frame Relay становятся более функциональными и управляемыми. Например, отдельные сетевые интерфейсы и подключенные к ним конечные узлы могут быть идентифицированы стандартными методами обнаружения и преобразования адресов. Кроме того, в этом случае для маршрутизаторов, расположенных на периферии сети Frame Relay, вся сеть Frame Relay выглядит как обычная локальная сеть.

Сообщения о состоянии виртуального канала обеспечивают обмен данными и синхронизацию между устройствами DTE и DCE сети Frame Relay. Эти сообщения используются для периодического отчета о состоянии каналов PVC, для того чтобы данные не отправлялись в "черные дыры" (т.е. по недействительным PVC-каналам).

Расширение LMI позволяет осуществлять многоадресатную рассылку. Такая рассылка экономит полосу пропускания, позволяя посылать сообщения об обновлении маршрутов и преобразовании адресов только определенным группам маршрутизаторов. Интерфейс LMI также помещает в сообщения об обновлениях сведения о состоянии групп многоадресатной рассылки.

Сетевые реализации протокола Frame Relay

Типичная реализация частной сети Frame Relay представляет собой установку на мультиплексоре T1 двух интерфейсов: обычного и Frame Relay. Фреймы Frame Relay направляются в сеть через интерфейс Frame Relay, а обычные потоки передаются соответствующему приложению или службам, таким как мини-АТС (private branch exchange — PBX), видео- и телеконференции.

Типичная сеть Frame Relay состоит из нескольких устройств DTE, например маршрутизаторов, соединенных с удаленными портами на мультиплексоре традиционными каналами типа "точка-точка", такими как T1, неполный T1 или каналами 56-Кбит/с. На рис. 10.3 приведен пример простой сети Frame Relay.

Большинство существующих в настоящее время сетей Frame Relay поддерживается провайдерами служб передачи данных. Часто эти службы называются общедоступными службами Frame Relay. Протокол Frame Relay реализуется как в общедоступных сетях, так и в частных сетях предприятий. В следующем разделе описываются две методологии реализации сети Frame Relay.

Общедоступные сети

В общедоступных сетях Frame Relay коммутирующее оборудование протокола Frame Relay располагается в центральных офисах телекоммуникационных компаний. С клиентов взимается плата в зависимости от степени использования ими сети, но им не приходится выполнять административные работы и поддерживать оборудование и службы сетей Frame Relay.

Обычно оборудование DCE также принадлежит телекоммуникационной компании (провайдеру службы) и арендуется клиентом, однако может принадлежать и пользователю.

Большинство современных сетей Frame Relay являются общедоступными.

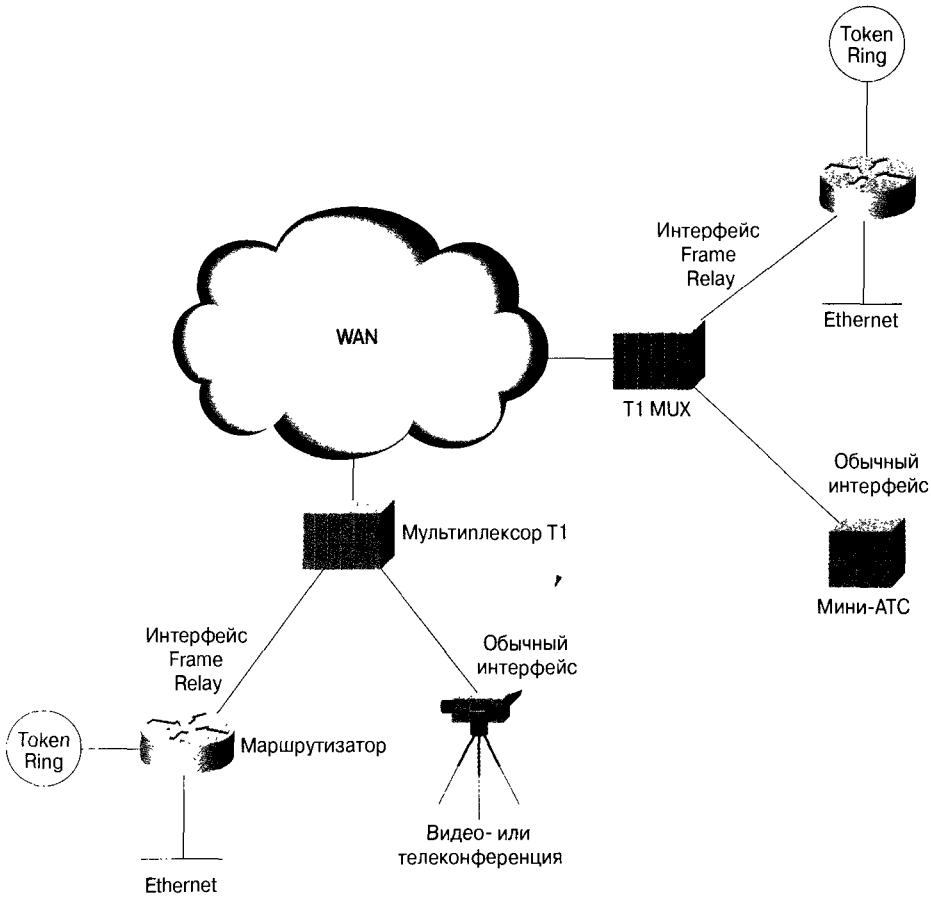


Рис. 10.3. Простая сеть Frame Relay, соединяющая различные устройства со службами распределенной сети

Частные сети

Все чаще различные организации в разных концах света внедряют частные сети Frame Relay. В таких сетях администрированием и поддержкой сети занимается само предприятие (частная компания). В этом случае все оборудование, включая коммутаторы, принадлежит потребителю.

Форматы фреймов Frame Relay

Для того чтобы лучше понять функционирование протокола Frame Relay, целесообразно изучить структуру его фреймов. Основной формат фрейма Frame Relay показан на рис. 10.4, а LMI-версия фрейма Frame Relay — на рис. 10.5.

Флаги отмечают начало и конец фрейма. Фрейм Frame Relay состоит из трех первичных компонентов: заголовка и области адреса, области данных пользователя и контрольной последовательности фрейма (Frame Check Sequence — FCS). Область

адреса, длиной 2 байта, состоит из 10 битов для идентификатора канала и из 6 битов для полей, связанных с управлением переполнением. Эта область называется идентификатором канального соединения (Data-Link Connection Identifier — DLCI). Каждое из перечисленных выше полей фрейма описывается ниже.

Стандартный фрейм протокола Frame Relay

Стандартные фреймы Frame Relay состоят из полей, показанных на рис. 10.4.

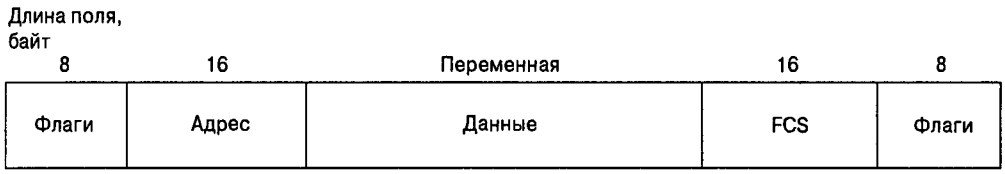


Рис. 10.4. Фрейм протокола Frame Relay

Основные поля фрейма Frame Relay, показанные на рис. 10.4, описаны ниже.

- **Флаги.** Определяют начало и конец фрейма. Значение этих полей всегда одинаково и равно 7E в шестнадцатеричном представлении или 01111110 в двоичном.
- **Адрес.** Содержит следующую информацию.
  - **DLCI.** 10-битовый идентификатор канального соединения DLCI является главной частью заголовка Frame Relay. Его значение идентифицирует виртуальное соединение между DTE-устройством и коммутатором. Каждое виртуальное соединение, которое мультиплексируется в физический канал, представляется уникальным идентификатором DLCI. Значения идентификатора DLCI являются локальными. Это означает, что они уникальны только для физического канала, которому принадлежат. Поэтому устройства, расположенные на противоположных концах линии связи, могут использовать для обозначения одного и того же виртуального соединения разные значения DLCI.
  - **Расширенный адрес (Extended Address — EA).** Поле EA используется для указания того, является ли байт, в котором поле EA равно 1, последним адресным полем. Если это значение расширенного адреса равно 1, то данный байт считается последним октетом идентификатора DLCI. Хотя во всех современных реализациях Frame Relay используется двухоктетный DLCI, это свойство позволяет в будущем использовать более длинные DLCI. Для указания на расширенный адрес EA применяется восьмой бит каждого байта адресного поля.
  - **C/R.** Этот бит следует за старшим байтом DLCI в адресном поле. В настоящее время назначение бита C/R пока не определено.
  - **Управление переполнением.** Данное поле состоит из 3 битов, предназначенных для управления механизмами оповещения о переполнении протокола Frame Relay. Этими последними тремя битами адресного поля являются биты FECN, BECN и DE.
  - Поле *прямого явного уведомления о переполнении FECN (Forward-Explicit Congestion Notification — FECN)* представляет собой однобитовое поле,

которому коммутатор может присвоить значение 1, чтобы указать конечному DTE-устройству, такому как маршрутизатор, на то, что при передаче фрейма от источника к получателю произошло переполнение. Главным преимуществом использования полей FECN и BECN является способность протоколов более высоких уровней "осмысленно" реагировать на эти индикаторы переполнения. В настоящее время единственными протоколами высших уровней, использующими эти возможности, являются протоколы DECnet и OSI.

— Поле *обратного явного уведомления о переполнении BECN (Backward-Explicit Congestion Notification — BECN)* представляет собой поле, состоящее из одного бита. Присвоение ему коммутатором значения 1 означает, что в сети, в направлении, противоположном исходному направлению передачи фреймов от источника к получателю, произошло переполнение.

— Бит *допустимости отбрасывания (Discard Eligibility — DE)* устанавливается устройством DTE, таким как маршрутизатор, для указания на то, что данный фрейм менее важен по сравнению с другими передаваемыми фреймами. В случае переполнения в сети фреймы, помеченные как допускающие отбрасывание, должны отбрасываться в первую очередь. Таким способом в сетях Frame Relay реализуется базовый механизм установки приоритетов.

- **Данные.** Это поле содержит инкапсулированные данные более высоких уровней. В этом поле переменной длины, которая может достигать 16000 октетов, содержатся данные пользователя или другая полезная нагрузка. Данное поле предназначено для доставки модулей данных протоколов высших уровней (PDU) по сети Frame Relay.
- **Контрольная последовательность фрейма.** Значение этого поля используется для проверки целостности передаваемых данных. Оно вычисляется устройством-источником и проверяется получателем.

Формат LMI-фрейма

Фреймы протокола Frame Relay, соответствующие спецификациям интерфейса LMI, состоят из полей, показанных на рис. 10.5.

Длина поля, байт

1	2	1	1	1	1	Переменная	2	1
Флаг	LMI DLCI	Индикатор ненумерованной информации	Признак протокола	Ссылка	Тип сообщения	Информационные элементы	FCS	Флаг

Рис. 10.5. Девять полей фрейма протокола Frame Relay формата LMI

Ниже описаны поля, показанные на рис. 10.5.

- **Флаг.** Определяет начало и конец фрейма.
- **Идентификатор DLCI интерфейса LMI.** Идентифицирует фрейм как фрейм LMI, а не стандартный фрейм Frame Relay. Соответствующее интерфейсу LMI зна-

чение идентификатора DLCI, определенное спецификациями консорциума LMI, равно 1023.

- **Индикатор ненумерованной информации.** Устанавливает конечный бит равным нулю.
- **Признак протокола.** Содержит величину, указывающую на то, что данный фрейм является фреймом интерфейса LMI.
- **Ссылка на вызов.** Всегда содержит нули. В настоящее время данное поле не используется.
- **Тип сообщения.** Указывает на то, что фрейм является сообщением и относится к одному из следующих типов.
  - **Запрос о состоянии.** Позволяет устройству пользователя делать запрос о состоянии сети.
  - **Сообщение о состоянии**. Отвечает на запрос о состоянии. Сообщениями о состоянии могут быть сообщения об активности или сообщения о состоянии каналов PVC.
- **Информационные элементы.** Это поле содержит переменное число отдельных информационных элементов (Information Element — IE). Элементы IE состоят из описанных ниже полей.
  - **Идентификатор IE.** Однозначно идентифицирует информационный элемент IE.
  - **Длина IE.** Определяет длину элемента IE.
  - **Данные.** Один или несколько байтов, содержащих инкапсулированные данные высших уровней.
- **Контрольная последовательность фрейма (FCS).** Используется для проверки целостности передаваемых данных.

Резюме

Frame Relay представляет собой протокол, который работает на двух нижних уровнях эталонной модели OSI — физическом и канальном. Он является представителем семейства технологий коммутации пакетов, которая позволяет конечным станциям динамически распределять сетевые ресурсы.

Устройства Frame Relay делятся на следующие две основные категории.

- Терминальное оборудование (Data Terminal Equipment — DTE), включающее в себя терминалы, персональные компьютеры, маршрутизаторы и мосты.
- Оборудование передачи данных (Data Circuit-Terminating Equipment — DCE). Эти устройства передают данные по сети и часто принадлежат провайдеру службы (хотя по мере развития предприятия часто приобретают собственные устройства DCE и используют их в своих сетях).

Сети Frame Relay передают данные, используя один из описанных ниже двух типов соединений.

- Коммутируемые виртуальные каналы (Switched Virtual Circuit — SVC). Эти каналы представляют собой временные соединения, создаваемые при каждой передаче данных и прерываемые по ее завершении (используются относительно редко).

- Постоянные виртуальные каналы (Permanent Virtual Circuit — PVC), представляющие собой постоянные соединения.

Идентификатор канального соединения DLCI (Data-Link Connection Identifier — DLCI) представляет собой номер, присваиваемый каждому виртуальному каналу и точке подключения устройства DTE к распределенной сети Frame Relay. Двум различным соединениям в одной распределенной сети Frame Relay могут быть присвоены одинаковые значения — по одному на каждом конце виртуального соединения.

В 1990 году корпорации Cisco Systems, StrataCom, Northern Telecom и Digital Equipment Corporation разработали несколько дополнений протокола Frame Relay, получивших название интерфейса локального управления (Local Management Interface — LMI). Дополнения LMI предлагают несколько дополнительных функций, называемых расширениями и предназначенных для управления сложными объединенными сетями. Основными дополнениями являются следующие:

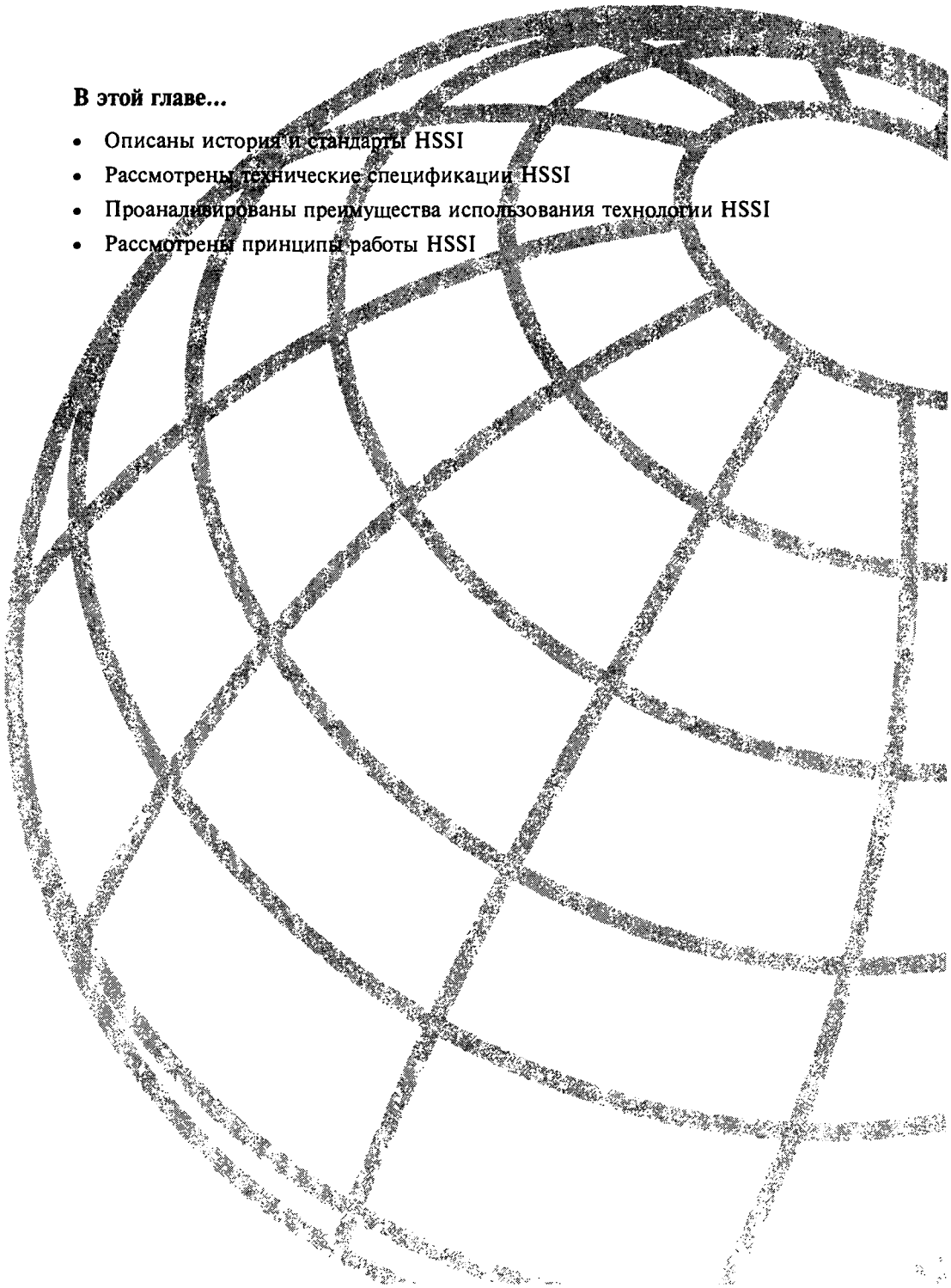
- глобальная адресация;
- сообщения о состоянии виртуального канала;
- многоадресатная рассылка.

Контрольные вопросы

1. К какому типу технологий относится протокол Frame Relay?
2. Назовите два вида технологий с коммутацией пакетов, описанных в настоящей главе, и кратко опишите каждый из них.
3. Опишите различия между каналами SVC и PVC.
4. Что представляет собой идентификатор канального соединения?
5. Опишите отличия протокола LMI Frame Relay от базового протокола Frame Relay.

В этой главе...

- Описаны история и стандарты HSSI
- Рассмотрены технические спецификации HSSI
- Проанализированы преимущества использования технологии HSSI
- Рассмотрены принципы работы HSSI



Глава 11

Интерфейс HSSI

Введение

Высокоскоростной последовательный интерфейс HSSI *(High-Speed Serial Interface — HSSI)* представляет собой интерфейс DTE/DCE, разработанный корпорациями Cisco Systems и T3plus Networking для высокоскоростных соединений по каналам распределенных сетей WAN. Спецификация HSSI доступна любой организации, желающей внедрить у себя HSSI.

Основы интерфейса HSSI

HSSI определяет электрический и физический интерфейсы между устройствами DTE и DCE. Он действует на физическом уровне эталонной модели OSI.

Технические характеристики интерфейса HSSI приведены в табл. 11.1.

Таблица 11.1. Технические характеристики интерфейса HSSI

Характеристика	Значение
Максимальная скорость передачи сигнала	52 Мбит/с
Максимальная длина кабеля	50 футов
Количество контактов в разъеме	50
Интерфейс	DTE-DCE
Электрическая технология	Дифференциальная эмиттерно-связанная логика
Номинальная потребляемая мощность	610 мВт
Топология	"Точка-точка"
Тип кабеля	Экранированная витая пара

Максимальная скорость передачи сигнала для интерфейса HSSI равна 52 Мбит/с. Таким образом, HSSI может поддерживать технологию T3 (45 Мбит/с) и большинство современных скоростных технологий WAN-сетей, а также технологии Office Channel-1 (OC-1, 52 Мбит/с) и иерархии синхронных цифровых сетей (Synchronous Digital

Hierarchy — SDH). Кроме того, интерфейс HSSI легко обеспечивает высокоскоростное соединение между локальными сетями, такими как Token Ring и Ethernet.

Применение микросхем с дифференциальной эмиттерно-связанной логикой (Emitter-Coupled Logic — ECL) позволяет интерфейсу HSSI добиться высокой скорости передачи данных и низкого уровня помех. Эмиттерно-связанная логика в течение многих лет использовалась в компьютерных интерфейсах Cray и описывается коммуникационным стандартом высокоскоростного параллельного интерфейса (HIgh-Performance Parallel Interface — HIPPI), разработанным институтом ANSI для объединения суперкомпьютеров в локальную сеть. Эмиттерно-связанная логика представляет собой готовую технологию, обеспечивающую прекрасное восстановление синхронизации на устройстве-получателе, результатом чего является достаточный запас надежности в отношении синхронизации.

Для интерфейса HSSI применяется микроминиатюрный, одобренный FCC, 50-контактный разъем, т.е. меньший, чем у его аналога V.35. Чтобы уменьшить потребность в адаптерах для соединения двух штекеров или двух гнезд, разъемы кабеля HSSI определены стандартом как штекеры. Количество контактов и проводов в кабеле HSSI такое же, как и в кабеле интерфейса SCSI-2, но HSSI отличается более жесткими электротехническими требованиями.

Функционирование интерфейса HSSI

Гибкость синхронизации и протокола обмена данными HSSI делает возможным для пользователя (или поставщика) распределение полосы пропускания по своему усмотрению. DCE-устройство управляет синхронизацией путем изменения ее скорости или удаления синхронизирующих импульсов. Таким образом телекоммуникационное устройство может перераспределять полосу пропускания между приложениями. Например, мини-АТС (PBX) может потребоваться одна ширина полосы пропускания, маршрутизатору — другая, а расширителю канала — третья. Возможность распределения полосы пропускания является ключевым фактором доступности и широкого применения Т3 и других широкополосных служб.

Интерфейс HSSI предполагает одинаковый уровень интеллектуальности DCE-устройств и DTE-устройств. Протокол управления упрощен и состоит лишь из двух управляющих сигналов: "DTE available" (терминальное устройство DTE доступно) и "DCE available" (телекоммуникационное устройство DCE доступно). Для функционирования информационного канала, необходимо получить оба эти сигнала. Терминальное и телекоммуникационное устройства должны быть в состоянии управлять сетями, которые находятся за их интерфейсами. Сокращение количества управляющих сигналов повышает надежность канала, поскольку уменьшается количество каналов, в которых может произойти сбой.

Контроль образования маршрутных петель

Как показано на рис. 11.1, интерфейс HSSI обеспечивает четыре вида контроля петель в сети. В первом из них локальный кабель тестируется при возврате сигнала после того, как он доходит до порта терминального устройства DTE. Во втором случае сигнал доходит до линейного порта локального телекоммуникационного устройства. В третьем сигнал доходит до линейного порта удаленного телекоммуникационного устройства DCE. Наконец, четвертый вид контроля представляет собой

инициируемую телекоммуникационным устройством DCE проверку DCE-порта терминального устройства DCE.

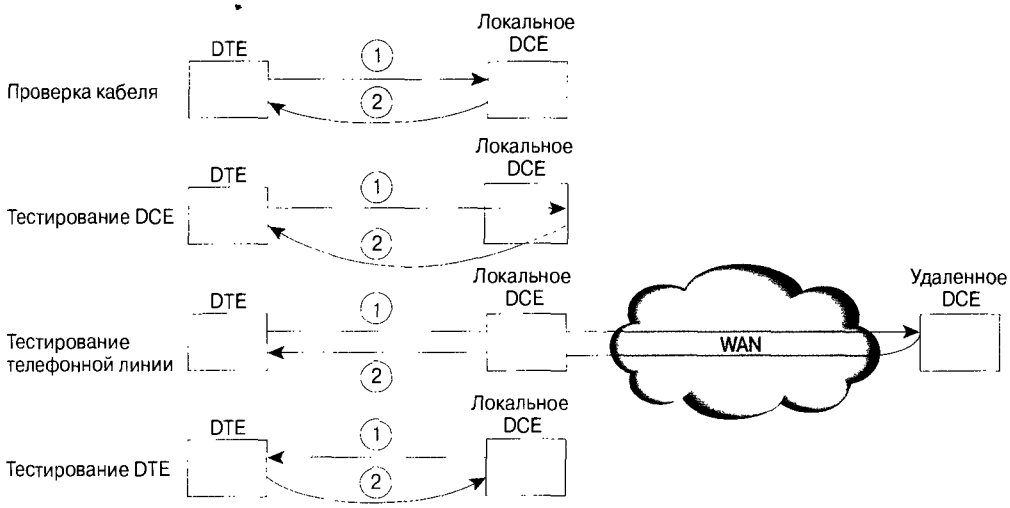


Рис. 11.1. Четыре вида контроля петель интерфейсом HSSI

Резюме

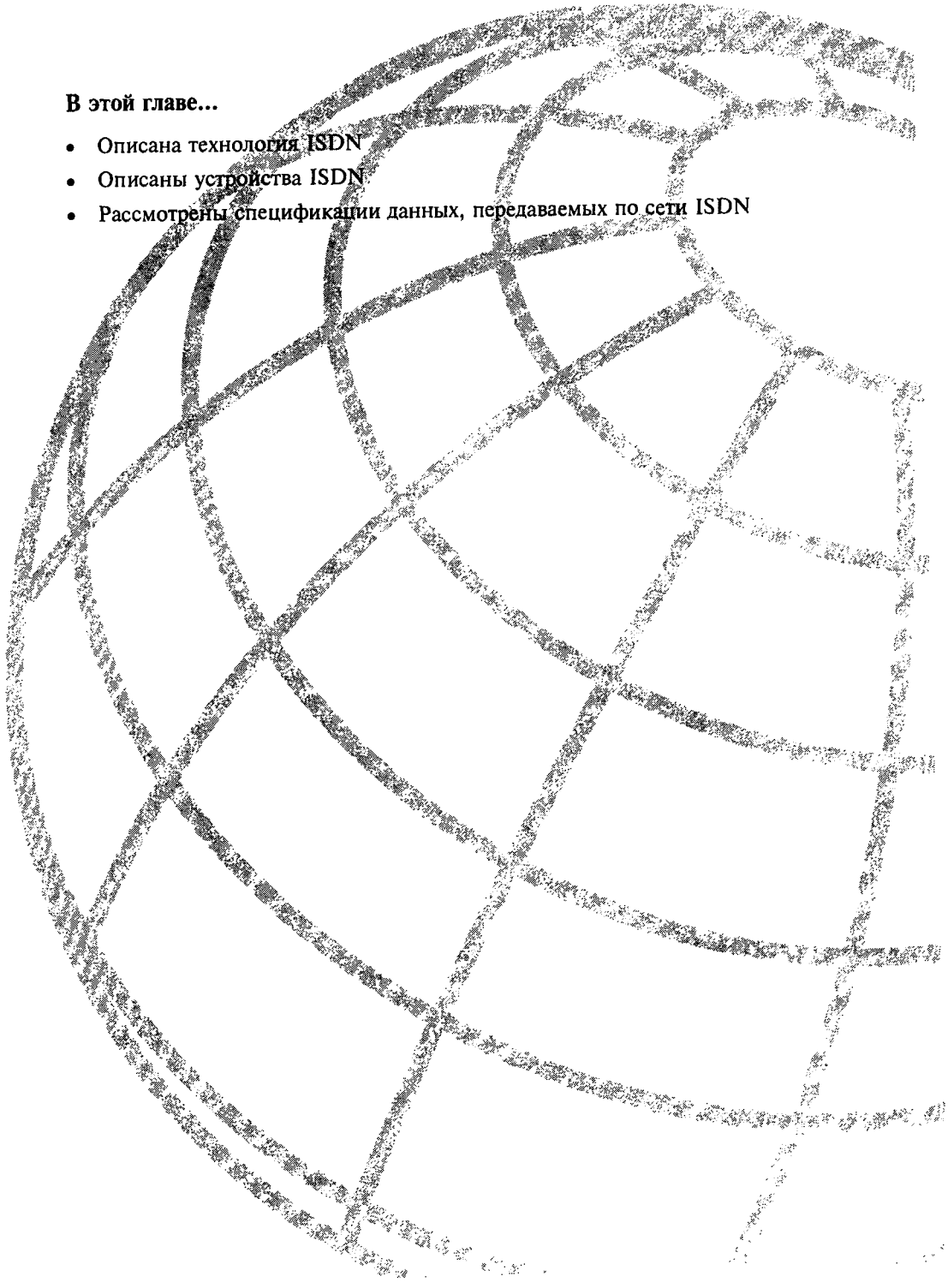
HSSI представляет собой интерфейс, разработанный в конце 90-х годов XX века корпорациями Cisco Systems и T3plus Networking для того, чтобы удовлетворить спрос на технологии высокоскоростной передачи данных по распределенным сетям. В интерфейсе HSSI применяется дифференцированная эмиттерно-связанная логика, которая обеспечивает быструю передачу данных при низком уровне шумов. Разъемы HSSI имеют значительно меньшие размеры, чем у конкурирующих технологий, а кабель HSSI имеет столько же контактов и проводов, сколько и кабель Small Computer System Interface 2 (SCSI2), но его электрическая спецификация отличается гораздо большей четкостью. Интерфейс HSSI облегчает перераспределение полосы пропускания, тем самым делая более доступными T3 и другие широкополосные службы. HSSI требует только двух управляющих сигналов, что обеспечивает высокую надежность данной технологии, поскольку при этом уменьшается количество каналов, в которых может произойти сбой. Для контроля надежности в HSSI выполняется четырехкратный контроль петель.

Контрольные вопросы

1. Назовите не меньше трех преимуществ реализации в сети технологии HSSI.
2. Перечислите четыре вида контроля маршрутных петель, которые осуществляются в HSSI.

В этой главе...

- Описана технология ISDN
- Описаны устройства ISDN
- Рассмотрены спецификации данных, передаваемых по сети ISDN



Глава 12

Технология ISDN

Цифровая сеть интегрированных служб (Integrated Services Digital Network — ISDN) включает в себя цифровую телефонию и службы передачи данных, предоставляемые региональными телефонными компаниями. Технология ISDN требует преобразования информации, передаваемой по телефонной сети, в цифровую форму. Это позволяет передавать по имеющимся телефонным проводам голос, обычные цифровые данные, текст, графику, музыку, видео и другую информацию. Целью использования ISDN является стандартизация абонентских служб, интерфейсов "пользователь/сеть", а также функций локальных и объединенных сетей. Технология ISDN применяется для высокоскоростной обработки графики (например для факсимильной связи Group IV), для предоставления дополнительных домашних телефонных каналов, быстрой передачи файлов, для видеоконференций, а также для передачи голосовых данных. В настоящей главе описываются основные технологии и службы, связанные с ISDN.

Устройства ISDN

В число устройств ISDN входят терминалы, терминальные адаптеры (Terminal Adapter — TA), сетевые и канальные терминаторы, а также терминаторы обмена. Существует два типа терминалов ISDN. Специализированные терминалы ISDN называются "терминальным оборудованием 1-го типа" (Terminal Equipment type 1 — TE1). Терминалы, не предназначенные для ISDN, такие как DTE-устройства, появившиеся раньше стандартов ISDN, называются "терминальным оборудованием 2-го типа" (Terminal Equipment type 2 — TE2). Терминалы TE1 подключаются к сети ISDN по четырехпроводному цифровому кабелю на основе витой пары. Терминалы TE2 подключаются к сети ISDN через терминальный адаптер. Терминальный адаптер ISDN может представлять собой как отдельное устройство, так и плату в составе терминала TE2. Если устройство TE2 является самостоятельным устройством, то оно подключается к адаптеру через стандартный интерфейс физического уровня, такой как EIA/TIA-232-C (ранее называвшийся RS-232-C), V.24 или V.35.

Следующей точкой соединений в сети ISDN после устройств TE1 и TE2 является сетевой терминатор 1-го типа (NT1) или 2-го типа (NT2). Эти устройства подключаются четырехпроводными абонентскими кабелями к обычной двухпроводной локальной замкнутой цепи. В США устройства NT1 входят в оборудование, устанавливаемое у пользователя (Customer Premises Equipment — CPE). В других странах устройства NT1, как правило, является частью коммерческой сети. Устройство NT2 является

более сложным и обычно применяется в цифровых мини-АТС, выполняет функции протоколов 2-го и 3-го уровней, а также сбор данных. Существуют также устройства, обозначаемые как NT1/2, сочетающие в себе функции устройств NT1 и NT2.

Технология ISDN предусматривает следующие контрольные точки, определяющие логические интерфейсы между функциональными группами, такими как устройства TA и NT1.

- **R.** Контрольная точка между оборудованием, изначально не предназначенным для ISDN, и адаптером TA.
- **S.** Контрольная точка между терминалом пользователя и устройством NT2.
- **T.** Контрольная точка между устройствами NT1 и NT2.
- **U.** Контрольная точка между устройствами NT1 и канальными терминаторами в коммерческих сетях. Контрольная точка типа U используется только в Северной Америке, где функционирование устройств NT1 коммерческими сетями не обеспечивается.

На рис. 12.1 показан пример конфигурации ISDN, включающей в себя три устройства, подключенные к коммутатору ISDN, находящемуся в центральном офисе. Два из этих устройств совместимы с ISDN, поэтому их можно подключить к устройствам NT2 через контрольную точку S. Третье устройство (обычный телефон, не предназначенный для ISDN) подключается к адаптеру TA через контрольную точку R. Вместо использования устройств NT1 и NT2 любое из вышеупомянутых устройств можно подключить к устройству NT1/2. Кроме того, к первому коммутатору ISDN, который находится справа, подключены аналогичные станции пользователей (на рисунке не показаны).

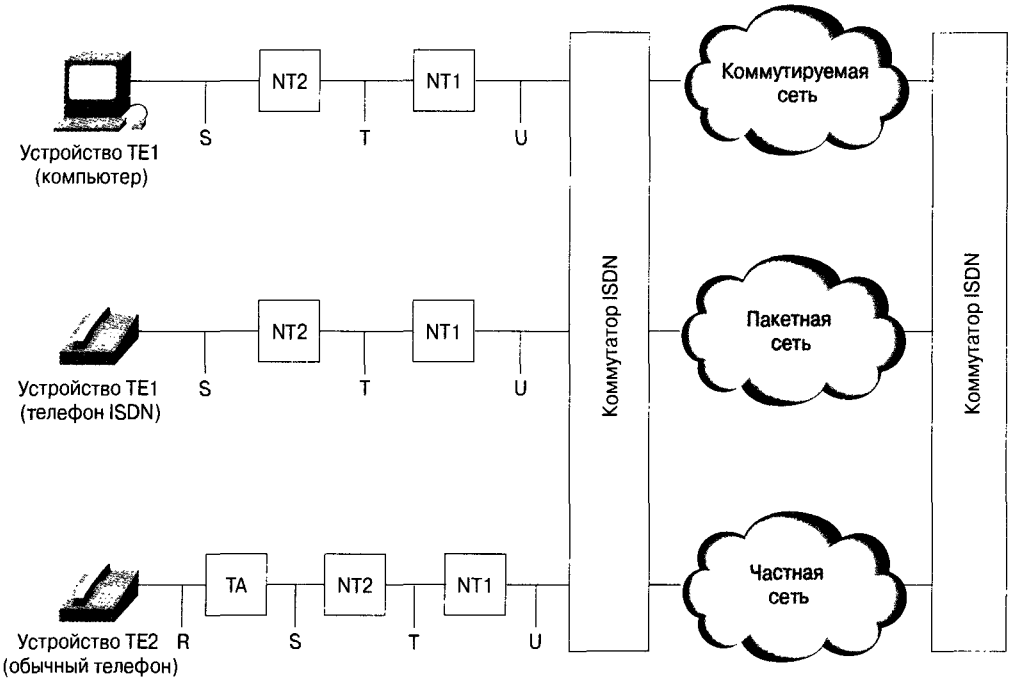


Рис. 12.1. Пример конфигурации ISDN, иллюстрирующий взаимосвязь между устройствами и контрольными точками

Службы ISDN

В сетях ISDN предусмотрены две службы:

- служба интерфейса базовой скорости BRI;
- служба интерфейса первичной скорости PRI.

Служба BRI-интерфейса в сети ISDN

Служба интерфейса базовой скорости передачи BRI ISDN (Basic Rate Interface — BRI) предоставляет два B-канала и один D-канал (2B+D). Служба B-канала BRI работает со скоростью 64 Кбит/с и предназначена для передачи управляющей и сигнальной информации, хотя в определенных условиях может обеспечивать и передачу данных пользователя. Сигнальный протокол D-канала соответствует уровням 1–3 эталонной модели OSI. Интерфейс BRI обеспечивает также управление фреймами и выполняет другие вспомогательные операции со скоростями до 192 Кбит/с. Спецификацией физического уровня BRI является стандарт I.430, выпущенный секцией стандартизации при Международном телекоммуникационном союзе (International Telecommunication Union-Telecommunications Standards Section — ITU-T, бывший комитет Consultative Committee for International Telegraph and Telephone — CCITT).

Служба PRI-интерфейса ISDN

Служба интерфейса первичной скорости передачи ISDN (Primary Rate Interface — PRI) предоставляет в Северной Америке и Японии 23 B-канала и один D-канал, которые обеспечивают общую скорость передачи 1,544 Мбит/с (D-канал PRI работает со скоростью 64 Кбит/с). В Европе, Австралии и других странах PRI ISDN обеспечивает 30 B-каналов и один D-канал (64 Кбит/с), которые обеспечивают общую скорость интерфейса 2,048 Мбит/с. Спецификацией физического уровня для интерфейса PRI является CCITT I.431.

Спецификации ISDN

1-й уровень (физический)

Форматы фреймов 1-го (физического) уровня ISDN зависят от того, является ли фрейм исходящим (отправляемым с терминала в сеть) или входящим (получаемым терминалом из сети). Оба интерфейса физического уровня показаны на рис. 12.2.

Длина фреймов составляет 48 битов, 36 из которых отводятся для данных. Биты фрейма ISDN физического уровня используются описанным ниже образом.

- **F.** Обеспечивает синхронизацию.
- **L.** Определяет среднее битовое значение.
- **E.** Используется для разрешения конфликтов, возникающих в тех случаях, когда несколько терминалов, расположенных на пассивной шине, претендуют на один канал.
- **A.** Активизирует устройства.

- S. Не используется.
- **B1, B2 и D.** Содержат данные пользователя.

Рис. 12.2. Форматы фреймов физического уровня ISDN зависят от направления передачи

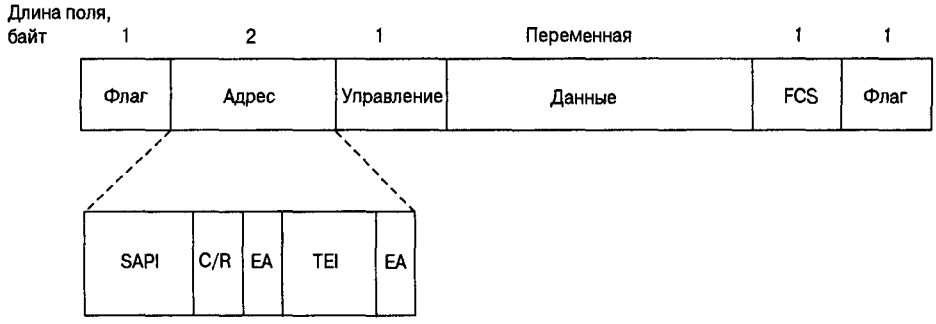
Физически к одной цепи может быть подключено несколько пользовательских устройств ISDN. В такой конфигурации возможны коллизии в результате попытки передачи данных двумя терминалами одновременно. Поэтому ISDN предусматривает средства обнаружения конфликтов при попытках доступа к каналу. Когда устройство NT получает D-бит от TE-устройства, оно дублирует этот бит в следующую E-позицию. TE-устройство следит за тем, чтобы следующий E-бит был таким же, как и последний переданный D-бит.

Терминалы не могут осуществлять передачу по D-каналу до тех пор, пока не получат определенное число единиц (указывающих на отсутствие сигнала в линии), соответствующее заранее установленному приоритету. Если TE-устройство обнаружит, что бит в эхо-канале (E) отличается от его D-битов, то оно должно немедленно прекратить передачу. Этот простой прием является гарантией того, что терминалы всегда будут передавать D-сообщения по очереди. После успешной передачи D-сообщения приоритет этого терминала понижается. Это выражается в том, что до передачи данных ему требуется распознать большее число последовательных единиц. Приоритет терминалов не может повыситься до тех пор, пока все остальные устройства, подключенные к данному каналу, не получат возможность отправить D-сообщение. Приоритет телефонных линий выше, чем у других служб, а приоритет сигнальной информации — выше, чем у других видов информации.

2-й уровень (канальный)

Вторым уровнем сигнального протокола ISDN является процедура доступа к каналу LAPD (Link Access Procedure, D channel — LAPD). Процедура LAPD аналогична HDLC и LAPB (см. главы 16 и 17). Как видно из названия, процедура

LAPD используется в D-канале для подтверждения того, что управляющая и сигнальная информация передается в нужном направлении и принимается получателем. Формат фрейма LAPD (рис. 12.3) во многом похож на формат фрейма протокола HDLC. Как и HDLC, протокол LAPD использует управляющий, информационный и ненумерованный фреймы. Протокол LAPD формально описан в стандартах ITU-T Q.920 и Q.921.



SAPI — идентификатор точки доступа к службе, 6 бит
C/R — бит команды/отклика
EA — биты расширенной адресации
TEI — идентификатор конечной терминальной точки

Рис. 12.3. Формат фрейма LAPD подобен форматам фреймов HDLC и LAPB

Поля флага и управления протокола LAPD идентичны одноименным полям протокола HDLC. Длина поля адреса LAPD может составлять один или два байта. Если в первом байте бит расширенного адреса (EA) установлен, то адрес состоит из одного байта, а если сброшен, то из двух. Первый байт поля Address содержит идентификатор точки доступа к службе SAPI (Service Access Point Identifier — SAPI), который определяет главный вход служб LAPD на 3-й уровень. Бит C/R указывает, что именно содержит фрейм — запрос или ответ. Поле идентификатора конечной точки терминала TEI (Terminal End-point Identifier — TEI) указывает на количество подключенных терминалов — один или несколько. Наличие в этом идентификаторе только единиц, означает широковещательную рассылку.

3-й уровень

В технологии ISDN для передачи сигналов используются две спецификации 3-го уровня: спецификация I.450 союза ITU-T (бывший комитет CCITT) (известная также как спецификация ITU-T Q.930) и ITU-T I.451 (известная также как ITU-T Q.931). Оба этих протокола обеспечивают соединения между пользователями, соединения с коммутацией каналов и с коммутацией пакетов. В них определены сообщения об установке и ликвидации вызова, информационные и другие сообщения, в том числе сообщения SETUP, CONNECT, RELEASE, USER INFORMATION, CANCEL, STATUS и DISCONNECT. Функционально они подобны сообщениям протокола X.25 (более подробно см. главу 17 "Протокол X.25 "). На рис. 12.4, взятом из спецификации ITU-T I.451, показаны типичные этапы установки соединения ISDN с коммутацией каналов.

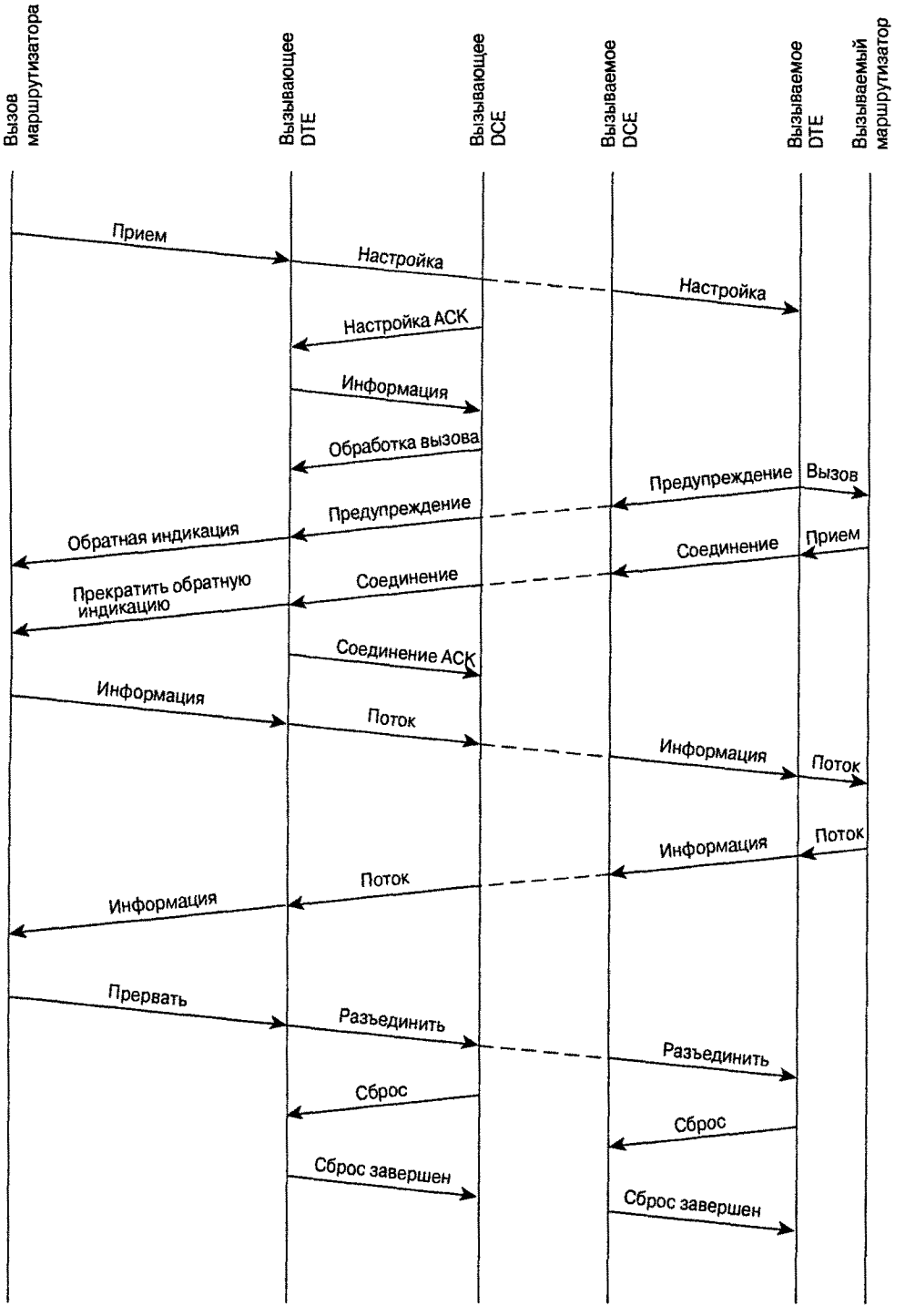


Рис. 12.4. Этапы установки соединения ISDN с коммутацией каналов

Резюме

Технология ISDN включает в себя службы цифровой телефонии и передачи данных, предоставляемые местными телефонными компаниями. При использовании ISDN требуется преобразование данных обычной аналоговой телефонной сети в цифровую форму, позволяющую передавать по имеющимся телефонным проводам голос, обычные цифровые данные, текст, графику, музыку, видео и другие виды информации.

В сетях ISDN используются следующие устройства:

- терминалы;
- терминальные адаптеры (TA);
- сетевые терминаторы;
- канальные терминаторы;
- терминаторы обмена.

В спецификации ISDN определены специальные точки соединения, являющиеся логическими интерфейсами между устройствами.

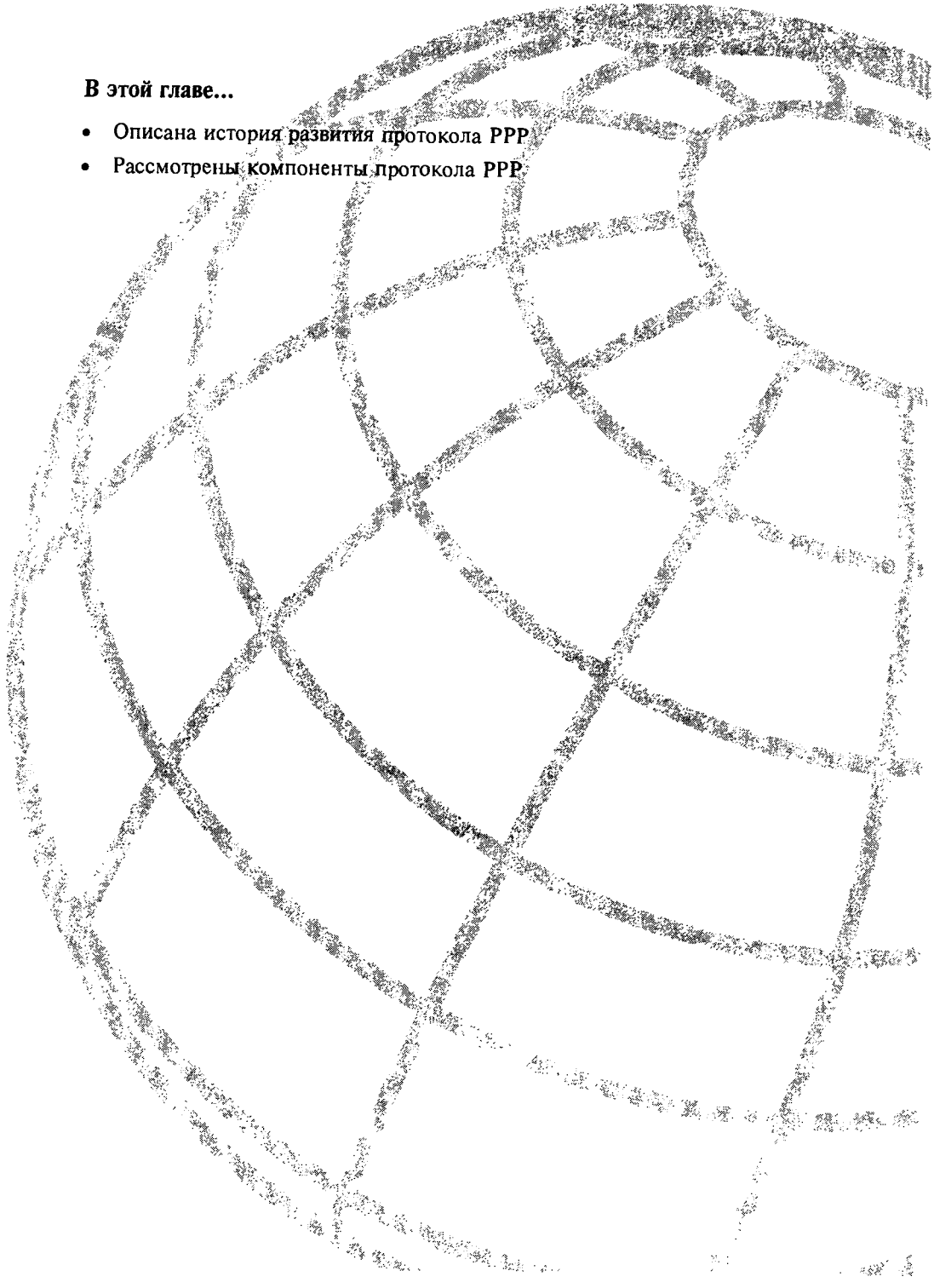
В ISDN используются следующие два типа служб:

- интерфейс базовой скорости (Basic Rate Interface — BRI), предоставляющий два B-канала и один D-канал (2B+D);
- интерфейс первичной скорости передачи (Primary Rate Interface — PRI), предоставляющий 23 B-канала и один D-канал в Северной Америке и Японии, и 30 B-каналов и один D-канал в Европе и Австралии.

Технология ISDN работает на трех нижних уровнях эталонной модели OSI; при этом на каждом уровне для передачи данных используется своя спецификация.

Контрольные вопросы

1. Какая контрольная точка для логических устройств ISDN используется только в Северной Америке?
2. Какие две скорости передачи предусмотрены для служб PRI-интерфейса сетей ISDN?
3. Сколько из 48 битов в формате физического фрейма ISDN занимают данные?



В этой главе...

- Описана история развития протокола PPP
- Рассмотрены компоненты протокола PPP

Глава 13

Протокол PPP

Введение

Протокол "точка-точка" (Point-to-Point Protocol — PPP) был первоначально разработан как протокол инкапсуляции для передачи данных протокола IP по каналам типа "точка-точка". Протокол PPP также определял стандарты назначения IP-адресов и управления ими, асинхронной (старт-стопной) и бит-ориентированной синхронной инкапсуляции, мультиплексирования сетевых протоколов, настройки и проверки качества канала, обнаружения ошибок и согласования таких характеристик, как адрес сетевого уровня и сжатие данных. Протокол PPP поддерживает эти функции используя протокол управления каналом (Link Control Protocol — LCP) и семейство протоколов управления сетью (Network Control Protocol — NCP), которые обеспечивают согласование дополнительных параметров конфигурации и используемых устройств. Кроме протокола IP протокол PPP поддерживает другие протоколы, в том числе Novell IPX (Internetwork Packet Exchange — IPX) и DECnet.

Компоненты протокола PPP

Протокол PPP обеспечивает передачу дейтаграмм по последовательным каналам типа "точка-точка" и состоит из приведенных ниже трех основных компонентов.

- Механизм инкапсуляции дейтаграмм для передачи по последовательным каналам. В качестве основы для инкапсуляции дейтаграмм при прохождении по каналам "точка-точка" PPP использует высокоуровневый протокол управления каналом HDLC (High-level Data Link Control — HDLC). Более подробно протокол HDLC описан в главе 16 "Протокол SDLC и его производные".
- Протокол LCP для установки, конфигурирования и тестирования соединения.
- Семейство протоколов NCP для установки и конфигурирования различных протоколов сетевого уровня. Протокол PPP предназначен для одновременного использования нескольких протоколов сетевого уровня.

Основные принципы работы протокола PPP

Для того чтобы установить соединение по каналу типа "точка-точка", протокол PPP вначале отправляет фреймы протокола LCP для настройки и, в некоторых случаях, тестирования канала. После установления связи и согласования дополнительных возможностей, как того требует протокол LCP, инициирующий соединение, протокол PPP отправляет фреймы протокола NCP для выбора и конфигурирования одного или более протоколов сетевого уровня. После того как все выбранные протоколы сетевого уровня будут сконфигурированы, их пакеты могут быть отправлены по данному каналу. Канал сохраняет конфигурацию до тех пор, пока не будут получены закрывающие его фреймы протоколов LCP или NCP, или не произойдет какое-либо внешнее событие (например, истечет допустимое время холостого хода или вмешается пользователь).

Требования, определяемые физическим уровнем

Протокол PPP может работать через любой интерфейс DTE/DCE (например EIA/TIA-232-C (ранее называвшийся RS-232-C), EIA/TIA-422 (ранее называвшийся RS-422), EIA/TIA-423 (RS-423) или интерфейс V.35 международного союза телекоммуникаций (International Telecommunication Union Telecommunication Standardization Sector — ITU-T, ранее CCITT). Единственным обязательным требованием, которое предъявляет протокол PPP, является обеспечение дуплексных каналов (выделенных или коммутируемых), которые могут работать в синхронном или асинхронном побитовом режиме, прозрачном для PPP-фреймов канального уровня. Протокол PPP не ограничивает скорость передачи, кроме тех случаев, когда она ограничивается применяемым интерфейсом DTE/DCE.

Канальный уровень протокола PPP

В протоколе PPP используются те же принципы, терминология и структура фрейма, что и в процедурах протокола HDLC (ISO 3309-1979), модифицированных стандартом ISO 3309:1984/PDAD1 "Addendum 1: Start/Stop Transmission", где описывается старт-стопная передача данных. Стандарт ISO 3309-1979 определяет структуру фрейма HLDC для синхронной среды, а ISO 3309:1984/PDAD1 — модификации, предложенные для стандарта ISO 3309-1979, которые позволяют использовать его в асинхронных средах. Процедуры управления протокола PPP применяют определения и способы кодирования управляющих полей, описанные стандартами ISO 4335-1979 и ISO 4335-1979/Addendum 1-1979. Формат фрейма PPP показан на рис. 13.1.

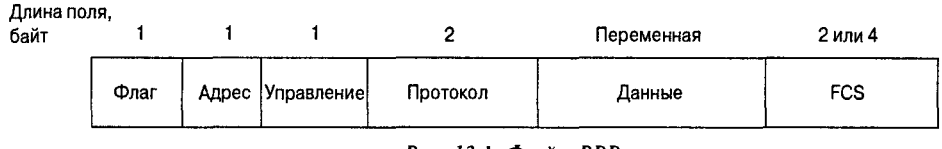


Рис. 13.1. Фрейм PPP

Поля фрейма PPP, показанные на рис. 13.1, описаны ниже.

- **Флаг.** Длина поля — 1 байт. Указывает на начало или конец фрейма и представляет собой двоичную последовательность 01111110.
- **Адрес.** Длина поля — 1 байт. Содержит двоичную последовательность 11111111, представляющую собой стандартный широковещательный адрес. Протокол PPP не назначает станциям индивидуальных адресов.
- **Управление.** Длина поля — 1 байт. Содержит двоичную последовательность 00000011, которая инициирует передачу данных пользователя в виде непоследовательного (unsequenced) фрейма. При этом обеспечивается служба, не требующая подтверждения соединения, аналогичная службам LLC Type 1. Подробнее типы службы LLC и типы фреймов описываются в главе 16 "Протокол SDLC и его производные".
- **Протокол.** Длина поля — 2 байта. Значение этого поля идентифицирует протокол, используемый в информационном поле фрейма. Последние данные о значениях этого поля содержатся в последнем выпуске спецификации Assigned Numbers Request For Comments.
- **Данные.** Длина поля — нуль или большее количество байтов. В этом поле содержится дейтаграмма протокола, указнного в поле протокола. Конец информационного поля определяется замыкающей флаговой последовательностью и двумя байтами поля FCS. По умолчанию максимальная длина информационного поля — 1500 байтов. В последних реализациях протокола PPP при наличии предварительного соглашения допускаются другие значения этой величины.
- **Контрольная последовательность фрейма.** Обычно составляет 16 битов (2 байта). В последних реализациях протокола PPP при наличии предварительного соглашения для более надежного обнаружения ошибок может использоваться 32-битовое (4-байтовое) поле FCS.

Протокол LCP позволяет согласовывать модификации стандартной структуры фрейма PPP. Однако модифицированные фреймы всегда будут явным образом отличаться от стандартных.

Протокол управления каналом (LCP) стека протоколов PPP

Протокол управления каналом (LCP) стека протоколов PPP обеспечивает открытие, конфигурирование, поддержку и ликвидацию соединения типа "точка-точка". Протокол LCP выполняет описанные ниже четыре операции.

- **Открытие и согласование конфигурации канала.** Прежде чем начать обмен дейтаграммами сетевого уровня (например дейтаграммами протокола IP), протокол LCP устанавливает соединение и согласовывает параметры конфигурации. Данный этап считается завершенным после того, как будет отправлен и получен фрейм подтверждения конфигурации.

- **Определение качества канала.** Протокол LCP обеспечивает дополнительную функцию — определение качества канала. Она выполняется после установки канала и согласования его конфигурации. На данном этапе проверяется, является ли качество канала достаточным для протоколов сетевого уровня. Этот этап не является обязательным. Протокол LCP может задержать передачу информации протоколов сетевого уровня до его завершения.
- **Согласование конфигурации протоколов сетевого уровня.** По окончании проверки качества канала производится конфигурирование каждого из сетевых протоколов в отдельности соответствующими протоколами семейства NCP. Затем эти сетевые протоколы могут быть в любой момент активизированы или отключены. Если протокол LCP закрывает канал, то он информирует об этом протоколы сетевого уровня, чтобы они могли предпринять соответствующие действия.
- **Закрытие канала.** Протокол LCP имеет возможность закрыть канал в любое время. Обычно это делается по запросу пользователя, однако может произойти и в результате какого-либо физического события, такого, например, как отказ носителя или превышение допустимого времени холостого хода.

Существует три класса LCP-фреймов. Фреймы открытия канала используются для установки и выбора конфигурации канала, фреймы закрытия канала предназначены для его отключения, а фреймы поддержки канала — для управления каналом и его отладки.

Эти фреймы используются для выполнения соответствующих действий на всех этапах работы протокола LCP.

Резюме

Протокол "точка-точка" (Point-to-Point Protocol — PPP) первоначально был разработан как протокол инкапсуляции для передачи данных протокола IP по каналам типа "точка-точка". Протокол PPP также определяет стандарты назначения IP-адресов и управления ими, асинхронной (старт-стопной) и бит-ориентированной синхронной инкапсуляции, мультиплексирования сетевых протоколов, конфигурирования и проверки качества канала, обнаружения ошибок и, при необходимости, согласования дополнительных возможностей.

Протокол PPP обеспечивает передачу дейтаграмм по последовательным каналам типа "точка-точка" и включает в себя следующие три компонента:

- механизм инкапсуляции дейтаграмм при передаче по последовательным каналам;
- протокол LCP для открытия, конфигурирования и тестирования канала;
- семейство протоколов NCP для установки и конфигурирования протоколов сетевого уровня.

Протокол PPP может работать с любым интерфейсом DTE/DCE. Он не налагает никаких ограничений на скорость передачи, кроме тех, которые обусловлены используемым интерфейсом DTE/DCE.

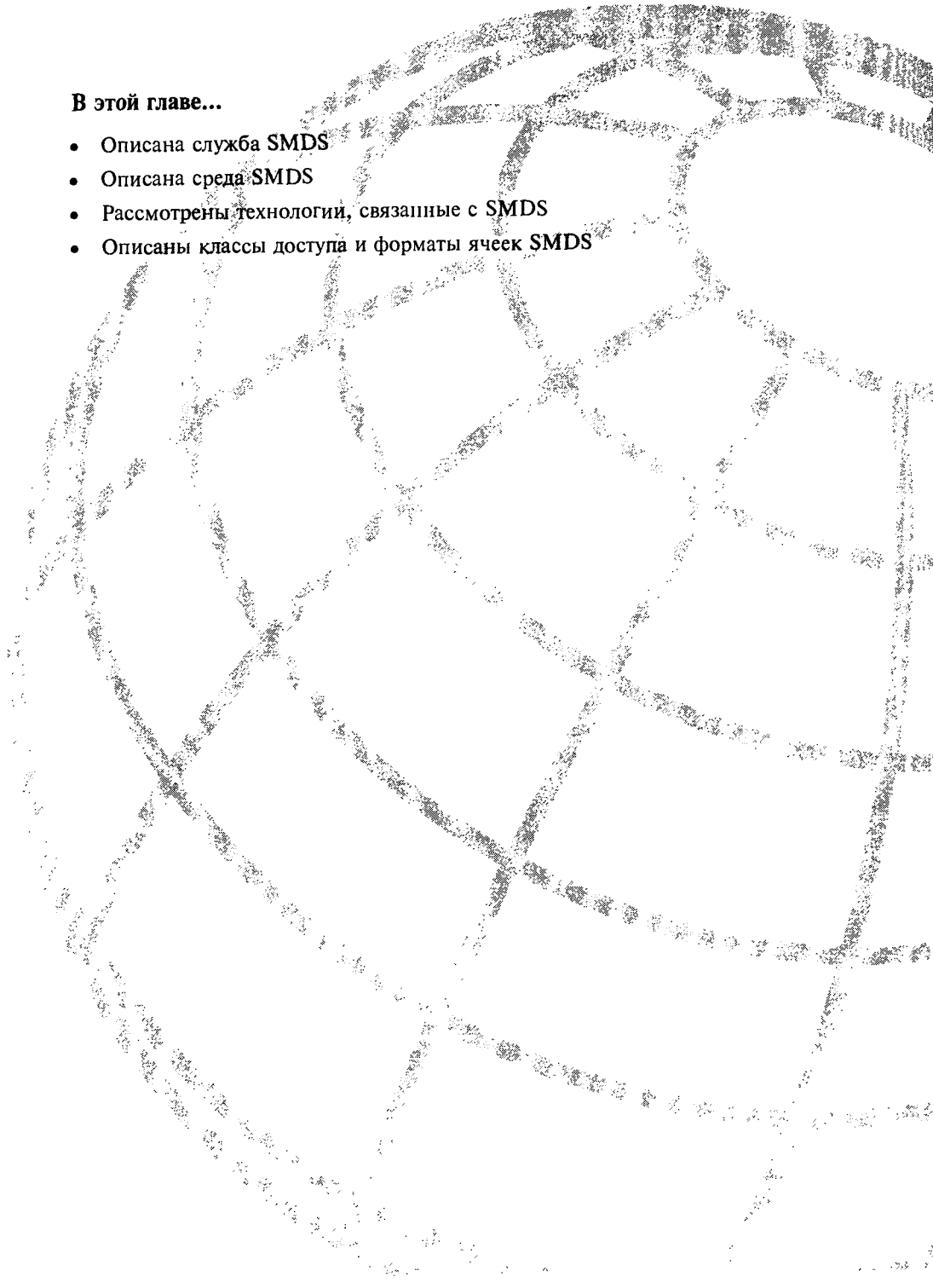
Фрейм протокола PPP состоит из шести полей. Протокол LCP стека протоколов PPP обеспечивает открытие, конфигурирование, поддержку и ликвидацию соединений типа "точка-точка".

Контрольные вопросы

1. Каковы главные компоненты протокола PPP?
2. Каково единственное абсолютное требование физического уровня, определяемое протоколом PPP?
3. Из каких полей состоит фрейм PPP?
4. Из каких этапов состоит работа протокола LCP, входящего в стек протоколов PPP?

В этой главе...

- Описана служба SMDS
- Описана среда SMDS
- Рассмотрены технологии, связанные с SMDS
- Описаны классы доступа и форматы ячеек SMDS



Глава 14

Служба SMDS

Введение

Служба мультимегабитовой коммутируемой передачи данных (Switched Multimegabit Data Service — SMDS) представляет собой технологию высокоскоростной коммутации для передачи дейтаграмм по распределенной сети, которая используется для обмена данными по общедоступным сетям передачи данных (Public Data Networks — PDN). Для службы SMDS может использоваться как оптоволоконная, так и проводная среда передачи; она обеспечивает передачу со скоростью 1,544 Мбит/с по каналам цифровых сигналов 1-го уровня (DS-1) и со скоростью 44,736 Мбит/с по каналам цифровых сигналов 3-го уровня (DS-3). Кроме того, модули данных SMDS достаточно велики для того, чтобы в них можно было полностью инкапсулировать фреймы спецификаций IEEE 802.3, IEEE 802.5 и FDDI. В настоящей главе описаны операционные элементы среды SMDS и определяющий ее протокол, а также связанные с ней технологии, такие как двойная шина распределенной очередности (Distributed Queue Dual Bus — DQDB). В заключение рассматриваются классы доступа и форматы ячеек службы SMDS.

Сетевые компоненты службы SMDS

Сети SMDS состоят из нескольких основных устройств, обеспечивающих высокоскоростную обработку данных. Это оборудование пользователя (Customer Premises Equipment — CPE), оборудование оператора связи и сетевой интерфейс абонента (Subscriber Network Interface — SNI). Под оборудованием CPE понимаются терминальные устройства, которые обычно принадлежат пользователю и обслуживаются им. В состав оборудования CPE также входят конечные устройства, такие как терминалы и персональные компьютеры, а также промежуточные узлы, такие как маршрутизаторы, модемы и мультиплексоры. Однако иногда промежуточные узлы обеспечиваются провайдером службы SMDS. Оборудование провайдера службы обычно включает в себя высокоскоростные коммутаторы распределенных сетей WAN, которые должны соответствовать определенным спецификациям сетевого оборудования, таким, например, как спецификации группы Bell Communications Research (Bellcore). Эти спецификации определяют сетевые операции, интерфейс между локальной и распределенной сетями, а также интерфейс между двумя коммутаторами, расположенными в сети провайдера.

Интерфейс SNI представляет собой интерфейс между оборудованием пользователя CPE и оборудованием провайдера службы и является точкой, в которой заканчивается сеть пользователя и начинается сеть провайдера. Назначение интерфейса SNI состоит в том, чтобы сделать технологию и функционирование передающего тракта SMDS прозрачными для пользователя. Связь между этими тремя компонентами сети SMDS показана на рис. 14.1.

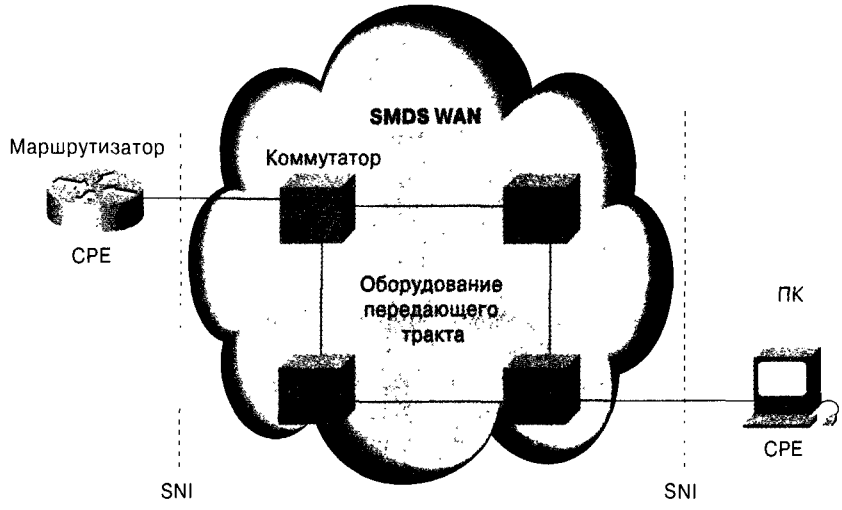


Рис. 14.1. SNI обеспечивает интерфейс между оборудованием пользователя CPE и передающим трактом SMDS

Протокол интерфейса SMDS

Протокол интерфейса службы SMDS (SMDS Interface Protocol — SIP) используется для обмена данными между оборудованием CPE и оборудованием передающего тракта SMDS. Интерфейс SIP обеспечивает службу без ориентации на соединение через сетевой интерфейс абонента (SNI), открывая устройствам CPE доступ к сети SMDS. Интерфейс SIP основан на стандарте DQDB IEEE 802.6 (Distributed Queue Dual Bus — DQDB) для передачи ячеек по сетям городского масштаба (Metropolitan-Area Networks — MAN). Стандарт DQDB был избран в качестве основы интерфейса SIP, поскольку он является открытым стандартом, поддерживающим все сервисные функции SMDS. Кроме того, стандарт DQDB совместим с современными стандартами передающего тракта и приводится в соответствие с разрабатываемыми стандартами широкополосной ISDN (Broadband ISDN — BISDN), что позволяет ему взаимодействовать с широкополосными службами передачи аудио- и видеоинформации. На рис. 14.2 показано место интерфейса SIP в сети SMDS.

Уровни SIP

Протокол SIP включает в себя три уровня. 3-й уровень SIP функционирует на подуровне управления доступом к среде передачи (Media Access Control — MAC) канального уровня эталонной модели OSI. На рис. 14.3 показана взаимосвязь интерфейса SIP и эталонной модели OSI, включая канальные подуровни IEEE.

Рис. 14.2. SIP обеспечивает службу без ориентации на соединение между оборудованием CPE и оборудованием передающего тракта

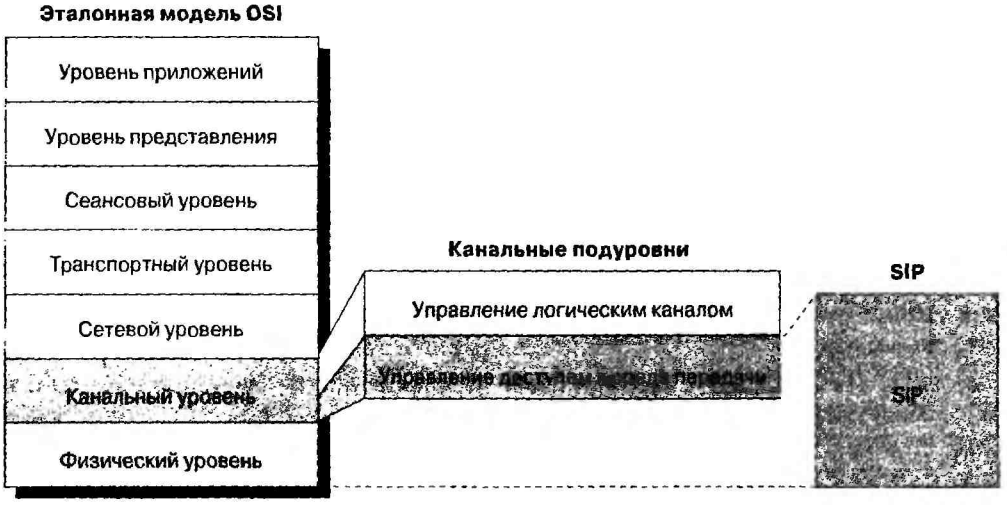


Рис. 14.3. Интерфейс SIP обеспечивает службы, связанные с физическим и канальным уровнями эталонной модели OSI

3-й уровень SIP начинает функционировать, когда через него в виде модулей данных службы SMDS (Service Data Units — SDU) передается информация пользователя. Затем модули SDU службы SMDS инкапсулируются между заголовком и трейлером 3-го уровня интерфейса SIP. Полученный фрейм называется модулем данных протокола (Protocol Data Unit — PDU) 3-го уровня. После этого модули PDU 3-го уровня интерфейса SIP передаются на 2-й уровень SIP.

2-й уровень SIP, работающий на подуровне доступа к среде передачи (MAC) канального уровня, вступает в действие, когда получает модули PDU с 3-го уровня интерфейса SIP. После этого модули PDU разбиваются на модули PDU 2-го уровня протокола SIP, имеющие одинаковую длину (53 октета) и называемые ячейками. Далее ячейки передаются на 1-й уровень SIP, где помещаются в физическую среду передачи.

1-й уровень интерфейса SIP функционирует на физическом уровне модели OSI и обеспечивает протокол физического канала, работающего со скоростями DS-1 и DS-3 между устройствами CPE и сетью. Первый уровень интерфейса SIP состоит из передающей системы и подуровней протокола конвергенции физического уровня (Physical Layer Convergency Protocol — PLCP). Подуровень передающей системы определяет характеристики и способ подключения к каналу передачи DS-1 или DS-3. Протокол PLCP определяет способ упорядочения ячеек 2-го уровня интерфейса SIP во фрейме DS-1 или DS-3, а также другую управляющую информацию.

Шина DQDB

Протокол распределенной последовательной двунаправленной шины (Distributed Queue Dual Bus — DQDB) представляет собой коммуникационный протокол канального уровня для региональных MAN-сетей ((Metropolitan-Area Networks — MAN). Протокол DQDB определяет топологию сети, состоящей из двух однонаправленных логических шин, соединяющих несколько систем. Эта топология определяется стандартом DQDB IEEE 802.6.

Доступ по шине DQDB описывает только функционирование протокола DQDB (в SMDS, SIP) через интерфейс между сетью и пользователем (в SMDS, через интерфейс SNI). Оно отличается от функционирования протокола DQDB в любой другой среде (например, между оборудованием передающего тракта в сети PDN службы SMDS).

Доступ по шине DQDB обеспечивается следующими базовыми компонентами сети SMDS.

- **Оборудование передающего тракта.** Одной из станций, подключенных к шине, является коммутатор сети SMDS.
- **CPE.** Одно или несколько устройств CPE действуют как станции, подключенные к шине.
- **SNI.** Интерфейс SNI действует как интерфейс между оборудованием CPE и оборудованием передающего тракта.

На рис. 14.4 показана основная схема доступа по шине DQDB, к которой подключены два устройства CPE и один коммутатор (оборудование передающего тракта).

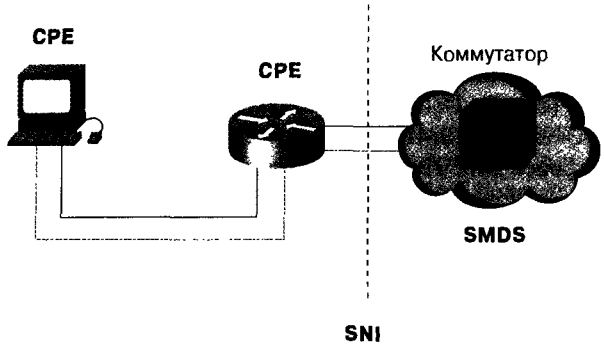


Рис. 14.4. Базовая схема доступа по DQDB включает в себя конечный узел, маршрутизатор и коммутатор

Обычно SMDS-доступ по DQDB обеспечивается конфигурацией из одного или нескольких CPE.

Конфигурация с одним CPE для доступа по DQDB состоит из одного коммутатора в передающем тракте сети SMDS и одной станции CPE на узле абонента. Конфигурация DQDB с одним CPE образует подсеть DQDB из двух узлов. Обмен данными происходит только между коммутатором и устройством CPE через интерфейс SNI. Конкуренции при доступе к шине не возникает, поскольку другие устройства CPE не пытаются получить к ней доступ.

Конфигурация с несколькими CPE состоит из одного коммутатора в передающем тракте сети SMDS и нескольких взаимосвязанных устройств CPE на узле абонента (все они принадлежат одному абоненту). В конфигурации с несколькими CPE возможен локальный обмен данными между устройствами CPE. Некоторые такие локальные коммуникации будут замечены коммутатором, обслуживающим интерфейс SNI, а другие останутся незамеченными.

Конкуренция относительно доступа к шине, возникающая между несколькими устройствами, требует использования распределенного алгоритма очередности DQDB, что усложняет реализацию конфигурации с несколькими CPE по сравнению с конфигурацией с одним CPE.

Классы доступа SMDS

Классы доступа службы SMDS позволяют сетям SMDS приспосабливаться к разнообразным требованиям, вытекающим из характера передаваемых данных и возможностей оборудования. Классы доступа ограничивают мгновенную и среднюю скорость передачи данных устройствами CPE путем задания максимальной мгновенной скорости передачи информации и максимально допустимого уровня всплесков скорости передачи. (Здесь под всплесками понимается резкое возрастание требований к полосе пропускания). Иногда классы доступа SMDS реализуются по схеме кредитного управления. В этом случае алгоритм кредитного управления создает кредитный баланс для каждого клиентского интерфейса и далее следит за ним. При передаче пакетов в сеть кредитный баланс уменьшается. Периодически выделяются новые кредиты, вплоть до достижения заранее определенного максимума. Кредитное управление применяется в интерфейсах SMDS только для скорости передачи DS-3 (для скорости DS-1 не используется).

Для скорости доступа DS-3 предусмотрено пять классов доступа, соответствующих мгновенным скоростям передачи информации 4, 10, 16, 25 и 34 Мбит/с.

Основы адресации SMDS

В модулях данных (Protocol Data Unit — PDU) протокола SMDS передаются адреса источника и получателя. Адреса SMDS представляют собой десятизначные значения, похожие на обычные телефонные номера.

Адресация SMDS обеспечивает многоадресатную рассылку и предоставляет функциизащиты сети.

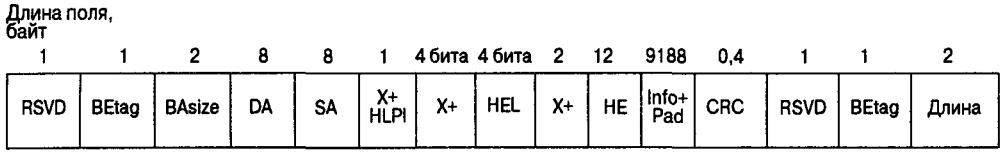
Групповая адресация SMDS позволяет при помощи одного адреса обращаться к нескольким станциям CPE, имеющим один и тот же адрес многоадресатной рассылки в поле адреса получателя. При этом сеть создает несколько копий модуля PDU, которые

доставляются всем членам группы. Использование адресов многоадресатной рассылки позволяет сократить потребность в сетевых ресурсах, требуемых для распространения маршрутной информации, преобразования адресов и динамического анализа ресурсов сети. Групповая адресация SMDS аналогична многоадресатной адресации в локальных сетях.

Служба SMDS предоставляет две функции обеспечения безопасности: подтверждение адреса источника и маскировку адресов. *Подтверждение адреса источника* позволяет убедиться, что адрес отправителя модуля PDU действительно принадлежит интерфейсу SNI, с которого он получен. Подтверждение адреса источника предотвращает подделку адреса, когда нелегальному потоку данных присваивается адрес легального источника. *Маскировка адресов* позволяет абоненту создать частную виртуальную сеть, исключающую поступление нежелательных потоков данных. Если адрес не является разрешенным, то модули данных не доставляются.

Стандарт SMDS: формат модуля PDU 3-го уровня интерфейса SIP

На рис. 14.5 показан формат протокольного модуля данных (PDU) третьего уровня протокола интерфейса SMDS (SMDS Interface Protocol — SIP).



RSVD — зарезервировано
BEtag — метка начала и конца
BAsize — размер выделенного буфера
DA — адрес получателя
SA — адрес источника
HLPI — идентификатор протокола высшего уровня
X+ — передается по сети без изменений
HEL — длина расширения заголовка
HE — расширение заголовка Info+Pad — информация + заполнение; поле должно заканчиваться на 32-м бите
CRC — контрольная сумма

Рис. 14.5. Модуль данных третьего уровня SIP

Ниже кратко описаны функции показанных на рис. 14.5 полей модуля PDU 3-го уровня интерфейса SIP.

- **X+.** Гарантирует, что формат модуля PDU интерфейса SIP соответствует формату протокола DQDB. Служба SMDS не обрабатывает и не изменяет значения, содержащиеся в этих полях, однако они могут использоваться системами, подключенными к сети SMDS.
- **RSVD.** Заполняется нулями.
- **BEtag.** Устанавливает связь между первым и последним сегментами сегментированного модуля PDU третьего уровня SIP. Оба поля (в начале и в конце

модуля PDU) содержат одинаковые значения и используются для обнаружения ситуаций, в которых последний сегмент одного и первый сегмент последующего PDU потеряны, что может привести к получению поврежденного модуля PDU третьего уровня.

- **BAsize.** Указывает размер выделяемого буфера.
- **DA.** Адрес получателя. Состоит из следующих двух частей.
  - **Тип адреса.** Занимает четыре старших бита. Может принимать значения 1100 или 1110. Первое означает 60-битовый индивидуальный адрес, а второе — 60-битовый адрес многоадресатной рассылки.
  - **Адрес.** Содержит индивидуальный или групповой SMDS-адрес получателя. Форматы SMDS-адресов соответствуют схеме североамериканской нумерации (North American Numbering Plan — NANP).
- Четыре старших бита в поле DA содержат значение 0001 (международный код Северной Америки). Следующие 40 битов содержат 10-значный адрес SMDS в двоичной форме. Последние 16 битов (младшие) содержат заполнители.
- **SA.** Адрес источника. Состоит из описанных ниже двух частей.
  - **Тип адреса.** Занимает четыре старших бита в поле. Адрес источника может быть только индивидуальным.
  - **Адрес.** Содержит индивидуальный SMDS-адрес источника. Это подполе имеет такой же формат, как и подполе адреса в поле DA.
- **HLPI.** Идентификатор протокола высшего уровня. Указывает на тип протокола, инкапсулированный в поле Info. Для службы SMDS он не имеет значения, но может использоваться системами, подключенными к сети.
- **HEL.** Длина расширения заголовка. Определяет количество 32-битовых слов в поле HE (расширение заголовка). В настоящее время для SMDS размер этого поля фиксирован и составляет 12 байтов (таким образом, значение HEL всегда равно 0011).
- **HE.** Расширение заголовка. Содержит номер версии SMDS. Кроме того, это поле сообщает о выбранной среде передачи, что используется при выборе конкретного передающего тракта для передачи данных протокола SMDS из одной локальной сети в другую.
- **Info+Pad.** Информация и заполнители. Содержит инкапсулированный модуль данных (Service Data Unit — SDU) службы SMDS и заполнители, необходимые для того, чтобы поле заканчивалось на 32-м бите.
- **CRC.** Контрольная сумма. Содержит значение, используемое для обнаружения ошибок.
- **Length.** Длина модуля PDU.

Стандарт SMDS: формат модуля PDU 2-го уровня интерфейса SIP

На рис. 14.6 показан формат модуля данных (PDU) 2-го уровня протокола интерфейса SMDS (SIP).

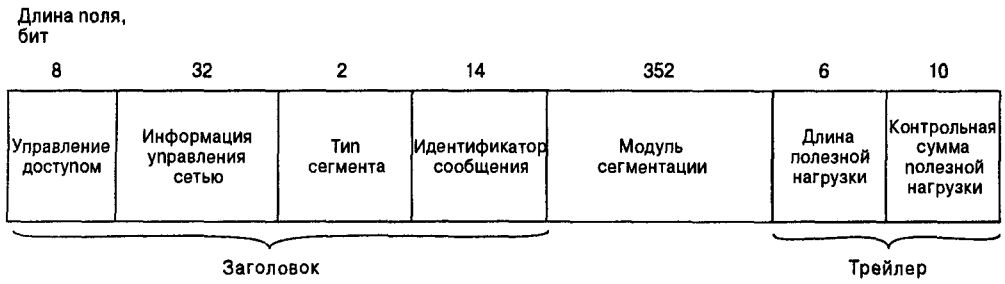


Рис. 14.6. Модуль данных второго уровня интерфейса SIP

Ниже кратко описаны функции изображенных на рисунке полей модуля PDU второго уровня SIP.

- **Управление доступом.** Содержит различные значения, в зависимости от направления информационного потока. Если ячейка передается с коммутатора на CPE-устройство, то имеет значение только то, содержится ли информация в модуле данных (PDU) третьего уровня протокола. Если же ячейка передается на коммутатор с одного из нескольких присутствующих в конфигурации устройств CPE, то это поле может содержать биты запроса, определяющие ячейки, передаваемые по шине от коммутатора к устройству CPE.
- **Информация управления сетью.** Содержит значение, указывающее, содержится ли в модуле PDU полезная информация.
- **Тип сегмента.** Указывает, является ли ячейка первой, последней или промежуточной в сегментированном модуле PDU третьего уровня. Возможны следующие четыре значения:
  - **00** — продолжение сообщения;
  - **01** — конец сообщения;
  - **10** — начало сообщения;
  - **11** — сообщение состоит из одного сегмента.
- **Идентификатор сообщения.** Связывает ячейки второго уровня с модулем PDU третьего уровня. Идентификатор сообщения одинаков для всех сегментов данного PDU третьего уровня. В конфигурации с несколькими CPE-устройствами модули PDU 3-го уровня, поступающие от разных устройств CPE, должны иметь разные идентификаторы. Это позволяет сети SMDS, получающей ячейки от разных модулей PDU третьего уровня в произвольном порядке, связывать каждую ячейку второго уровня с требуемым модулем PDU третьего уровня.
- **Модуль сегментации.** Содержит порцию данных ячейки. Если ячейка второго уровня пуста, то это поле заполняется нулями.
- **Длина полезной нагрузки.** Указывает, сколько байтов PDU третьего уровня содержатся в поле модуля сегментации. Если второй уровень пуст, то это поле заполняется нулями.
- **Контрольная сумма полезной информации.** Содержит значение CRC для обнаружения ошибок в следующих полях:

— тип сегмента;

— идентификатор сообщения;

— модуль сегментации;

— длина полезной информации;

— CRC полезной информации.

При вычислении значения CRC для полезной нагрузки не учитывается содержимое полей управления доступом и информации управления сетью.

Резюме

Служба мультимегабитовой коммутируемой передачи данных (Switched Multimegabit Data Service — SMDS) представляет собой высокоскоростную технологию коммутации пакетов для передачи дейтаграмм по распределенной сети, которая используется для обмена данными по общедоступным сетям (Public Data Networks — PDN). Для службы SMDS может использоваться как оптоволоконная, так и проводная среда передачи; она обеспечивает передачу со скоростью 1,544 Мбит/с по каналам цифрового сигнала 1-го уровня (DS-1) и со скоростью 44,736 Мбит/с по каналам цифрового сигнала 3-го (DS-3).

Сеть службы SMDS состоит из следующих устройств:

- оборудование пользователя (Customer Premises Equipment — CPE);
- оборудование передающего тракта;
- сетевой интерфейс абонента (Subscriber Network Interface — SNI).

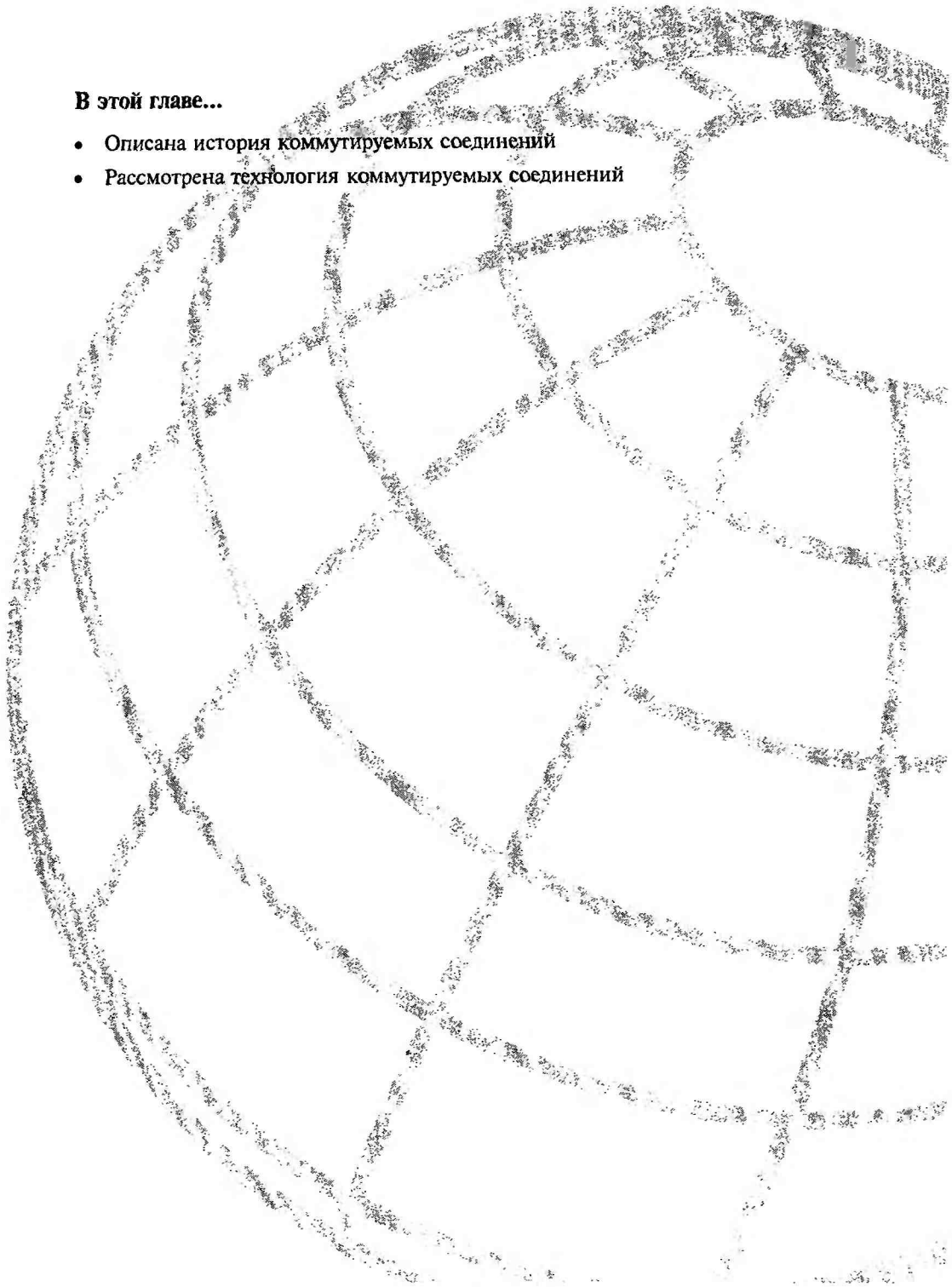
SNI представляет собой интерфейс между оборудованием CPE и оборудованием передающего тракта. Он обеспечивает прозрачную передачу данных между сетями источника и получателя.

- Служба SMDS использует интерфейс SIP для обмена данными между оборудованием CPE и передающим трактом по стандарту DQDB для передачи ячеек по сетям MAN.
- интерфейс SIP включает в себя следующие три уровня:
  - 3-й уровень, действующий на MAC-подуровне канального уровня эталонной модели OSI;
  - второй уровень, также действующий на MAC-подуровне канального уровня эталонной модели OSI;
  - 1-й уровень, действующий на физическом уровне эталонной модели OSI.
- В модулях PDU службы SMDS передаются адреса источника и получателя; эти модули также обеспечивают групповую адресацию и функции защиты.

Контрольные вопросы

1. Где расположен интерфейс SNI?
2. Что представляет собой интерфейс SIP?

3. На каких уровнях эталонной модели OSI действует каждый из трех уровней интерфейса SIP?
4. Каким образом обеспечивается использование шины DQDB несколькими устройствами?
5. В каких интерфейсах SMDS для реализации классов доступа SMDS иногда применяется схема кредитного управления?



В этой главе...

- Описана история коммутируемых соединений
- Рассмотрена технология коммутируемых соединений

Глава 15

Коммутируемые соединения

Введение

Под *коммутируемым соединением (dialup)* понимается передача данных пользователя по общедоступной коммутируемой телефонной сети (Public Switched Telephone Network — PSTN). Для этого используется устройство пользователя (Customer Premises Equipment — CPE), сообщающее коммутатору телефонной станции номер, с которым требуется установить соединение. Некоторые маршрутизаторы, такие как AS3600, AS5200, AS5300 и AS5800, позволяют работать как с PRI-интерфейсом ISDN, так и со многими цифровыми модемами. Маршрутизатор AS2511, в отличие от вышеперечисленных, также дает возможность устанавливать соединение с внешними модемами.

Со времени последнего издания *Руководства по технологиям объединенных сетей* рынок операторов связи значительно расширился и продолжает увеличиваться, требуя все более высокоскоростных модемов. Ответом на такую потребность стало повышение уровня взаимодействия с телекоммуникационным оборудованием и совершенствование цифровых модемов — появились модемы, обеспечивающие прямой цифровой доступ к общедоступной телефонной сети. Это позволило разрабатывать более скоростные пользовательские модемы, которые используют преимущества чистоты сигнала, свойственной цифровым модемам. Тот факт, что цифровые модемы, подключенные к общедоступной телефонной сети через интерфейсы PRI или BRI, могут передавать данные со скоростью более 53 Кбит/с по стандарту V.90, полностью подтверждает целесообразность этой идеи.

Краткая история коммутируемых соединений

Технологическая история коммутируемых соединений восходит к телеграфу. Простые сигналы, передаваемые по длинной электрической цепи, создавались вручную, путем замыкания и размыкания контактов. Пытаясь усовершенствовать это средство связи, Александр Белл в 1875 году изобрел телефон, чем навсегда изменил характер средств коммуникации. Возможность передачи по проводам звука сделала эту технологию более доступной и привлекательной для клиентов. К 1915 году линия Белла была проведена от

Нью-Йорка до Сан-Франциско. Спрос на услуги телефонной связи вызвал технологические нововведения, которые в 1927 году привели к появлению первой трансатлантической телефонной линии, использующей радиосигналы. Параллельно с этим были разработаны СВЧ-радиостанции, которые в 1948 году соединили американские города, интегрированные цифровые сети для повышения качества связи и телекоммуникационные спутники, первым из которых был Telstar 1, запущенный в 1962 году. К 1970 году почти во всех американских домах были установлены телефоны.

В 1979 году появились первые модуляторы-демодуляторы (модемы), а вместе с ними и сети, основанные на технологии коммутируемых соединений. Первые модемы работали медленно и зависели от типа частных систем связи. Сначала они применялись для периодических соединений типа "точка-точка" через распределенную сеть. Часто вызов поступал на обычный телефон в центре обработки данных. Оператор центра слышал характерный звук модема и клал трубку на специальный рычаг; это и был модем.

В конце 80-х годов прошлого века международный телекоммуникационный союз ITU-T начал выпускать рекомендации V-серии по стандартизации связи между телекоммуникационным оборудованием (Data Communication Equipment — DCE) и терминальным оборудованием (Data Terminal Equipment — DTE). Первыми были разработаны следующие стандарты.

- **V.8.** Стандартизация метода, используемого модемами для первоначального определения модуляции V-серии, по которой должна осуществляться связь. Следует обратить внимание на то, что этот стандарт применим только для сеансов связи между двумя устройствами DCE. Позднее появился обновленный вариант этого стандарта — V.8bis, который также определял некоторые стандарты связи между устройствами DTE, осуществляемой по каналу оборудования DCE.
- **V.21, V.23, V.27ter, V.29.** Эти стандарты определяли параметры связи со скоростями, соответственно, 300, 600/1200, 2400/4800 и 9600 бод.
- **V.25, V.25bis, V.25ter.** Серия стандартов для автоматизированного набора номера, ответа и контроля связи.

В конце 80-х годов прошлого века модемы стали гораздо сложнее. Одной из причин этого стало прекращение использования в 1984 году системы Белла. С появлением на частных предприятиях собственного оборудования возникшая конкуренция стимулировала разработку более скоростных соединений. Появились следующие стандарты.

- **V.32bis, V.34, V.90.** Стандартизация скоростей взаимодействия 14400, 33600 и вплоть до 56000 бод.
- **V.110.** Этот стандарт позволил асинхронному терминальному устройству использовать передающее оборудование ISDN (терминальный адаптер).

Первыми серверами доступа были модели AS2509 и AS2511. Сервер AS2509 поддерживал восемь входных подключений с использованием внешних модемов, а AS2511 — 16 таких подключений. Также была представлена модель AS5200 с двумя первичными интерфейсами обмена, которая поддерживала 48 пользователей, используя цифровые модемы, что было серьезным шагом вперед в развитии технологии коммутируемых соединений. Плотность модемов постоянно увеличивалась: модель AS5300 поддерживала сначала четыре, а затем восемь первичных интерфейсов обмена. Затем появилась модель AS5800, которая могла удовлетворить потребности операторов связи, которые должны

были обслуживать десятки входных подключений по линиям T1 и сотни пользовательских подключений.

Говоря об истории технологии коммутируемых соединений, следует упомянуть о некоторых ныне устаревших технологий. 56 Kflex — предшествовавший V.90 стандарт модемов 56K, предложенный фирмой Rockwell. Внутренние модемы Cisco поддерживают версию 1.1 стандарта 56 Kflex, однако корпорация рекомендует при первой возможности перевести пользовательские модемы на стандарт V.90. Другой ныне устаревшей технологией является сервер AS5100, который представляет собой совместный проект корпорации Cisco и производителя модемов. AS5100 был создан как один из способов повышения плотности модемов путем использования квадратурных модемных плат. Проект предусматривал использование AS521 в виде плат, устанавливаемых на заднюю панель, совместно используемую квадратурными модемными платами, и двойной платы T1.

В настоящее время коммутируемые соединения по-прежнему являются экономичной альтернативой выделенным линиям (в зависимости от конкретных требований, предъявляемых к соединению). Они важны и как запасные линии связи на тот случай, если основная линия выйдет из строя. Коммутируемые соединения также предоставляют возможность создания динамических соединений.

Технология коммутируемых соединений

В этом разделе представлена информация о различных типах коммутируемых соединений, в том числе о расширенных возможностях и различных методах подключения.

Общедоступная телефонная сеть

Общедоступной телефонной сетью (Plain Old Telephone Service — POTS) называют обычные телефонные линии, используемые для передачи голоса. Они широко распространены, привычны и доступны; местные звонки обычно бесплатны. Именно на базе этой службы была построена телефонная сеть. При преобразовании в цифровые сигналы частота дискретизации звука, передаваемого по таким линиям, составляет 8000 Гц (по 8 битов на одну выборку), что позволяет передавать звук с приемлемым качеством по 64-килобитовому каналу.

Внимание!

Возникает, однако, естественный вопрос: какое качество следует считать приемлемым? Исследования показали, что частота человеческого голоса находится в пределах от 300 до 3400 Гц. Казалось бы, частота 4000 Гц должна быть достаточной, но, согласно теореме Найквиста, частота выборки должна быть вдвое большей, чтобы покрыть как высоко-, так и низкочастотные составляющие звуковых волн.

Кодирование и декодирование звуковой информации осуществляется с помощью телекоммуникационного устройства, называемого кодеком. Кодек потребовался для обратной совместимости с традиционными аналоговыми телефонами, которые уже были широко распространены, когда появилась цифровая сеть. Поэтому большинство домашних телефонов в тот момент представляли собой простые аналоговые аппараты.

Скорость соединения по коммутируемым линиям обычной телефонной сети через модем исторически была ограничена значением 33600 бит/с , которое часто называют скоростью V.34. Последние усовершенствования позволили увеличить скорость пере-

дачи данных от цифрового источника модему, подключенному к обычной телефонной сети, однако использование телефонных каналов на обоих концах соединения все равно приводит в результате к скорости V.34 в обоих направлениях.

Базовый интерфейс ISDN

Такое применение сети ISDN предназначено для домашнего использования. В этом случае сигналы идут по тому же телефонному кабелю общедоступной сети, однако при этом обеспечивается непосредственное цифровое подключение к телефонной сети. Для этого требуется специальное оборудование, называемое терминальным адаптером (хотя в некоторых странах он встраивается в маршрутизатор или телекоммуникационное оборудование). Всегда следует проверить маркировку (S/T или U), ибо вилка, подключаемая к стенной розетке, в обоих случаях выглядит одинаково. Обычно интерфейс BRI ISDN (Basic Rate Interface — BRI) имеет два B-канала (от слова bearer — носитель) для передачи данных и один D-канал (от слова delta) для управления каналом и сигнализации. У местных телефонных компаний могут быть различные схемы их использования. Каждый B-канал является линией со скоростью передачи 64 Кбит/с. Отдельные 64-килобитовые каналы телефонной сети обычно называют цифровой службой нулевого уровня (digital sevice 0 — DS0). Как будет показано ниже в данной главе, такое соединение является "общим знаменателем", не зависящим от типа предлагаемых услуг.

Интерфейс BRI представляет собой выделенное подключение к коммутатору, которое сохраняется даже при отсутствии звонков.

Внимание!

Как удается использовать три канала на одной паре проводов? Такой процесс называется мультиплексной передачей (мультиплексированием) с разделением времени (Time Division Multiplexing — TDM). Сигналы, передаваемые по кабелю, делятся на "временные окна" (или таймслоты). Это означает, что при инициализации оба конца линии связи должны быть синхронизированы. О работоспособности линии можно судить по состоянию MULTIPLE_FRAME_ESTABLISHED, которое, кроме всего прочего, означает, что произошла синхронизация и два соединенных устройства обмениваются TDM-фреймами.

Линии T1/E1

Линии связи T1/E1 предназначены для коммерческого использования. Линии T1 имеют 24 TDM-канала, проходящие по кабелю, который состоит из двух пар медных проводов. Линия E1 имеет 32 канала, однако один из них предназначен для синхронизации фреймов. Как и в случае с интерфейсом BRI, линия T1/E1 подключается непосредственно к коммутатору. Линия является выделенной, поэтому как и в случае с интерфейсом BRI, линия T1/E1 подключена к коммутатору постоянно, даже при отсутствии вызовов. Каналы линий T1/E1 являются B-каналами, т.е. каналами DS0 со скоростью передачи 64 Кбит/с. Линии T1/E1 называют также цифровой службой первого уровня (DS1).

В США и Канаде в сетях T1 для синхронизации отдельных каналов используются фреймы. Каждый фрейм в линиях T1 имеет 24 9-битовых канала (8 битов данных и 1 бит для разделения фреймов). Таким образом, общая длина фрейма составляет 193 бита. Передавая 8000 таких фреймов в секунду, линия T1 обеспечивает скорость

передачи между коммутатором и оборудованием пользователя (Customer Premises Equipment — CPE) 1,544 Мбит/с.

На линиях E1 для синхронизации также применяются фреймы, но линия E1 имеет 32 8-битовых канала, поэтому длина фрейма составляет 256 битов. При той же частоте 8000 Гц канал обеспечивает скорость передачи данных между коммутатором и пользователем, равную 2048 Мбит/с. Линии E1 являются наиболее распространенными.

Выбор кодирования в линии и схемы фреймов (чтобы коммутатор и устройство пользователя "поняли" друг друга) зависит от региона. Например, в США и Канаде наиболее распространенной схемой кодирования является двоичная подстановка 8-нулевых битов (Binary 8 Zero Substitution — B8ZS), а наиболее распространенным типом фреймов — расширенный суперфрейм (Extended Super Frame — ESF). Телефонные компании, предоставляющие службу T1/E1, при заключении договора о предоставлении службы должны указать вид кодирования в линии и способ создания фреймов.

Для коммутируемых соединений используются два типа линий T1/E1: интерфейс первичной скорости передачи (Primary Rate Interface, PRI) и канально-ассоциированная сигнальная система (Channel Associated Signaling — CAS). Линии T1/E1 с интерфейсами PRI и CAS обычно расположены в центрах, к которым поступают вызовы от удаленных узлов и отдельных пользователей.

Интерфейс первичной скорости передачи

Служба интерфейса первичной скорости передачи (Primary Rate Interface — PRI) имеет 23 B-канала со скоростью передачи 64 Кбит/с и один D-канал (24-й) для сигнализации при вызове. Потери, связанные с использованием одного из каналов для сигнализации, можно несколько уменьшить при помощи NFAS, что позволяет нескольким интерфейсам PRI использовать общий D-канал. При использовании PRI-интерфейса служба линии E1 обеспечивает 30 каналов, однако 16-й канал используется для сигнализации ISDN. Службы PRI являются ISDN-подключениями. Они позволяют отправлять и принимать по линии T1/E1 как звуковые (через модем), так и "натуральные" ISDN-вызовы. Службы этого типа часто используются на серверах доступа, поскольку обеспечивают более высокие скорости передачи.

Канально-ассоциированная сигнальная система

Линии T1 канально-ассоциированной сигнальной системы (Channel Associated Signaling — CAS) имеют 24 канала со скоростью передачи 56 Кбит/с. Часть каждого канала используется для сигнализации вызова. Службы этого типа также называют сигнализацией заимствованного бита (robbed-bit signaling). В линиях E1, использующих CAS для сигнализации вызова, до сих пор используется только 16-й канал, однако для аналоговых вызовов применяется международный стандарт R2.

В CAS не используется интерфейс ISDN и на сервер доступа поступают только аналоговые вызовы. Часто это делается для того, чтобы сервер доступа мог работать с группой каналов. Такой подход широко распространен в Южной Америке, в Европе и Азии.

Внимание

Какие сигналы нужны для канала сигнализации при вызове? Каждый из двух участников обмена данными должен информировать другого о том, что происходит с сообщением, например передавать идентификационные данные абонента, сообщать о том, ответил

абонент или нет, передавать параметры вызова. Если в сообщении, посланном с коммутатора, говорится о том, что поступил новый входящий звонок, то устройство пользователя должно сообщить коммутатору, какие каналы являются доступными. Если коммутатор направляет вызов на канал, который к этому не готов, то коммутатор получит сообщение о недоступности данного канала. Сервер доступа должен иметь последнюю информацию о состоянии своих линий связи и быть готовым к согласованию с коммутатором входящих и исходящих вызовов.

Модемы

С точки зрения терминологии, модем является устройством для передачи данных (Data Communication Equipment — DCE), а устройство, использующее модем, — терминальным оборудованием (Data Terminal Equipment — DTE). Как уже говорилось выше, модемы, для обеспечения совместимости с другими модемами, должны соответствовать ряду коммуникационных стандартов, в том числе стандартам Bell103, Bell212A, V.21, V.22, V.22bis, V.23, V.32, V.32bis, V.FC, V.34. Эти стандарты соответствуют модели двойного аналогового преобразования(рис. 15.1).

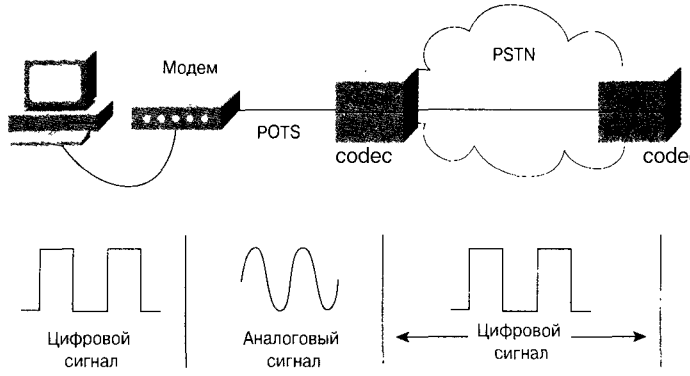


Рис. 15.1. Коммуникационные стандарты соответствуют модели двойного аналоговую преобразования

Развитие технологий использования серверов доступа позволило создать новые стандарты, такие как X2, 56 Kflex и V.90, которые используют преимущества усовершенствованного сервера. Появившиеся ранее частные стандарты X2 и 56 Kflex с появлением V.90 морально устарели. Все эти стандарты построены на предположении, что сервер доступа связан с телефонной сетью цифровым каналом. Эта новая модель показана на рис. 15.2.

Следует обратить внимание на то, что сигнал преобразуется в аналоговый лишь один раз. Поскольку это преобразование выполняется на стороне пользователя, поток данных, генерируемый пользовательским модемом, ограничен скоростью V.34. Поток данных от сервера доступа не содержит шумов, вызываемых аналоговым преобразованием, поэтому он может передаваться на значительно большей скорости. Таким образом, пользователь имеет возможность получать данные со скоростью V.90, но отправлять только со скоростью V.34.

Возникает вопрос о том, как в реальности работает такая схема. На рис. 15.3 показан общий поток данных, проходящий через модем.

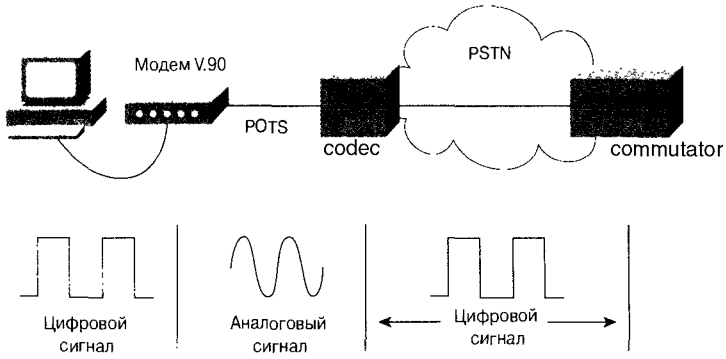


Рис. 15.2. Модель, отраженная в новых стандартах

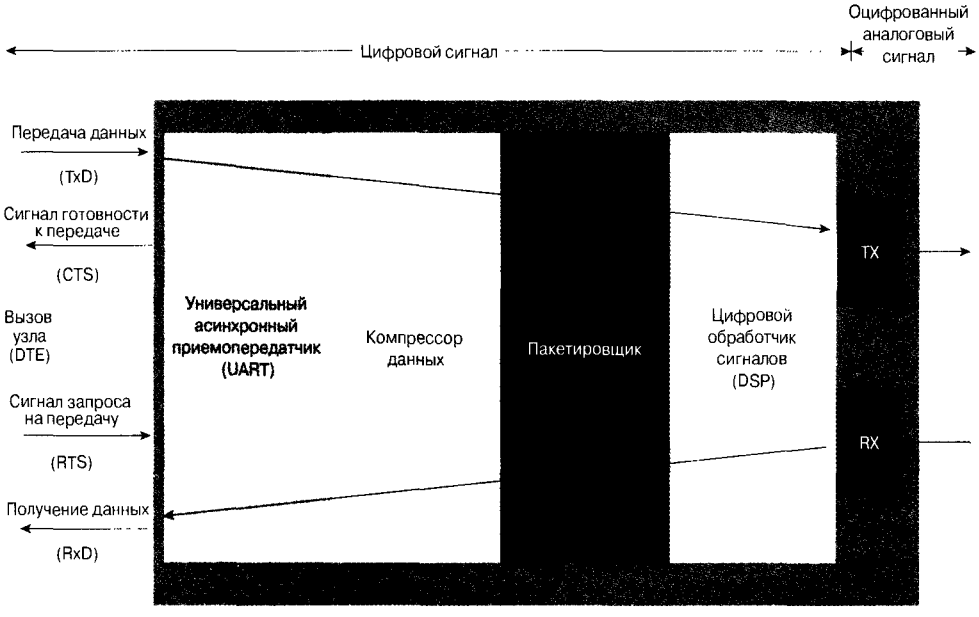


Рис. 15.3. Общий поток данных, проходящий через модем

Исходящие от терминального устройства данные направляются через универсальный асинхронный приемопередатчик (трансивер)(Universal Asynchronous Receiver/Transmitter — UART), осуществляющий буферизацию и контроль обмена данными с узлом. Устройство или программа сжатия данных передает данные программе, создающей пакеты, которая записывает в них контрольную сумму и отправляет их процессору обработки цифровых сигналов (Digital Signal Processor — DSP). Этот процессор также выполняет повторную передачу, в случае если данные не дойдут до следующего передающего устройства. Затем данные попадают на цифро-аналоговый преобразователь, который посылает их через разъем RJ11 в телефонную линию. Получение информации происходит в обратном порядке.

Теоретически модемы V.90 могут посылать данные со скоростью 56 Кбит/с, однако из-за ограничений, налагаемых на телефонные линии государственными структурами, скорость 53 Кбит/с является в настоящее время максимально возможной.

Протокол PPP

Протокол PPP является жизненно важным для работы коммутируемых соединений. До появления протокола PPP в 1989 году (стандарт RFC 1134; в настоящее время используются RFC с номерами до RFC 1661) протоколы коммутируемых соединений были связаны с используемыми сетевыми протоколами. Чтобы использовать несколько протоколов, требовалось инкапсулировать данные всех других протоколов в пакеты протокола, используемого коммутируемым соединением. Многие из фирменных протоколов передачи (в частности протокол SLIP) даже не имели возможности обсуждения адресации. Однако протокол PPP выполняет эту и многие другие задачи, обладает достаточной гибкостью и возможностями расширения. Установка PPP-соединения происходит в три этапа, на которых используются: протокол контроля подключения (Link Control Protocol — LCP), протокол аутентификации и протокол управления сетью (Network Control Protocol — NCP). (Более подробная информация о протоколе PPP приведена в главе 13 "Протокол PPP ".)

Протокол LCP

Протокол LCP выполняет функции самого нижнего уровня в стеке протоколов PPP. Поскольку PPP не использует модель "клиент-сервер", оба конца соединения "точка-точка" должны согласовать используемые протоколы. В начале такого согласования каждый из узлов, желающих установить PPP-соединение, должен отправить конфигурационный запрос (CONFREQ). В CONFREQ включены все параметры соединения, не настраиваемые по умолчанию. Обычно это максимальное количество принимаемых модулей данных, таблица асинхронных управляющих кодов, протокол аутентификации и "магическое число". На этой стадии узлы согласовывают метод аутентификации и определяют, будут ли они поддерживать многоканальный PPP.

В обычном потоке сообщений протокола LCP, используемых для согласования, присутствуют три следующих возможных ответа на любой запрос CONFREQ.

1. Если узел распознал все параметры запроса CONFREQ и согласен с их значениями, то он высылает сообщение о подтверждении конфигурации (Configure-Acknowledge — CONFACK).
2. Если какой-либо из параметров запроса CONFREQ не распознан (например, параметры, присущие определенному производителю) или значения некоторых параметров явно недопустимы в конфигурации данного узла, то он высылает сообщение с отказом от данной конфигурации (CONFigure-REJect — CONFREJ).
3. Если все параметры CONFREQ распознаны, но их значения неприемлемы для данного узла, то он высылает отрицательное подтверждение конфигурации (Configure-Negative-Acknowledge — CONFNAK).

Обмен сообщениями CONFREQ, CONFREJ и CONFNAK продолжается до тех пор, пока оба узла не отправят друг другу сообщения CONFACK, или пока не прервется соединение, или пока оба узла признают, что согласование не может быть достигнуто.

Аутентификация

Аутентификация является необязательным этапом, но ее проведение *настоятельно* рекомендуется для всех коммутируемых соединений. В некоторых случаях она необходима для правильной работы, например, при использовании профилей набора.

Протокол PPP использует два основных типа аутентификации: протокол аутентификации по паролю (Password Authentication Protocol — PAP) и протокол аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol — CHAP), определенные в RFC 1334 и обновленные в RFC 1994.

Говоря об аутентификации, удобно использовать термины *запрашивающая сторона* (requester) и *удостоверяющая сторона* (authenticator), отражающие роль устройств, расположенных на концах соединения.

Запрашивающей стороной называют устройство, которое запрашивает доступ к сети и предоставляет аутентификационную информацию; *удостоверяющая сторона* подтверждает достоверность этой информации и разрешает либо запрещает подключение. Когда между маршрутизаторами устанавливается DDR-соединение, обычно обе стороны по очереди выступают в обеих этих ролях.

Протокол PAP достаточно прост. После успешного LCP-согласования запрашивающая сторона продолжает посылать свое имя и пароль до тех пор, пока удостоверяющая сторона не ответит подтверждением или пока не прервется связь. Если удостоверяющая сторона определит, что комбинация имени и пароля неверна, то она может разорвать соединение.

Протокол CHAP несколько сложнее. Удостоверяющая сторона направляет запрашивающей стороне вызов, на который последняя отвечает некоторым значением. Это значение вычисляется с помощью функции "одностороннего совмещения", чтобы совместить запрос и CHAP-пароль. Результат отправляется удостоверяющей стороне в виде ответного сообщения вместе с CHAP-именем узла запрашивающей стороны (которое может отличаться от обычного имени узла).

Удостоверяющая сторона читает в ответном сообщении имя узла, находит для этого имени ожидаемый пароль и вычисляет значение, которое она ожидает получить от запрашивающей стороны, проделывая описанную выше операцию совмещения. Если полученные значения совпадают, то аутентификация считается успешно законченной. Несовпадение этих значений приводит к разрыву соединения. Согласно стандартам RFC, подтверждающая сторона во время соединения в любой момент может выполнить повторный запрос на аутентификацию .

Протокол NCP

Согласование по протоколу NCP во многом аналогично LCP-согласованию и также использует сообщения CONFREQ, CONFREJ, CONFNAK и CONFACK. Однако на этой стадии согласовываются элементы протоколов более высокого уровня — IP, IPX, мостовых протоколов, CDP и т.д. Могут согласовываться один или несколько таких протоколов. Более подробно эти протоколы описаны в следующих стандартах RFC:

- RFC 1332 "IP Control Protocol";
- RFC 1552 "IPX Control Protocol";
- RFC 1378 "AppleTalk Control Protocol";
- RFC 1638 "Bridging Control Protocol";

- RFC 1762 "DECnet Control Protocol";
- RFC 1763 "VINES Control Protocol".

Дополнительные замечания

Функции многосвязного протокола "точка-точка" (MultiLink Point-to-point protocol — MLP, RFC 1990) обеспечивают разделение и объединение пакетов в единую конечную систему через логический канал (также называемый пучком), образованный несколькими линиями связи. Многосвязный PPP обеспечивает предоставление по требованию необходимой пропускной способности и снижает задержку передачи по распределенной сети. В то же время он обеспечивает взаимодействие оборудования разных производителей, фрагментацию пакетов с соблюдением правильной последовательности и вычисление нагрузки как для входящих, так и для исходящих потоков данных. Разработанный корпорацией Cisco многосвязный PPP поддерживает фрагментацию и требования по обеспечению правильного порядка пакетов, описанные в RFC 1717.

Многосвязный PPP работает со следующими типами интерфейсов (с одним или несколькими):

- асинхронные последовательные интерфейсы;
- интерфейс BRI;
- интерфейс PRI.

Многоопорный многосвязный PPP (Multichassis Multilink PPP — MMP), напротив, обеспечивает дополнительную возможность разрыва соединения на нескольких маршрутизаторах с различными удаленными адресами. MMP также может работать как с аналоговыми, так и с цифровыми данными.

Эти функции предусмотрены для ситуаций, когда работает большое количество пользователей, подключенных по коммутируемой линии, и есть лишь один сервер доступа, который не может обеспечить достаточное количество коммутируемых портов. Протокол MMP позволяет компаниям использовать один телефонный номер для всех пользователей независимо от типа вызова — аналогового или цифрового. Эта функция, в частности, предоставляет возможность провайдерам службы Internet выделять один ISDN-номер для нескольких первичных ISDN-интерфейсов обмена и не беспокоиться о том, попадает ли второе подключение пользователя на этот же маршрутизатор.

Протокол MMP не требует изменения настройки коммутаторов телефонной компании.

Протокол аутентификации, авторизации и учета (AAA)

Еще одной важной технологией, которую следует упомянуть, является использование аутентификации, авторизации и учета (Authentication, Authorization, and Accounting — AAA). В AAA используется протокол TACACS или протокол RADIUS. Эти два протокола разработаны для поддержки централизованного метода регистрации работы пользователей и доступа к сети. Использование AAA осуществляется путем настройки сервера (или группы серверов) для централизованного администрирования базы данных, содержащей информацию о пользователях. Такая информация, как пароль пользователя, адрес, который следует ему присвоить, протоколы,

которыми ему разрешено пользоваться, может контролироваться с одной рабочей станции. Протокол AAA также имеет мощные средства аудита, которые можно использовать для наблюдения за важными для администрирования показателями, такими как скорость соединений и причины отключений. Протокол AAA следует использовать в любой средней или крупной системе коммутируемых соединений, но и в небольших учреждениях его применение вполне оправдано.

Методы реализации коммутируемых соединений

Большинство маршрутизаторов поддерживают автоматическое соединение динамических каналов при поступлении предназначенных для них потоков данных. В реализации Cisco это называется маршрутизацией по требованию (Dial-on-Demand Routing — DDR). Она обеспечивает экономичное соединение по распределенной сети, создаваемое по мере необходимости, которое может использоваться как в качестве основного, так и в качестве резервного некоммутируемого последовательного канала связи.

В своей основе маршрутизация DDR представляет собой просто дополнение к обычной маршрутизации. Представляющие интерес пакеты направляются на интерфейс номеронабирателя , который предпринимает попытку набора номера. Понятия *интерфейс номеронабирателя* и *поток данных, представляющих интерес* требуют отдельного пояснения.

Что такое номеронабиратель?

Термин *номеронабиратель* (dialer) имеет несколько значений в зависимости от особенностей конфигурации, но обычно это интерфейс, где, собственно, и происходит маршрутизация. Этому интерфейсу известен адрес и телефонный номер того пункта, куда должен быть доставлен поток данных. При просмотре таблицы маршрутизации маршрутизатор находит в ней тот интерфейс номеронабирателя, который указан как адрес следующего перехода на пути к сети-получателю. Интерфейс номеронабирателя не обязательно должен быть физическим интерфейсом, выполняющим набор номера, но может и быть таковым, если на физическом интерфейсе выполнена конфигурационная команда **`dialer in-band`**. После ее выполнения интерфейс становится номеронабирателем. Например, асинхронный интерфейс не является номеронабирателем по умолчанию, однако если выполнить на нем конфигурационную команду **`dialer in-band`**, то у него появятся функции номеронабирателя. В частности, вызовам, полученным по такому асинхронному интерфейсу после выполнения указанной выше команды, с момента ее выполнения будет назначено время ожидания. Примером физического интерфейса, являющегося также номеронабирателем, является интерфейс BRI.

Внимание!

В IOS Cisco для отсчета времени подключения, в течение которого не передаются предстаающие интерес данные, используется таймер ожидания. По умолчанию он установлен на 2 мин, по истечении которых неактивное соединение прерывается.

Кроме физических интерфейсов, используемых в качестве номеронабирателей, существуют так называемые интерфейсы номеронабирателя. Они представляют собой

логические интерфейсы, которые связываются с реальными интерфейсами для осуществления вызова. Преимущество интерфейсов номеронабирателя заключается в их гибкости. Группа потенциальных DDR-подключений может совместно использовать несколько BRI-интерфейсов. Существует два вида конфигурации интерфейса номеронабирателя: карта номеров (иногда называемая традиционной маршрутизацией DDR) и профиль. Выбор одного из них зависит от конкретной ситуации, в которой осуществляется соединение. Использование DDR-маршрутизации на базе карты номеров впервые появилось в версии IOS 9.0, а на базе профиля — в версии 11.2.

Представляющие интерес данные

Под представляющими интерес (interesting) данными понимаются пакеты или потоки данных, по которым либо будет предпринята попытка вызова, если связь уже установлена, либо будет сброшен таймер ожидания на интерфейсе номеронабирателя. Для того чтобы пакет представлял интерес, он должен отвечать следующим требованиям:

- пакет должен соответствовать критерию "допуска", определенному списком доступа;
- на список доступа должен ссылаться список номеронабирателя или пакет должен соответствовать такому протоколу, который всегда допускается списком номеронабирателя;
- список номеронабирателя должен быть связан с интерфейсом номеронабирателя посредством группы номеронабирателя.

Пакеты никогда не считаются представляющими интерес по умолчанию. Описания представляющих интерес пакетов должны быть явным образом включены в конфигурацию маршрутизатора или сервера доступа.

Преимущества и недостатки коммутируемых соединений

Преимуществами коммутируемых соединений являются их гибкость и экономичность. Сначала необходимо понять, почему для них столь важна гибкость. Периодическое соединение чаще всего требуется для мобильных устройств. Мобильный работник должен быть в состоянии подключиться отовсюду, где бы он ни находился. Телефонные линии доступны практически повсеместно, поэтому для мобильных пользователей подключение через модем является единственным разумным вариантом.

Если пользователь находится далеко от офиса, то он часто дозванивается до местного провайдера службы Internet и использует IPSec-туннель для доступа к шлюзу, а уже оттуда получает доступ ко всей корпоративной сети. В данном случае телефонный звонок является бесплатным, а оплата услуг провайдера будет значительно ниже, чем стоимость междугородного звонка. Еще одним примером является ситуация, когда BRI-интерфейс, подключенный к центральному офису, находящемуся в регионе с недорогими услугами ISDN, имеет серверы баз данных, настроенные на коммутируемое соединение с другими узлами и периодически обменивающиеся с ними информацией. Каждый узел нуждается всего лишь в одном BRI-канале, что гораздо дешевле, чем выделенные линии для каждого удаленного адреса. Кроме того, если коммутируемое соедине-

ние используется в качестве запасного, то достигается дополнительная экономия: если основной канал связи выходит из строя, то работа продолжается, хотя и медленнее обычного.

Однако экономичность коммутируемых соединений имеет и оборотную сторону, состоящую в том, что затраты на связь по очень загруженной линии оказываются выше, чем стоимость выделенной линии, а при передаче данных на дальние расстояния она становится еще большей.

Выбирая тип доступа, следует также учитывать скорость передачи. Коммутируемые соединения отличаются высокой пропускной способностью, особенно для каналов, объединенных по протоколу Multilink PPP, однако связь по выделенной линии через последовательный порт может оказаться эффективнее.

Еще одним фактором, который необходимо учитывать, является безопасность. Конечно, любое PPP-соединение должно проходить аутентификацию, но в принципе оно все же позволяет каждому владельцу телефона вторгнуться в систему. Значительная часть конфигурирования любой коммутируемой системы состоит в придании ей способности не пропускать нежелательных гостей. Это, к счастью, возможно, и в AAA достигнут значительный прогресс в решении данной проблемы. Однако недостатком является сама принципиальная возможность проникновения потенциальных злоумышленников через коммутируемые соединения.

Резюме

Технология коммутируемых соединений существует в течение длительного времени, однако только за последние примерно двадцать лет телефонные линии стали доступны для компьютерных сетей. За это время был разработан ряд стандартов, гарантирующих корректное взаимодействие между модемами и использующими их системами. Корпорация Cisco вышла на рынок серверов доступа с моделями AS2509 и AS2511, которые использовали внешние аналоговые модемы, однако в настоящее время она производит серверы доступа, построенные на технологии цифровых модемов.

Современные технологии коммутируемых соединений по-прежнему применяют обычные телефонные сети — дешевый и повсеместно распространенный способ соединения через модем. Для этого используются одиночные каналы DS0. Шагом вперед по сравнению с телефонной линией является линия BRI ISDN с двумя каналами DS0 и одним D-каналом, используемым для сигнализации. На промышленном уровне применяются линии T1/E1. Линия T1 имеет 24 канала, а линия E1 — 32, хотя E1 использует нулевой канал для разделения на фреймы и 16-й канал для сигнализации при установке вызова. Служба PRI-интерфейса ISDN предназначена для соединения клиентов ISDN, а сигнализация CAS пропускает только асинхронные вызовы.

За последние годы значительно усовершенствовались сами модемы. В настоящее время они обеспечивают прямое цифровое подключение по телефонной линии к модему сервера доступа. Это привело к появлению соединений V.90, позволяющих передавать данные клиенту от сервера со скоростью до 53 Кбит/с. Но из-за необходимости аналогового преобразования для передачи по аналоговой линии связи передача данных от клиентского модема пока что может осуществляться только со скоростью до 33,6 Кбит/с.

После того как соединение установлено, необходимо обеспечить надежную передачу данных. Эту потребность удовлетворяет протокол PPP. Благодаря трехэтапной процедуре установки соединения (использование протокола LCP, протокола аутенти-

фикации и протокола NCP) протокол PPP адаптируется к условиям среды и анализирует относящуюся к соединению информацию, а также имеет надежную схему аутентификации. Протокол PPP допускает передачу данных через "пучок" соединений благодаря использованию опции многоканального Multilink PPP. Еще одним шагом вперед является расширение возможностей Multilink PPP за счет многоопорности. Для крупных организаций эту возможность трудно переоценить, поскольку она обеспечивает сеансы Multilink PPP по любому свободному каналу DS0.

С маршрутизацией по требованию (Dial-on-Demand Routing — DDR) связаны два важных понятия: номеронабиратель и представляющие интерес данные. Номеронабиратель представляет собой интерфейс, управляющий маршрутизацией и контролирующий поступление вызова. Под представляющими интерес данными подразумеваются потоки данных, для которых нужно либо прервать, либо продолжить соединение.

В каких случаях следует использовать коммутируемые соединения? Ответ на этот вопрос зависит от поставленных конкретной ситуацией целей. При некоторых обстоятельствах, например, для мобильных пользователей, коммутируемые соединения являются единственным решением проблемы. В тех случаях, когда выходить на связь требуется лишь время от времени, коммутируемые соединения также будут наиболее экономичным решением. Однако в тех случаях, когда требуется поддерживать соединение практически постоянно, коммутируемые соединения приведут к большим затратам. Еще одной проблемой является скорость передачи — коммутируемые соединения обычно работают медленнее, чем выделенные линии. Обеспечить безопасность узлов, подключенных к телефонной сети, в этом случае также непросто.

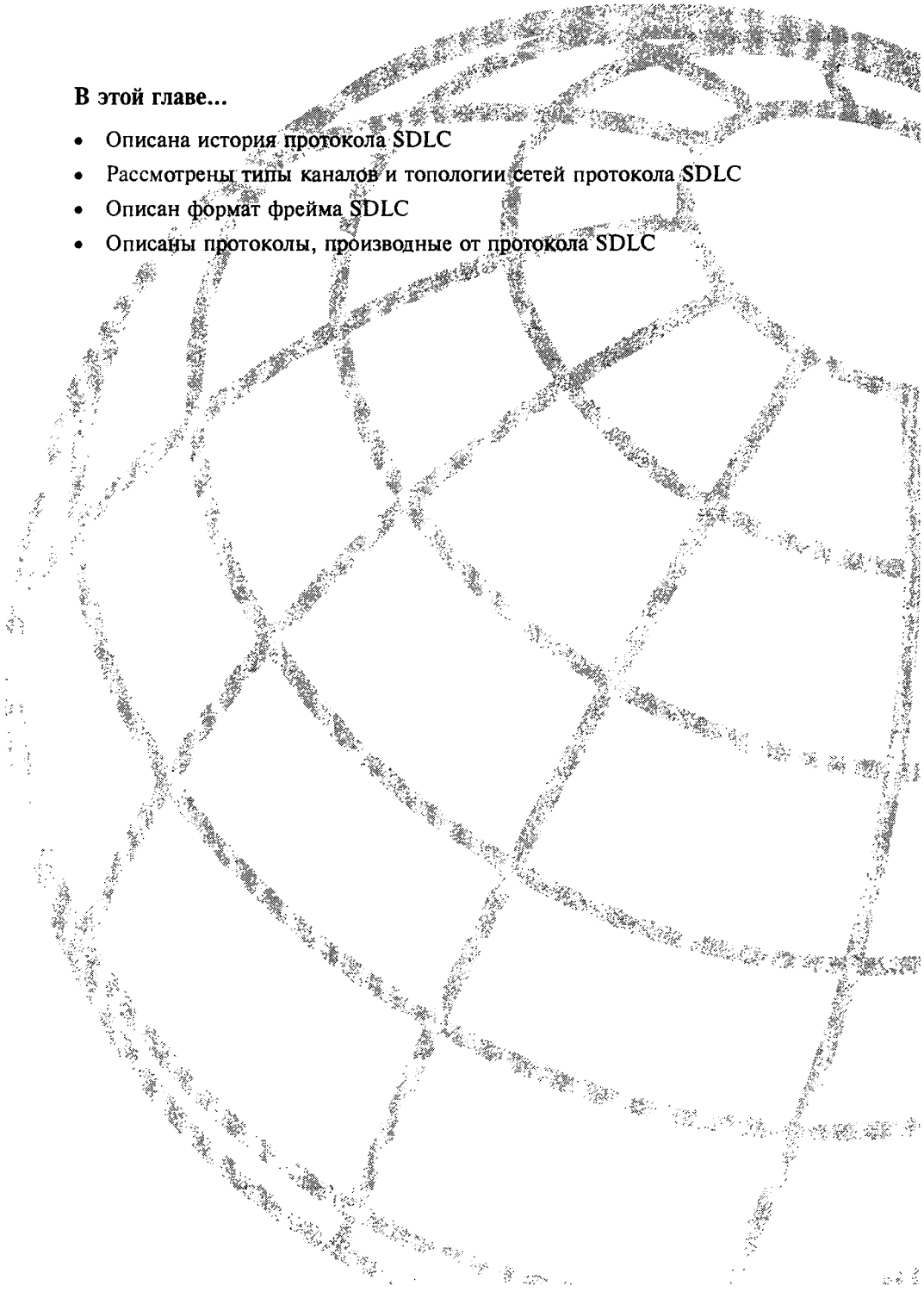
Очевидно, что сегодня технология коммутируемых соединений играет важную роль на внешних границах сети, обеспечивая доступ к ней мобильных пользователей, а также пользователей из тех регионов, где просто нет ничего лучшего. В ситуациях, требующих гибкости установки соединения, или в тех случаях, когда соединение требуется лишь изредка, коммутируемые соединения являются вполне приемлемым решением.

Контрольные вопросы

1. Сколько лет потребовалось для того, чтобы количество телефонов в американских домах достигло 90%?
2. Какие рекомендации V-серии относятся к скорости передачи?
3. Сколько каналов DS0 в линиях BRI-интерфейса, T1 и E1?
4. Что представляет собой поток данных, поступающий через модем от разъема RJ 11 к терминальному устройству?
5. Из каких трех этапов состоит согласование PPP? Почему так важно соблюсти их последовательность?
6. Как связаны между собой представляющие интерес данные и таймер задержки?
7. Является ли интерфейс BRI номеронабирателем? Как асинхронный интерфейс может стать номеронабирателем?
8. В каких случаях целесообразно использовать коммутируемые соединения, а когда нет?

Дополнительные источники

1. Cisco Systems. *Cisco IOS Dial Solutions.* Cisco Press, 1998.
2. ftp://ftp.cisco.com/pub/rfc/RFC/.
3. http://hea-www.harvard.edu/~fine/ISDN/overview.html.
4. http://isds.bus.lsu/edu/cvoc/projects/TechLibrary/CableIS/history.html.
5. http://www.att.com/history/.
6. http://www.cisco.com/tac/.
7. http://www.digitalcentury.com/encyclo/update/cmodem.html.
8. http://www.itu.int/itudoc/itu-t/rec/v/.



В этой главе...

- Описана история протокола SDLC
- Рассмотрены типы каналов и топологии сетей протокола SDLC
- Описан формат фрейма SDLC
- Описаны протоколы, производные от протокола SDLC

Глава 16

Протокол SDLC и его производные

Введение

Корпорация IBM разработала *протокол управления синхронной передачей данных (Synchronous Data Link Control — SDLC)* в середине 70-х годов XX века для использования в средах системной сетевой архитектуры SNA (Systems Network Architecture — SNA). SDLC был первым синхронным, бит-ориентированным протоколом канального уровня. В настоящей главе будут описаны основные функциональные характеристики протокола SDLC и перечислены некоторые производные от него протоколы.

Корпорация IBM представила протокол SDLC на рассмотрение различных комитетов по стандартизации. Международная организация по стандартизации (ISO) модифицировала SDLC, создав высокоуровневый протокол управления каналом (High-Level Data Link Control — HDLC). Международный телекоммуникационный союз (ITU-T, бывший Международный консультативный комитет по телеграфии и телефонии, CCITT), в свою очередь, внес изменения в протокол HDLC, создав протокол процедуры доступа к каналу (Link Access Procedure — LAP), а затем протокол процедуры сбалансированного доступа к каналу LAPB (Link Access Procedure, Balanced — LAPB). Институт инженеров по электротехнике и электронике (IEEE) изменил протокол HLDC, создав протокол IEEE 802.2. Каждый из этих протоколов нашел свою область применения, но основным протоколом канального уровня в архитектуре SNA для соединений по распределенной сети остается SDLC.

Типы каналов и топологии SDLC

Протокол SDLC поддерживает несколько типов каналов и топологий. Он может использоваться в соединениях типа "точка-точка" и в многоточечных соединениях, в ограниченных и неограниченных средах, полудуплексном и дуплексном режимах передачи, в сетях с коммутацией каналов и коммутацией пакетов.

В протоколе SDLC различаются два типа сетевых узлов: первичные и вторичные. *Первичные узлы* управляют работой других станций, называемых вторичными. Первичный узел опрашивает вторичные в установленном порядке, после чего вторичные могут начинать передачу, если у них есть данные для передачи. Кроме того, первичный узел устанавливает и ликвидирует соединения, а также управляет активным со-

единением. *Вторичные узлы* управляются первичными. Это означает, что они имеют возможность посылать информацию первичному узлу только в том случае, если последний даст на это разрешение.

Первичные и вторичные узлы протокола SDLC могут образовывать следующие четыре основные конфигурации.

- **"Точка-точка".** Состоит только из двух узлов — первичного и вторичного.
- **Многоточечная.** Состоит из одного первичного и нескольких вторичных узлов.
- **Замкнутая.** Первичный узел соединен с первым и последним вторичными узлами. Промежуточные вторичные узлы, отвечая на запросы первичного узла, передают сообщения по цепочке.
- **Концентраторная.** Используются входящий и исходящий каналы. По исходящему каналу первичный узел связывается со вторичными. По входящему каналу вторичные узлы связываются с первичным. Входящий канал проходит к первичному узлу через все вторичные узлы.

Формат фрейма протокола SDLC

Формат фрейма SDLC показан на рис. 16.1.

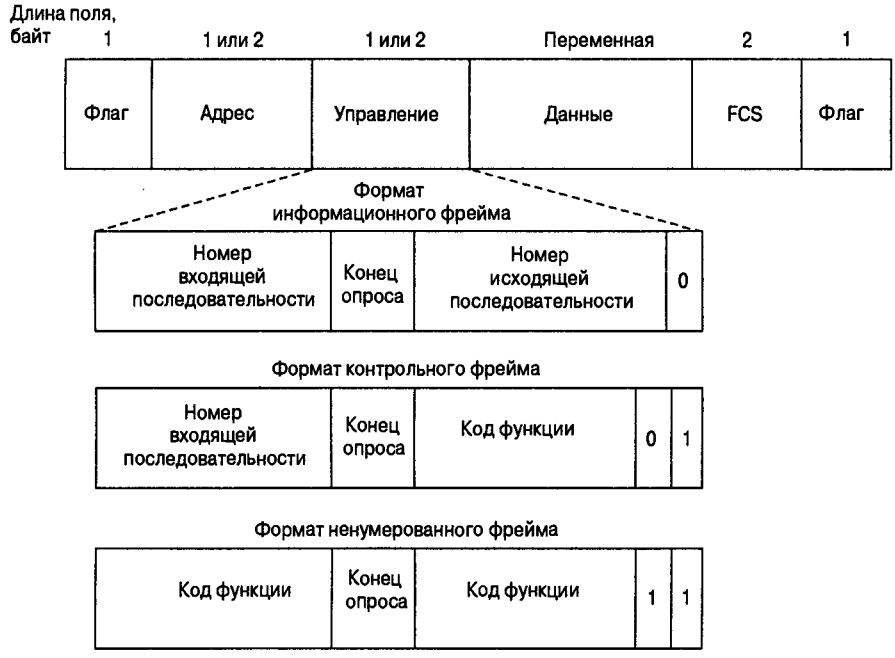


Рис. 16.1. Фрейм SDLC

Поля, показанные на рис. 16.1, описаны ниже.

- **Флаг.** Включает и отключает проверку ошибок.
- **Адрес.** Содержит SDLC-адрес вторичного узла, который показывает, откуда поступил фрейм — с первичного или со вторичного узла. В этом поле может со-

держаться адрес одиноадресатной, многоадресатной или широковещательной рассылки. Первичный узел может являться как источником, так и получателем, что исключает необходимость дополнительно указывать адрес первичного узла.

- **Управление.** Использует следующие три формата, в зависимости от типа SDLC-фрейма.
- **Информационный (I) фрейм.** Содержит информацию высших уровней и некоторую управляющую информацию. Этот фрейм посылает и получает номера последовательностей, а бит конца опроса (Poll Final — P/F) предназначен для управления потоком и обнаружения ошибок. Номер исходящей последовательности представляет собой номер фрейма, который будет отправлен следующим, номер входящей последовательности — номер фрейма, который будет получен следующим. И отправитель, и получатель соблюдают последовательность номеров входящей и исходящей последовательности.

  Первичная станция использует бит P/F для того, чтобы сообщить вторичной, требуется ли немедленный ответ. Вторичная станция использует этот бит, чтобы сообщить первичной, является ли текущий фрейм последним в данном ответе.

  — **Управляющий (S, supervisory) фрейм.** Содержит управляющую информацию. S-фрейм может запрашивать и поддерживать передачу, сообщать о состоянии и подтверждать получение I-фреймов. S-фреймы не содержат информационного поля.

  — **Ненумерованный (U) фрейм.** Предназначен для управления и поэтому не нумеруется. U-фрейм может быть использован для активизации вторичных узлов. В зависимости от функции U-фрейма его управляющее поле занимает 1 или 2 байта. Некоторые U-фреймы содержат и информационное поле.
- **Данные.** Содержит модуль маршрутной информации (Path Information Unit — PIU) или обменные идентификационные данные (eXchange IDentification — XID).
- **Контрольная последовательность фрейма** (Frame Check Sequence — FCS). Предшествует конечному флагу и обычно содержит контрольную сумму (CRC). После поступления фрейма к получателю CRC вычисляется повторно. Если результат отличается от значения, указанного во фрейме, то считается, что произошла ошибка при передаче.

Типичная конфигурация сети протокола SDLC показана на рис. 16.2. Как видно из рисунка, основной контроллер IBM (ранее называвшийся контроллером кластера) на удаленном узле подключается к терминалам ввода-вывода и сети Token Ring. На местном узле узел IBM подключается (методом связанных каналов) к устройству предварительной обработки данных IBM (Front-End Processor — FEP), которое также связано с локальными сетями Token Ring и магистралью SNA. Два узла соединяются по выделенному SDLC-каналу со скоростью 56 Кбит/с.

Производные протоколы

Несмотря на то, что в протоколе HDLC отсутствуют некоторые функции, используемые в SDLC, в целом он считается совместимым расширением протокола SDLC. Протокол LAP является сокращенным вариантом протокола HDLC и был создан для обеспечения дальнейшей совместимости с HDLC, который был изменен

в начале 1980-х годов. Протокол IEEE 802.2 представляет собой модификацию HDLC для локальных сетей. *Протокол ограниченного управления логическим каналом (Qualified Logical Link Control — QLLC)* представляет собой протокол канального уровня, разработанный корпорацией IBM и позволяющий передавать данные SNA по сетям протокола X.25.

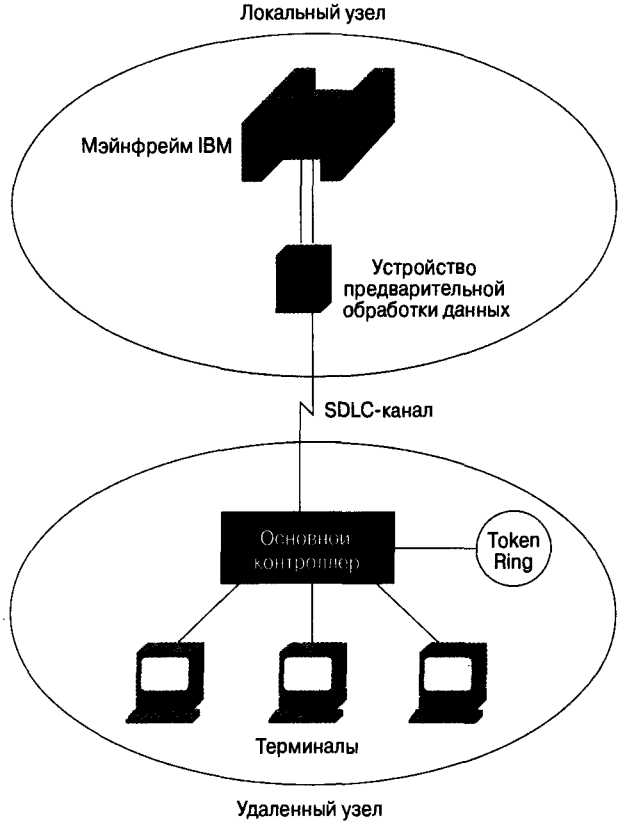


Рис. 16.2. Локальный и удаленный узлы соединяются по последовательному SDLC-каналу

Протокол HDLC

Высокоуровневый протокол управления каналом (High-Level Data Link Control — HDLC) имеет такой же формат фрейма, что и SDLC, а поля HDLC выполняют те же функции. Протокол HDLC обеспечивает работу в синхронном дуплексном режиме. Однако имеются некоторые особенности, отличающие протокол HDLC от SDLC. Прежде всего, в HDLC есть возможность проверки 32-разрядной контрольной суммы. Кроме того, протокол HDLC, в отличие от SDLC, не поддерживает замкнутую и концентраторную конфигурации.

Главное различие между HDLC и SDLC состоит в том, что SDLC поддерживает только один режим передачи, а HDLC — три режима.

- **Режим нормального отклика** (Normal Response Mode — NRM). Этот режим передачи используется также протоколом SDLC. В нем вторичные станции не могут обмениваться данными с первичной станцией без ее разрешения.
- **Режим асинхронного отклика** (Asynchronous Response Mode — ARM). В этом режиме передачи вторичные станции могут устанавливать соединение с первичной станцией без ее разрешения.
- **Асинхронный сбалансированный режим** (Asynchronous Balanced Mode — ABM). В режиме ABM появляется комбинированный узел, который может действовать и как первичный, и как вторичный, в зависимости от ситуации. Все коммуникации в режиме ABM происходят между несколькими комбинированными узлами. Любая комбинированная станция в среде ABM может инициировать передачу данных без разрешения другой станции.

Протокол LAPB

Протокол процедуры сбалансированного доступа к каналу *LAPB* (Link-Access Procedure, Balanced — LAPB) известен благодаря тому, что он входит в стек протоколов X.25. LAPB имеет такие же, как и в протоколах SDLC и HDLC, формат фрейма, типы фреймов и функции полей. Но, в отличие от них, применение LAPB ограничено режимом передачи ABM и только комбинированными станциями. Каналы LAPB могут устанавливаться как устройствами DTE, так и DCE-устройствами Вызывающая станция считается первичной, а отвечающая — вторичной. Кроме того, в протоколе LAPB бит P/F используется несколько иначе, чем в других протоколах. Более подробно протокол LAPB описан в главе 17 "Протокол X.25".

Протокол IEEE 802.2

Протокол *IEEE 802.2* часто называется протоколом управления логическим каналом (Logical Link Control — LLC). Он чрезвычайно распространен в локальных сетях, где взаимодействует с такими протоколами, как IEEE 802.3, IEEE 802.4 и IEEE 802.5. Протокол IEEE 802.2 предусматривает использование описанных ниже трех типов служб.

Служба 1-го типа не требует подтверждения соединения. Иными словами, протокол LLC 1-го типа не подтверждает передачу данных. Многие протоколы высшего уровня, такие как TCP/IP, обеспечивают надежную передачу данных, что компенсирует ненадежность протоколов нижнего уровня, поэтому службы 1-го типа получили широкое распространение.

Служба 2-го типа ориентирована на соединение. Служба LLC 2-го типа (часто называемая LLC2) устанавливает логические соединения между отправителем и получателем, являясь, таким образом, ориентированной на соединение. LLC2 подтверждает прием данных и используется в коммуникационных системах IBM.

Служба 3-го типа обеспечивает гарантированное соединение без подтверждения. LLC 3-го типа подтверждает передачу данных, но не устанавливает логическое соединение. LLC 3-го типа является компромиссом между первыми двумя службами LLC и применяется в промышленных автоматизированных системах, где важно обнаружение ошибок, но пространство контекстного хранения (для виртуальных каналов) крайне ограничено.

Конечные станции могут поддерживать несколько типов служб LLC. Устройство класса I поддерживает только службу 1-го типа, устройства класса II — службы 1-го и 2-го типов, устройства класса III — службы 1-го и 3-го типов, а устройства класса IV поддерживают все три типа служб.

Процессы более высоких уровней применяют службы IEEE 802.2 путем использования точек доступа к службам (Service Access Points — SAP). Заголовок IEEE 802.2 начинается с поля точки доступа к службе получателя (Destination Service Access Point — DSAP), которое идентифицирует процессы приема более высоких уровней. Иными словами, после получения информации реализация IEEE 802.2 на узле завершает обработку, а процесс высшего уровня, определенный в поле DSAP, получает оставшиеся данные. После адреса DSAP следует адрес точки доступа к службе источника (Source Service Access Point — SSAP), который идентифицирует процесс отправки на более высоком уровне.

Протокол ограниченного управления логическим каналом (QLLC)

Протокол ограниченного управления логическим каналом (Qualified Logical Link Control — QLLC) обеспечивает возможность управления каналом данных, необходимую для передачи данных SNA по сетям X.25. Протоколы QLLC и X.25 заменяют SDLC в стеке протоколов SNA. Протокол QLLC использует пакетный уровень (3-й уровень) стека протоколов X.25. Для того чтобы указать, что пакет 3-го уровня X.25 должен обрабатываться протоколом QLLC, в общем идентификаторе форматов (General Format Identifier — GFI) в заголовке пакета 3-го уровня протокола X.25 устанавливается специальный бит, называемый уточнителем (qualifier). Данные SNA передаются как данные пользователя в пакетах 3-го уровня протокола X.25. Более подробно стек протоколов X.25 описан в главе 17 "Протокол X.25".

Резюме

Протокол SDLC был разработан компанией IBM в середине 70-х годов XX века для использования в средах SNA. SDLC был первым протоколом канального уровня, основанным на синхронном, бит-ориентированном режиме работы, и остается главным протоколом канального уровня SNA для распределенных сетей.

Протокол SDLC поддерживает различные типы каналов и топологий. Он может использоваться для соединений типа "точка-точка" и многоточечных соединений, ограниченной и неограниченной среды передачи, полудуплексного и дуплексного режимов, в сетях с коммутацией каналов и коммутацией пакетов.

В протоколе SDLC определены два типа сетевых узлов: первичные и вторичные. Первичные узлы контролируют работу других станций, называемых вторичными.

Первичные и вторичные станции SDLC могут образовывать четыре базовые конфигурации: "точка-точка", многоточечная, замкнутая и концентраторная.

У протокола SDLC есть следующие производные от него протоколы.

- **HDLC.** Поддерживает три режима передачи, в то время как SDLC поддерживает лишь один.
- **LAPB.** Использование этого протокола ограничено режимом передачи ABM и комбинированными станциями.

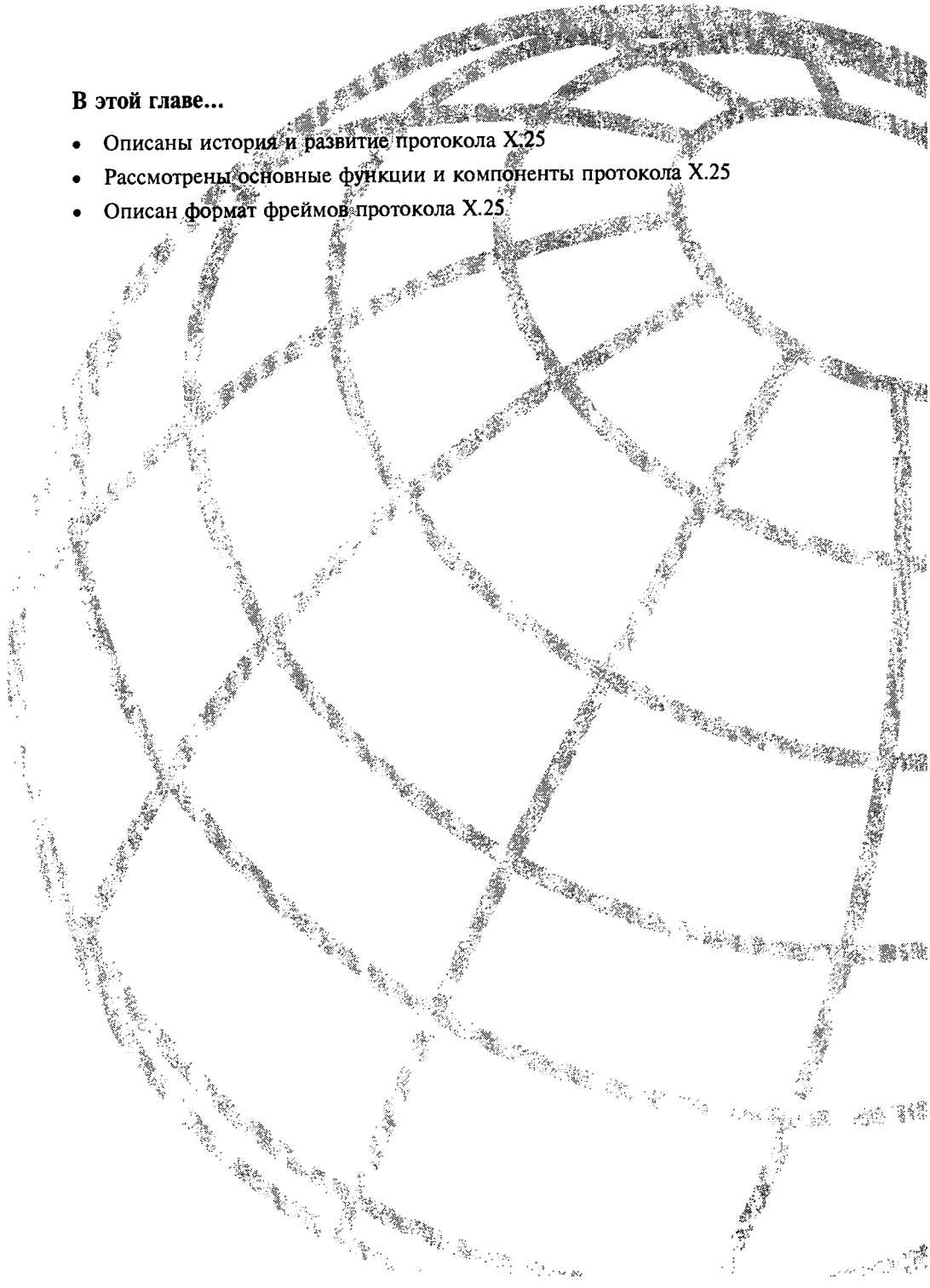
- **IEEE 802.2.** Этот протокол часто называют протоколом LLC. Имеет три типа служб.
- **QLLC.** Обеспечивает контроль канала данных, что требуется для передачи данных SNA по сетям X.25.

Контрольные вопросы

1. Назовите два типа соединений, поддерживаемых протоколом SDLC.
2. Назовите четыре основные конфигурации соединений протокола SDLC.
3. Из каких полей состоит фрейм протокола SDLC?
4. Назовите протоколы, производные от SDLC, и укажите их основные отличия от протокола SDLC.

В этой главе...

- Описаны история и развитие протокола X.25
- Рассмотрены основные функции и компоненты протокола X.25
- Описан формат фреймов протокола X.25



Глава 17

Протокол X.25

Введение

X.25 является стандартом Сектора телекоммуникационных стандартов при Международном союзе электросвязи (International Telecommunication Union — Telecommunication Standardization Sector — ITU-T) для распределенных сетей, который определяет установку и поддержание соединений между устройствами пользователя и сетевыми устройствами. X.25 предназначен для обеспечения эффективной работы независимо от типа систем, подключенных к сети. Обычно он применяется в сетях с коммутацией пакетов (Packet-Switched Networks — PSN), использующих общедоступные линии связи (например телефонных линий). Абонентская плата взимается в зависимости от интенсивности использования сети. Толчок к развитию стандарта X.25 был дан телекоммуникационными компаниями в 70-х годах XX века. В то время возникла потребность в протоколах для распределенных сетей, способных обеспечить связь по общедоступным сетям передачи данных (Public Data Networks — PDN). В настоящее время протокол X.25 является международным стандартом, утвержденным ITU-T.

Устройства протокола X.25 и его функционирование

Сетевые устройства протокола X.25 делятся на три большие категории: терминальное оборудование, оборудование передачи данных и пункты коммутации пакетов. Под терминальным оборудованием (Data Terminal Equipment — DTE) понимаются конечные системы, которые обмениваются данными по сети X.25. Обычно это терминалы, персональные компьютеры или сетевые узлы, размещенные у абонентов. Под оборудованием передачи данных (Data Circuit-terminating Equipment — DCE) понимаются коммуникационные устройства, такие как модемы и пакетные коммутаторы, которые служат интерфейсом между устройствами DTE и пунктами коммутации пакетов и обычно принадлежат телекоммуникационной компании. Пунктами коммутации пакетов (Packed-Switching Exchange — PSE) обычно являются коммутаторы, образующие значительную часть внешней сети. Пункты PSE передают данные от одного устройства DTE к другому через PSN-сети протокола X.25. Взаимосвязи между этими тремя типами сетевых устройств X.25 показаны на рис. 17.1.

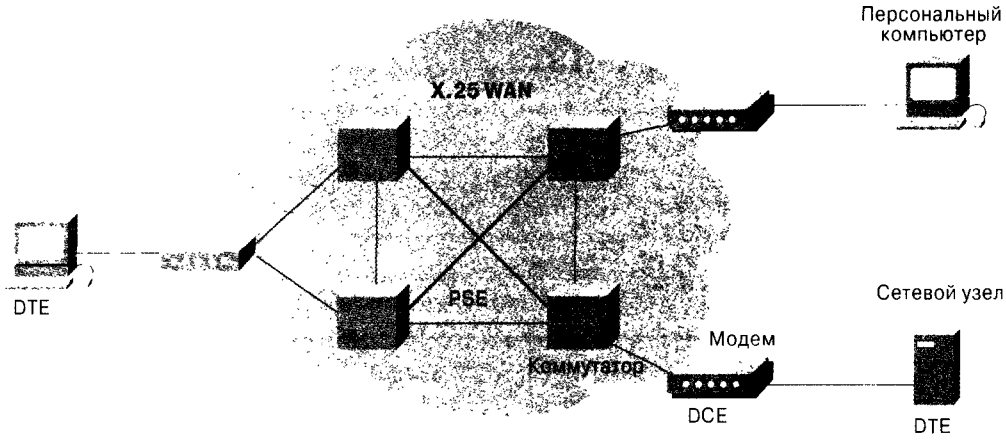


Рис. 17.1. Сеть X.25 образована устройствами DTE, DCE и PSE

Сборщик/разборщик пакетов

Сборщик/разборщик пакетов (Packet Assembler/Disassembler — PAD) представляет собой устройство, часто встречающееся в сетях X.25. Устройства PAD применяются в тех случаях, когда устройство DTE, такое как алфавитно-цифровой терминал, слишком примитивно для того, чтобы обеспечить выполнение всех функций протокола X.25. Устройства PAD размещаются между DTE и DCE и выполняют следующие три основные функции: буферизацию (сохранение данных до тех пор, пока устройство не будет готово их обработать), сборку и разборку пакетов. В буфере PAD сохраняются данные, отправленные на устройство DTE или с него. Устройство PAD также собирает исходящие данные в пакеты и передает их на устройство DCE (а также снабжает пакет заголовком X.25). Наконец, PAD разбирает входящие пакеты перед тем, как передать данные устройству DTE (и удаляет заголовок X.25). Основные операции, выполняемые устройством PAD при приеме пакетов из распределенной сети X.25, показаны на рис. 17.2.

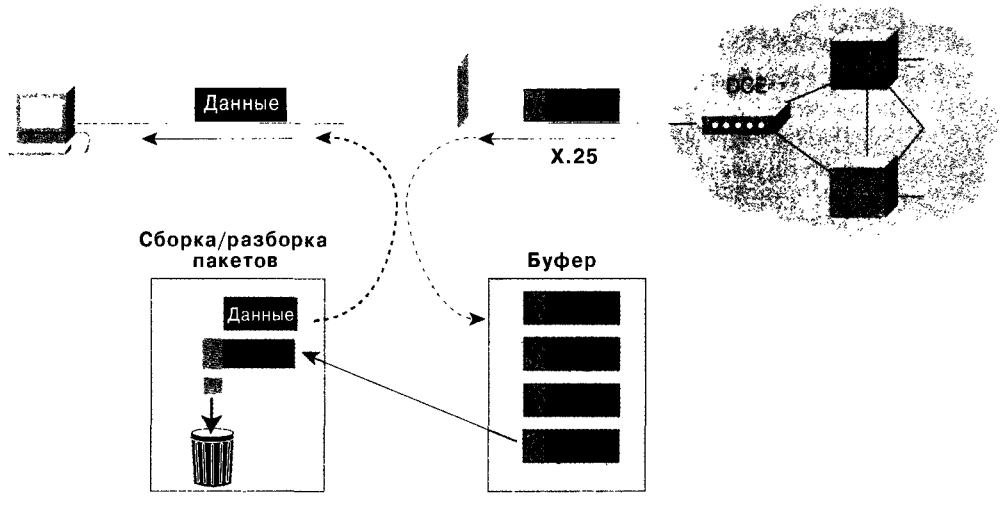


Рис. 17.2. Буферизация, сборка и разборка пакетов данных с помощью устройства PAD

Создание сеанса X.25

Сеансы X.25 устанавливаются в том случае, когда одно устройство DTE обращается к другому с запросом на создание сеанса связи. Устройство DTE, получившее этот запрос, может либо дать согласие на соединение, либо отказаться от него. В случае согласия обе системы начинают передачу информации в дуплексном режиме. Разорвать соединение может любое из устройств DTE. После прекращения сеанса дальнейший обмен данными потребует создания нового сеанса.

Виртуальные каналы X.25

Виртуальный канал (virtual circuit — VC) представляет собой логическое соединение, созданное для обеспечения надежного обмена данными между двумя сетевыми устройствами. Виртуальный канал представляет собой двусторонний логический маршрут от одного DTE-устройства к другому по сети X.25. Физически соединение может проходить через любое количество промежуточных узлов, таких как устройства DTE и PSE. Несколько виртуальных каналов (логических соединений) могут быть мультиплексированы в один физический канал (физическое соединение). При достижении удаленной станции виртуальные каналы демультиплексируются и данные отправляются соответствующим адресатам. На рис. 17.3 показаны четыре отдельных виртуальных канала, мультиплексированных в один физический канал.

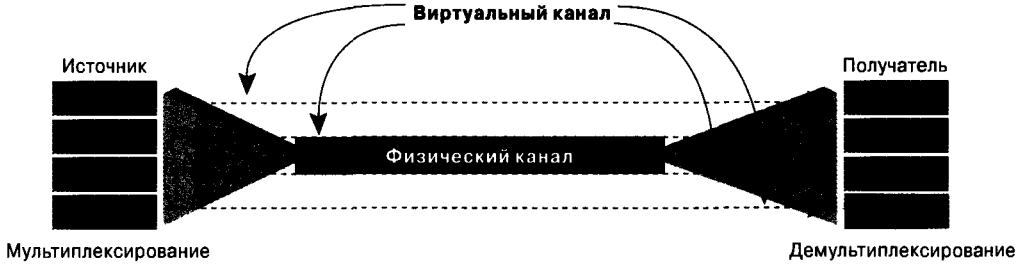


Рис. 17.3. Несколько виртуальных каналов могут быть мультиплексированы в один физический канал

Существует два типа виртуальных каналов X.25: коммутируемые и постоянные. *Коммутируемые виртуальные* каналы *(Switched Virtual Circuits — SVC)* представляют собой временные соединения для одноразовой передачи данных. При их использовании требуется, чтобы два устройства DTE устанавливали, поддерживали и прекращали сеанс каждый раз, когда им нужно обменяться данными. *Постоянные виртуальные* каналы *(Permanent Virtual Circuits — PVS)* являются постоянными соединениями, используемыми для частой или постоянной передачи данных. PVS-каналы не требуют установки и завершения сеанса. Поскольку сеанс всегда активен, устройства DTE могут начинать передачу данных в любой момент, когда в этом есть необходимость.

Основная работа виртуального канала X.25 начинается тогда, когда DTE-источник задает используемый виртуальный канал (в заголовках пакетов) и посылает пакеты на локальное устройство DCE. Локальное устройство DCE проверяет заголовки пакетов, определяет, какой виртуальный канал следует использовать, и посылает пакеты ближайшему устройству PSE на маршруте виртуального канала. Устройства PSE (коммутаторы) передают данные по маршруту следующему промежуточному узлу, который может быть другим коммутатором или удаленным устройством DCE.

Когда поток данных достигает удаленного устройства DCE, заголовки пакетов просматриваются и определяется адрес получателя. Затем пакеты отправляются DTE-получателю. Если обмен данными происходит по SVC-каналу и ни одно из устройств не имеет дополнительных данных для передачи, то виртуальный канал отключается.

Набор протоколов X.25

Набор протоколов X.25 соответствует трем нижним уровням эталонной модели OSI. В реализации X.25 обычно входят протокол LAPB PLP и последовательные интерфейсы физического уровня, такие как EIA/TIA-232, EIA/TIA-449, EIA-530 и G.703. Соответствие основных протоколов X.25 уровням эталонной модели OSI показано на рис. 17.4.

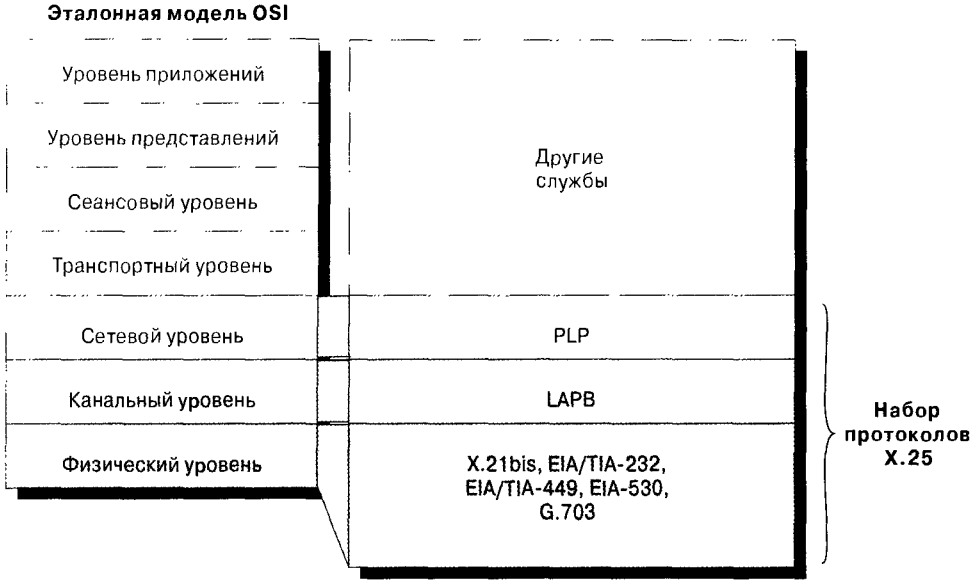


Рис. 17.4. Соответствие основных протоколов X.25 трем нижним уровням эталонной модели OSI

Протокол PLP

Протокол пакетного уровня (Packet-Layer Protocol — PLP) является протоколом сетевого уровня стека X.25. PLP управляет пакетным обменом между устройствами DTE, осуществляемым по виртуальным каналам. Кроме того, PLP может работать с протоколом LLC2 в локальных сетях и с интерфейсами ISDN по процедуре LAPD.

Протокол PLP может работать в одном из пяти режимов: настройки вызова, передачи данных, ожидания, отмены вызова и перезапуска.

Режим настройки вызова используется для открытия SVC-канала между устройствами DTE. Для открытия виртуального канала протокол PLP применяет схему адресации X.121. Настройка вызова выполняется для каждого виртуального канала в отдельности. Иными словами, один виртуальный канал может находиться в состоянии настройки вызова, а другой — в режиме передачи данных. Этот режим используется только для каналов SVC (но не для PVC-каналов).

В режиме передачи происходит передача данных по виртуальному каналу между двумя устройствами DTE. В этом режиме протокол PLP управляет сегментацией и повторной сборкой пакетов, заполнением битов, обработкой ошибок и управлением потоком данных. Передача данных выполняется для каждого виртуального канала в отдельности и применяется как для PVC-каналов, так и для каналов SVC.

Режим ожидания используется в том случае, когда виртуальный канал открыт, но данные не передаются. Он действует для каждого виртуального канала в отдельности и применяется только для каналов SVC.

Режим отмены вызова используется для завершения сеанса между устройствами DTE и разъединения каналов SVC. Этот режим действует для каждого виртуального канала в отдельности и применяется только для SVC-каналов.

Режим перезапуска используется для синхронизации передачи данных между устройством DTE и локально подключенным устройством DCE. Этот режим, в отличие от предыдущих, влияет на все виртуальные каналы, открытые DTE-устройством.

Пакет PLP содержит описанные ниже четыре типа полей.

- **Общий идентификатор формата (General Format Identifier — GFI)).** Это поле идентифицирует параметры пакета, такие как вид хранимой информации (информация пользователя или управляюшая информация), а также указывает используемый тип создания фреймов и сообщает, необходимо ли подтверждение доставки.
- **Идентификатор логического канала (Logical Channel Identifier — LCI).** Идентифицирует виртуальный канал в пределах локального интерфейса DTE/DCE.
- **Идентификатор типа пакета (Packet Type Identifier — PTI).** Идентифицирует пакет как один из 17 типов пакетов протокола PLP.
- **Данные пользователя.** Инкапсулированная информация протоколов верхних уровней. Это поле присутствует только в пакетах данных. В противном случае добавляются дополнительные поля, содержащие управляющую информацию.

Протокол LAPB

Процедура сбалансированного доступа к каналу LAPB (Link Access Procedure, Balanced — LAPB) представляет собой протокол канального уровня, управляющий созданием фреймов и обменом данными между устройствами DTE и DCE. Процедура LAPB представляет собой бит-ориентированный протокол, обеспечивающий упорядочение фреймов и отсутствие в них ошибок.

Используются три типа фреймов LAPB: информационный, супервизорный и ненумерованный. Информационный фрейм (I-фрейм) содержит информацию верхних уровней и некоторую управляющую информацию. Назначение I-фрейма — построение последовательности, управление потоком, обнаружение ошибок и их исправление. I-фреймы содержат номера последовательностей приема и передачи. Супервизорные фреймы (S-фреймы) содержат управляющую информацию. Назначением S-фреймов является запрос на передачу и ее прекращение, сообщение о состоянии и подтверждение получения I-фреймов. S-фреймы содержат только номера последовательностей приема. В ненумерованных фреймах (U-фреймы) передается управляющая информация. В функции U-фреймов входят открытие и закрытие канала, а также передача сообщений об ошибках. U-фреймы не содержат номеров последовательностей.

Протокол X.21bis

Протокол X.21bis представляет собой протокол физического уровня, используемый в X.25 для определения электрических и механических процедур, используемых физической средой передачи. X.21bis управляет активизацией и деактивизацией физической среды передачи, соединяющей устройства DTE и DCE. Он поддерживает соединения типа "точка-точка" со скоростью до 19,2 Кбит/с и синхронную дуплексную передачу по четырехпроводному каналу. Формат пакета протокола PLP и его взаимосвязь с фреймами LAPB и X.21bis показаны на рис. 17.5.

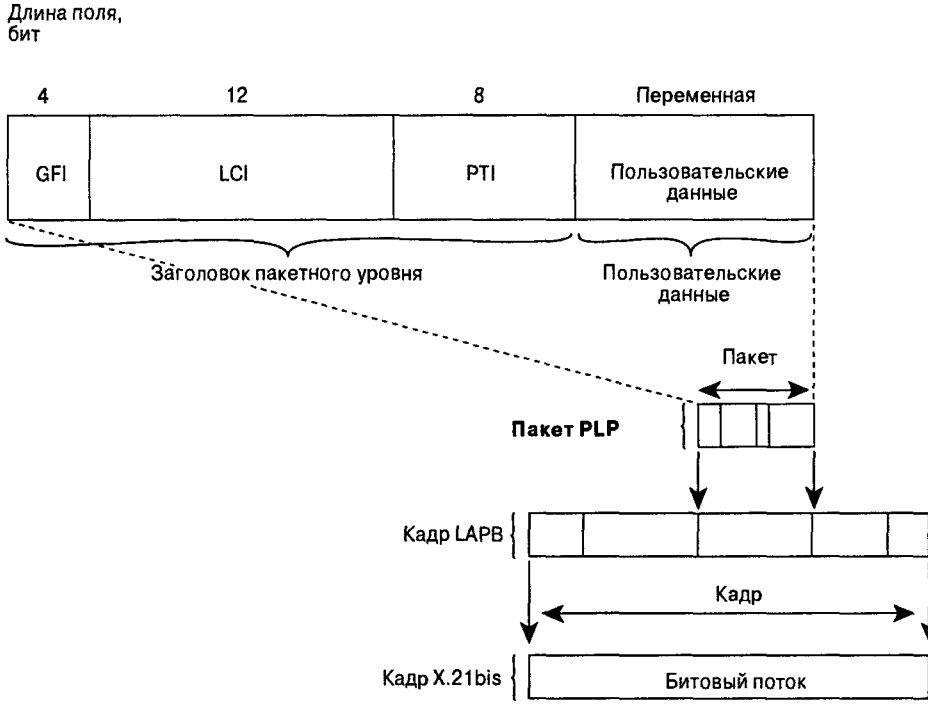


Рис. 17.5. Пакет PLP инкапсулируется во фреймы LABP и X.21bis

Формат фрейма протокола LAPB

Фреймы протокола LAPB состоят из заголовка, инкапсулированных данных и трейлера. На рис. 17.6 показан формат фрейма LAPB и его связь с пакетом PLP и фреймом X.21bis.

Ниже описаны поля, показанные на рис. 17.6.

- **Флаг.** Определяет начало и конец фрейма LAPB. Для предотвращения попадания флага в тело фрейма используется заполнение пустыми битами.
- **Адрес.** Показывает, что содержится в фрейме: команда или ответ.
- **Управление.** Квалифицирует фреймы команд и ответов и показывает, является ли фрейм информационным, супервизорным или ненумерованным. Кроме того,

это поле содержит номер последовательности фрейма и его функцию (например, готовность получателя или разъединение). Длина управляющих фреймов является переменной и зависит от типа фрейма.

- **Данные.** Данные верхних уровней в виде инкапсулированного пакета PLP.
- **Контрольная последовательность FCS.** Предназначается для выявления ошибок и обеспечения целостности передаваемых данных.

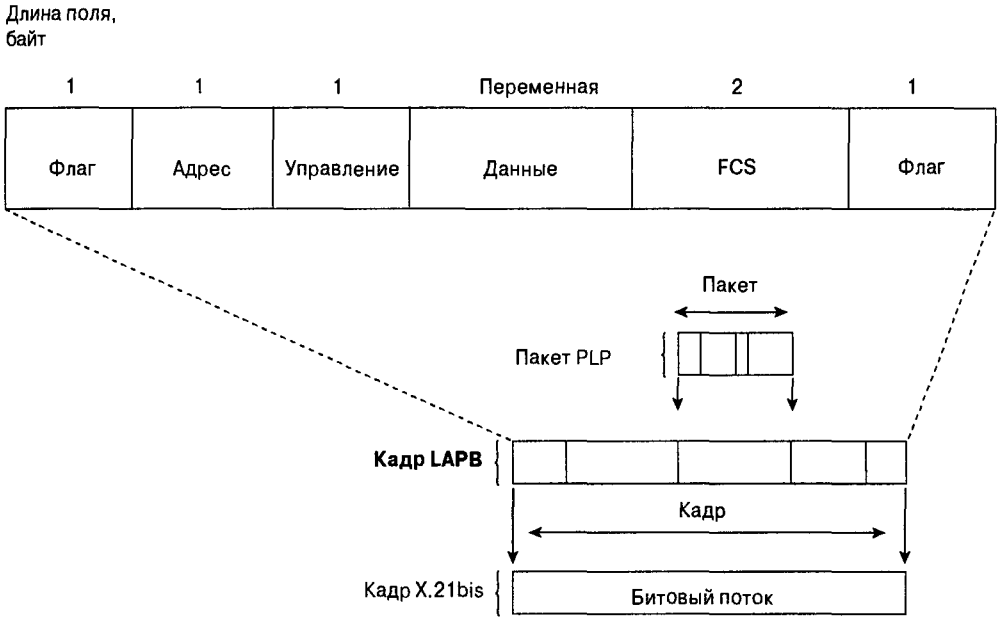


Рис. 17.6. Фрейм LAPB состоит из заголовка, трейлера и инкапсулированных данных

Формат адреса X.121

Адреса X.121 используются протоколом PLP стека X.25 в режиме настройки вызова для установки SVC-канала. Формат адреса X.121 показан на рис. 17.7.

Поле адреса X.121 включает в себя международный код данных IDN (International Data Number — IDN), состоящий из двух полей: идентификационного кода сети передачи данных (Data Network Identification Code — DNIC) и национального терминального кода (National Terminal Number — NTN).

Поле DNIC является дополнительным полем, которое строго идентифицирует PSN-сеть, в которой расположено устройство DTE. При вызовах в пределах одной PSN-сети это поле иногда опускается. Поле DNIC имеет два подполя: подполя страны и PSN-сети. Подполе страны определяет страну, в которой находится PSN-получатель, а подполе PSN уникальным образом определяет сеть PSN, которой принадлежит DTE-получатель.

Поле NTN уникальным образом идентифицирует в PSN-сети устройство DTE, которому предназначен пакет. Это поле имеет переменную длину.

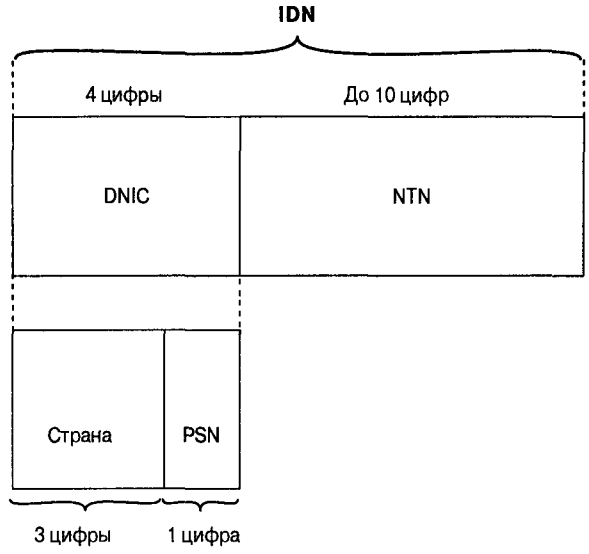


Рис. 17.7. Адрес X.121 с полем IDN

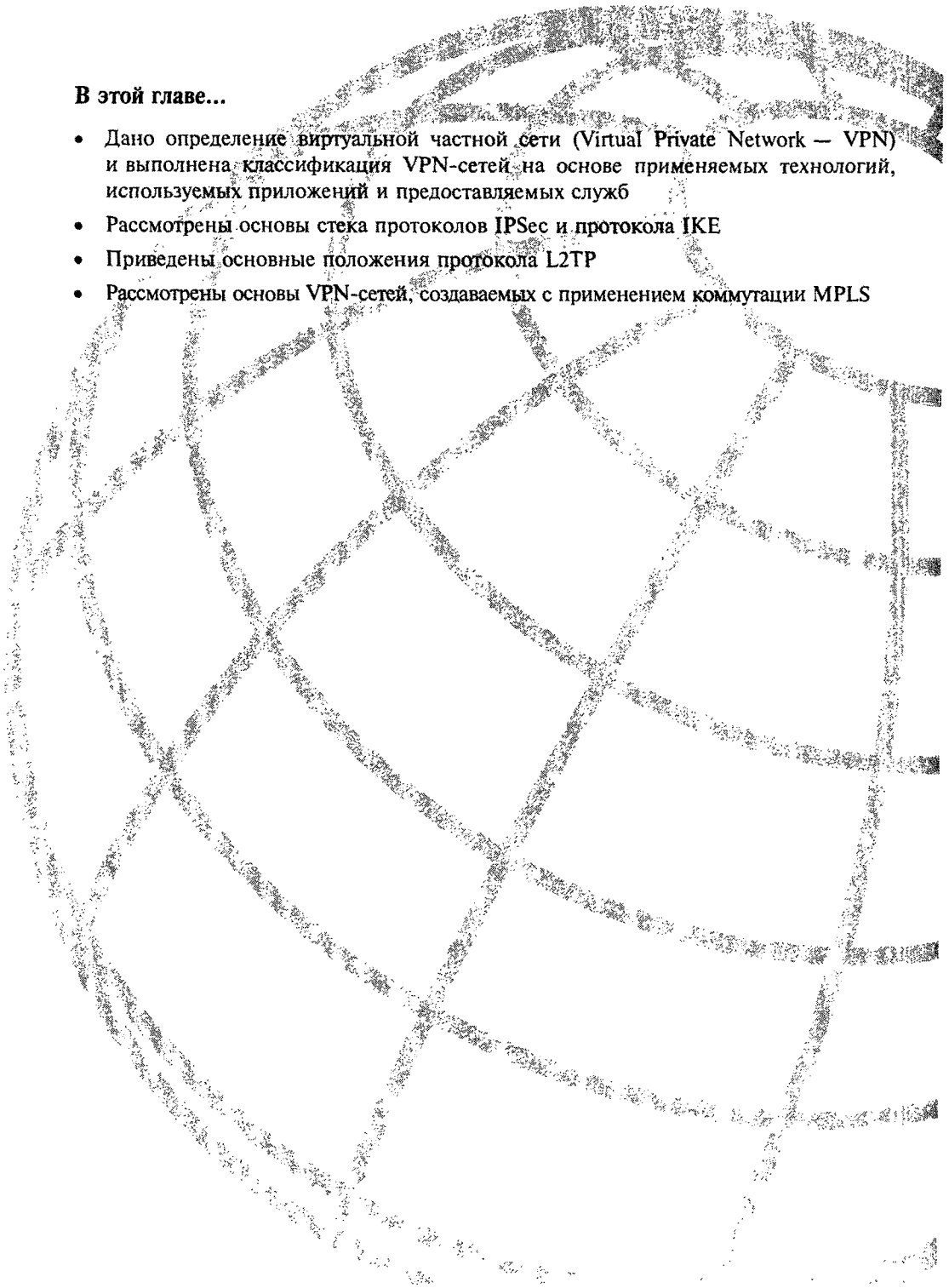
Резюме

Протокол X.25 является протоколом стандарта ITU-T, который определяет порядок открытия и поддержания соединений между устройствами пользователя и сетевыми устройствами и обеспечивает их эффективное функционирование независимо от типов систем, подключенных к сети. В число устройств протокола X.25 входят устройства DTE, DCE и каналы PVC. Соединения X.25 используют каналы SVC и PVC в пределах одной физической сети. В стеке X.25 используются следующие три протокола, соответствующие трем нижним уровням эталонной модели OSI:

- Протокол PLP, соответствующий сетевому уровню;
- Протокол LAPB, соответствующий канальному уровню;
- Протоколы X.21bis, EIA/TIA-232, EIA/TIA-449, EIA-530 и G.703, соответствующие физическому уровню.

Контрольные вопросы

1. С каким видом сетей обычно работает протокол X.25?
2. Назовите три основные категории, к которым относятся устройства протокола X.25.
3. Назовите три основные функции устройства PAD.



В этой главе...

- Дано определение виртуальной частной сети (Virtual Private Network — VPN) и выполнена классификация VPN-сетей на основе применяемых технологий, используемых приложений и предоставляемых служб
- Рассмотрены основы стека протоколов IPSec и протокола IKE
- Приведены основные положения протокола L2TP
- Рассмотрены основы VPN-сетей, создаваемых с применением коммутации MPLS

Глава 18

Виртуальные частные сети

В последние годы, когда все большее число компаний для обеспечения связи стали использовать глобальную сеть Internet, рынок виртуальных частных сетей (Virtual Private Network — VPN) значительно вырос и расширился. По мере того, как появляются новые стандарты, службы, программные и аппаратные продукты, технологии VPN-сетей также претерпевают значительные изменения. Это, однако, привело к тому, что компании, которые желают реализовать у себя VPN-сети, испытывают трудности в понимании того, что представляют собой эти сети, какие службы предоставляют различные типы VPN и какой тип VPN-сети является для них оптимальным.

Попытка ясно определить и классифицировать VPN-сети представляет собой непростую задачу, которая, видимо, будет решена лишь в будущем. В настоящей главе не ставится цель дать всеобъемлющее определение VPN-сетей, а лишь описываются различные технологии таких сетей.

Определение сетей VPN

Частная виртуальная сеть VPN представляет собой логическую сеть, которая функционирует в уже существующей физической сетевой инфраструктуре. По сравнению с традиционными способами построения частных сетей путем использования выделенных линий для соединения географически удаленных друг от друга офисов компаний, современные частные VPN-сети являются виртуальными в том смысле, что сетевые устройства и соединения (кабели и т.д., в частности, оборудование Internet) применяемые для их построения, используются также и другими компаниями. Как и ранее использовавшиеся частные сети, сети VPN обеспечивают конфиденциальность передаваемых данных. Каналы при этом выделяются отдельным пользователям, которые могут иметь свою собственную систему IP-адресации, свои схемы маршрутизации и проводят собственную политику безопасности.

Определение "частная" в терминологии VPN-сетей может также рассматриваться в контексте обеспечения безопасности. Вопрос о том, какие возможности обеспечения безопасности могут предоставить службы VPN, все чаще ставится компаниями при реализации ими своих частных виртуальных сетей.

Целесообразно сначала рассмотреть пример VPN-сети, использующей выделенные линии, такой, например, как сеть Frame Relay. Такие сети иногда называют *"вызывающими доверие" (trusted),* поскольку в этом случае пользователь доверяет решение

вопросов надежности и безопасности устройствам провайдера. В действительности такой тип VPN-сети реальной безопасности не обеспечивает.

По мере того как все большее число компаний использует Internet в качестве магистрали своих VPN-сетей, предположение о безопасности таких сетей перестает быть верным. Более того, именно данные, передаваемые по сети Internet более подвержены атакам, таким как нарушение конфиденциальности, целостности или прослушивание идентификационных данных. Поэтому для таких VPN-сетей становятся критически важными меры по обеспечению безопасности и предотвращению возможных атак, включая защиту конфиденциальности, целостности данных и аутентификацию. В качестве таких мер при передаче данных по сети Internet используются туннельные технологии и алгоритмы шифрования. Такие VPN-сети называются *безопасными (secure)*.

На основе данного определения все современные технологии VPN-сетей можно разделить на две категории.

- **Надежные VPN-технологии.** Наиболее многообещающими из них являются технологии, основанные на MPLS-коммутации с использованием протокола BGP или протокола L2VPN.
- **Безопасные VPN-технологии**. Наиболее популярными являются технологии IPSec, L2TP или L2TP с использованием протоколов IPSec и PPTP. В последние годы использование технологии IPSec де-факто стало стандартом обеспечения безопасности в VPN-сетях.

VPN-приложения

VPN-технологии применяются в следующих ситуациях.

- **Сети интранет (intranet)**. С помощью VPN-технологий компании могут использовать глобальную сеть Internet в качестве магистрали для связи своих географически удаленных друг от друга узлов через VPN-сети.
- **Сети экстранет (extranet)**. В таких сетях VPN-технологии могут использоваться для быстрого создания соединений по требованию между компанией и ее бизнес-партнерами.
- **Сети удаленного доступа**. Используя VPN-сеть удаленные пользователи могут получить доступ к корпоративной сети, зарегистрировавшись у регионального провайдера службы Internet (Internet service provider — ISP). Это значительно более эффективно в финансовом отношении, чем традиционное поддержание самой компанией большого банка модемов.

Технология IPSec

Международная группа, организованная при проблемной группе Internet (Internet Engineering Task Force — IETF) разработала набор протоколов IPSec (IPSecurity — IPSec) для обеспечения безопасности при передаче данных протокола IP на сетевом уровне. Стек протоколов IPSec описан в нескольких RFC. В нем используются различные технологии шифрования для выполнения ключевых функций обеспечения безопасности против наиболее типичных угроз в сети Internet. Ниже дано краткое описание этих служб.

- Аутентификация гарантирует, что устройство VPN-сети осуществляет связь именно с требуемым узлом.
- Конфиденциальность данных обеспечивается посредством их шифрования.
- Поддержка целостности данных обеспечивает предотвращение изменения данных в процессе передачи.

Ниже приведены некоторые ключевые технологии шифрования, используемые стеком протоколов IPSec для поддержки описанных выше служб безопасности.

- Алгоритмы шифрования содержимого (контента — content) обычно являются симметричными алгоритмами. Наиболее часто используются алгоритмы DES, 3DES и AES.
- Криптографические символы "hard-to-invert" и "strong collision-free" некоторых хэш-алгоритмов используются для генерирования цифровой подписи, аутентификации и обеспечения целостности данных конкретного сообщения. В протоколе IPSec используется хэш-функция с ключом для генерирования кода аутентификации основанного на хэш-функции с ключом сообщения (Keyed Hash-Based Message Authentication Code — HMAC) в целях аутентификации источника данных и проверки их целостности. В качестве хэш-алгоритмов в протоколе IPSec используются алгоритмы MD5 и SHA-1.
- Протокол обмена ключами Диффи-Хеллмана (Diffie-Hellman — DH) позволяет двум VPN-устройствам безопасно сгенерировать общий секретный код по небезопасному каналу без предварительного совместно используемого кода. После завершения взаимной DH-идентификации два одноранговых устройства VPN-сети могут создать безопасный канал, который защищает обмен сообщениями между ними во время обсуждения параметров безопасности протокола IPSec
- Инфраструктура открытого ключа (Public Key Infrastructure — PKI) состоит из протоколов, стандартов и служб, которые поддерживают применение алгоритмов открытого ключа. В отличие от алгоритмов шифрования контента, алгоритмы открытого ключа являются асимметричными. Каждое устройство генерирует два математически связанных ключа. Один из них, общедоступный (открытый) ключ предоставляется всему домену, а соответствующий конфиденциальный ключ остается секретным. Даже при наличии общедоступного ключа вычисление секретного ключа является математически невозможным. Это свойство делает алгоритмы открытого ключа полезными как для шифрования, так и для использовании цифровых подписей. Алгоритм RSA является наиболее известным примером алгоритма общедоступного ключа. При посредстве соответствующей организации, осуществляющей сертифицирование (Certificate Authority — CA), каждое VPN-устройство в системе PKI может логически связать свой общедоступный ключ со своими идентификационными данными, такими как IP-адрес и полностью определенное доменное имя, используя сертификат, полученный от CA. При использовании в VPN-сети с протоколом IPSec система PKI обеспечивает службы безопасности, такие как аутентификация и предотвращение несанкционированного изменения передаваемой информации.

Структура VPN-сети, использующей технологию IPSec, включает в себя следующие компоненты.

- Заголовок аутентификации (Authentication Header — AH) добавляется к IP-пакету для аутентификации источника данных и проверки целостности данных.
- Нагрузка безопасности (Encapsulating Security Payload — ESP) — обеспечивает шифрование, аутентификацию источника и проверку целостности данных.
- Протокол ассоциаций безопасности и управления ключами Internet (Internet Security Association and Key Management Protocol — ISAKMP) и протокол обмена Internet-ключами (Internet Key Exchange — IKE) позволяют VPN-устройствам безопасно обсуждать параметры безопасности (Security Association — SA) и управлять ими в процессе генерации, обмена и управления ключами, используемыми для алгоритмов шифрования в протоколе IPSec.

В последующих разделах отдельно обсуждаются следующие темы:

- Заголовок аутентификации;
- Нагрузка обеспечения безопасности;
- Транспортный режим и туннельный режим протокола IPSe;
- Параметры безопасности;
- Протокол обмена Internet-ключами.

Заголовок аутентификации

Определенный в RFC 2402 заголовок аутентификации (Authentication Header — AH) добавляется протоколом IPSec к IP-дейтаграмме. Он находится между IP-заголовком и заголовком протокола 4-го (транспортного) уровня. Как правило, он представляет собой ключевой код аутентификации HMAC, вычисленный на основе полезной нагрузки протокола IP и IP-заголовка, кроме случая переменных полей, которые изменяются при передаче, таких как поле TTL. Проверка заголовка AH дает получателю возможность выполнить аутентификацию источника данных и их целостность. На рис. 18.1 показан формат заголовка AH.

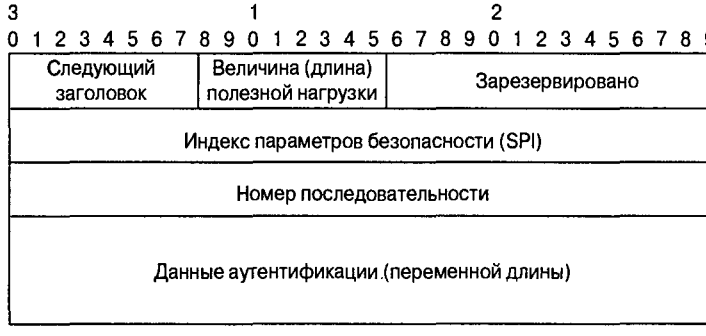


Рис. 18.1. Заголовок аутентификации

Заголовок содержит следующие поля.

- Поле заголовка следующего уровня (1 байт) указывает AH-протокол более высокого уровня, такой как TCP или UDP.
- Величина нагрузки безопасности (1 байт) задает длину AH-заголовка.

- 2 зарезервированных байта для будущего использования (в настоящее время они устанавливаются равными нулю).
- Индекс параметров безопасности (Security Parameters Index — SPI) (4 байта) задает набор параметров безопасности, также называемых нагрузкой безопасности для IPSec-соединения.;
- Номер в последовательности (4 байта) отражает порядок IPSec-пакетов для предотвращения атаки воспроизведения.
- Поле данных аутентификации (переменного размера) содержит результат проверки целостности (Integrity Check Value — ICV) для IP-пакета.

АН-пакеты представляют собой IP-пакеты, соответствующие протоколу типа 51.

Нагрузка безопасности

Понятие нагрузки безопасности (Encapsulating Security Payload — ESP) определено в RFC 2406. В отличие от заголовка АН, инкапсуляция ESP гарантирует конфиденциальность данных путем шифрования IP-пакетов. Необходимо отметить, что ESP-аутентификация не охватывает IP-заголовок.

На рис. 18.2 показан формат инкапсуляции ESP.

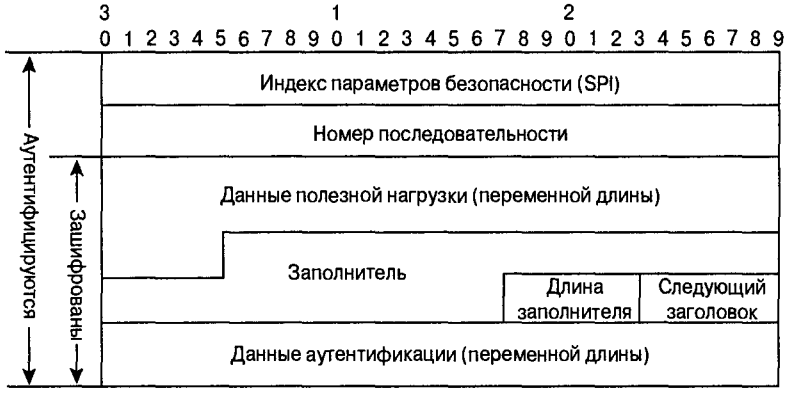


Рис. 18.2. Инкапсуляция нагрузки безопасности

Поля включают в себя следующие компоненты.

- Индекс параметров безопасности (Security Parameters Index — SPI) (4 байта) задает набор параметров, известных также как нагрузка безопасности для IPSec-соединения.
- Номер в последовательности (4 байта) задает порядок следования IPSec-пакетов для предотвращения атаки воспроизведения.

Приведенные ниже поля шифруются:

- Поле данных полезной нагрузки содержит конкретные данные, передаваемые в IP-пакете.
- Заполнитель (от 0 до 255 байтов) используется для того, чтобы весь обычный текст состоял из нескольких блоков равной длины, что требуется некоторыми

алгоритмами шифрования, которые оперируют блоками данных или требуют упорядочения данных;

- Длина заполнителя (1 байт) задает длину заполнителя, описанного в предыдущем пункте.
- Поле следующего заголовка (1 байт) определяет тип протокола данных, переносимых в поле данных полезной нагрузки;
- Поле данных аутентификации (переменной длины) содержит результат проверки целостности данных (Integrity Check Value — ICV). В отличие от случая использования заголовка AH, ESP-проверка целостности данных не включает в себя IP-заголовок.

Транспортный и туннельный режимы IPSec

Как AH, так и ESP имеют два режима инкапсуляции — транспортный и туннельный (рис. 18.3).

В транспортном режиме IP-заголовок первоначального IP-пакета используется в качестве IP-заголовка пакета IPSec, а сам IPSec-заголовок вставляется между IP-заголовком и полезной нагрузкой протокола IP. В туннельном режиме протокол IPSec инкапсулирует весь первоначальный IP-пакет, а к пакету IPSec добавляется новый IP-заголовок.

В туннельном режиме обеспечивается ограниченный уровень конфиденциальности потока данных за счет скрытия информации об IP-адресе первоначального пакета.

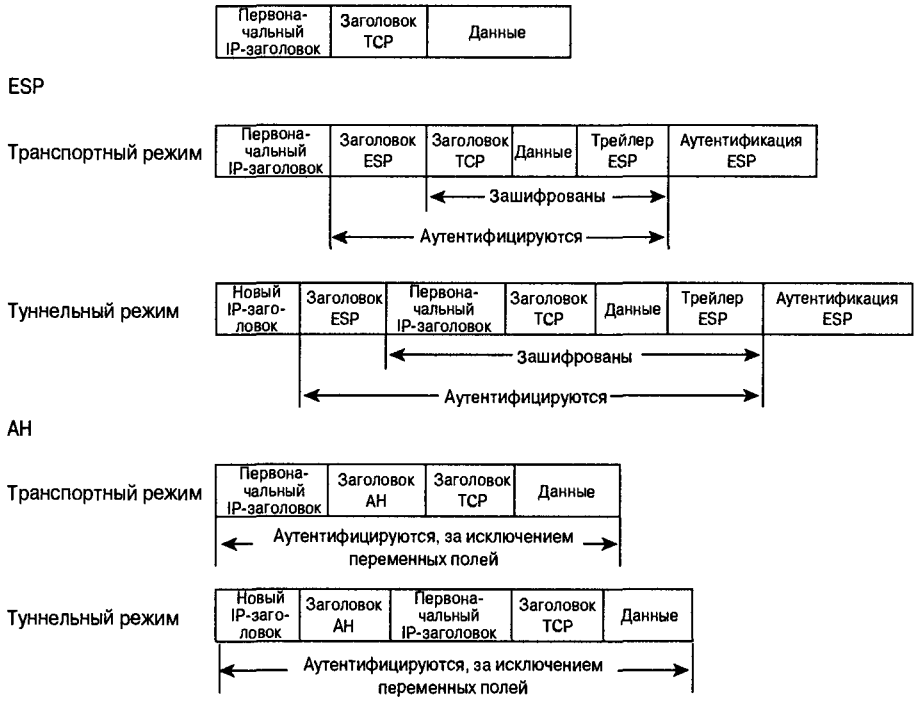


Рис. 18.3. Транспортный и туннельный режимы протокола IPSec

Параметры безопасности (Security Association — SA)

В предыдущем разделе было показано, что устройство IPSec имеет возможность выбора из нескольких алгоритмов шифрования: хэш-алгоритмы, режимы IPSec и т.д. Эти параметры и другая информация, требуемые для установки IPSec-соединения, регистрируются в параметрах SA протокола IPSec. В целом параметры SA используются для поддержки связи между двумя устройствами, при которой к передаваемым потокам данных применяются службы обеспечения безопасности. Для каждого одноранговое соединения протокола IPSec поддерживаются два односторонних набора параметров SA: по одному для исходящих и входных потоков данных.

Набор параметров безопасности протокола IPSec однозначно идентифицируется тремя значениями: использование AH или ESP, SPI и IP-адрес пункта назначения.

Протокол обмена ключами в Internet (Internet Key Exchange — IKE)

Хотя протокол IPSec поддерживает ручное конфигурирование набора параметров безопасности, становится очевидным, что для достижения масштабируемости и гибкости необходим определенный механизм автоматизации. Это механизм должен позволить устройствам VPN-сети обсуждать параметры SA протокола IPSec и управлять ими, а также генерировать и распределять ключи без вмешательства пользователя. Этой цели служит протокол IKE, описанный в RFC 2409.

IKE представляет собой гибридный протокол, объединяющий ISAKMP и Oakley Key Exchange. Протокол ISAKMP, определенный в RFC 2408, представляет собой открытую структуру, задающую процедуру и формат пакета для установки, обсуждения, изменения и удаления наборов параметров безопасности. В сочетании с доменом интерпретации IPSec (IPSec Domain of Inerpretation), определенном в RFC 2407, протокол IKE подробно описывает реализацию управления параметрами безопасности IPSec в рамках ISAKMP.

Работа протокола IKE включает в себя две фазы. В первой фазе обмена сообщениями IKE два устройства пытаются создать аутентифицированный, безопасный канал, который обеспечил бы безопасность последующего обмена сообщениями между этими двумя устройствами. Эта фаза включает в себя три этапа.

Этап 1. Два устройства сети VPN обсуждают алгоритмы шифрования, которые будут использоваться в первой фазе обмена для установки параметров безопасности для первой фазы, известных также как *ISAKMP SA* или *IKE SA*.

Этап 2. Два устройства VPN-сети осуществляют DH-обмен. Этот обмен позволяет им безопасно сгенерировать по небезопасному каналу общий секретный ключ при отсутствии предварительного общего секретного кода. Вместе с другой информацией, касающейся этого обсуждения, общий секретный ключ используется для генерации нескольких ключей, один из которых используется для защиты последующей связи между этими двумя VPN-устройствами.

Этап 3. Каждое VPN-устройство аутентифицирует другое устройство путем отправки своих идентификационных данных, таких как IP-адрес, FQDN и обработанная хэш-функцией с ключом полезная нагрузка для их проверки другой стороной.

Существует три метода IKE-аутентификации.

- Аутентификация с общим ранее согласованным ключом. Этот ключ представляет собой секретный код, заранее установленный на каждом из устройств с помощью внеполосных механизмов. Этот заранее согласованный общий ключ является одним из входных параметров полезной нагрузки, обработанной хэш-функцией с ключом. Поэтому без проверки соответствия этому ключу хэш-тестирование IKE-аутентификации не даст положительного результата.
- Аутентификация с помощью шифрования по общедоступному ключу. Все одноранговые устройства протокола IPSec сначала генерируют псевдослучайное число, называемое нонсом (nonce). После этого нонс шифруется с использованием общедоступного ключа другой стороны. Способность другой стороны расшифровать нонс с использованием своего конфиденциального ключа и восстановить хэш-нагрузку означает положительный результат аутентификации при IKE-обмене. Одноранговым устройствам протокола IPSec может потребоваться внеполосный механизм для предварительного обмена своими общедоступными ключами.
- Аутентификация с помощью цифровой подписи. Хэш-нагрузка, используемая для IKE-аутентификации, подписывается частным ключом устройства протокола IPSec. Во время IKE-аутентификации каждая сторона выполняет хэш-проверку после расшифровки хэш-нагрузки с использованием частного ключа однорангового устройства, который получается из цифрового сертификата этого устройства. Использование цифрового сертификата обеспечивает защиту от несанкционированного изменения информации.

Первая IKE-фаза обмена может быть выполнена в главном или в агрессивном режиме. Главный режим использует минимум шесть пакетов, а агрессивный режим использует минимум три пакета. Главный режим более безопасен чем агрессивный, однако он менее эффективен.

Во второй фазе IKE-обмена, также известной как *быстрый режим*, два VPN-устройства обсуждают и устанавливают параметры безопасности SA протокола IPSec. Этот обмен защищен установкой параметров в первой фазе и все сообщения, которыми обмениваются устройства, подвергаются аутентификации. На этом этапе извлекаются также ключи шифрования данных, используемые протоколом IPSec. При этом может быть выполнен дополнительный DH-обмен для генерирования новых заранее согласованных секретных кодов, которые используются для получения ключей шифрования данных протокола IPSec. Новые ключи, сгенерированные при этом DH-обмене, независимы от прежних ключей, сгенерированных в первой фазе. Это дополнительное средство обеспечения безопасности называется совершенной опережающей секретностью (Perfect Forward Secrecy — PFS).

После обмена в быстром режиме устанавливаются два односторонних набора параметров SA протокола IPSec. Протокол IPSec использует их для защиты потоков данных.

Протокол создания туннелей на 2-м уровне (Layer 2 Tunneling Protocol — L2TP)

Группе IETF были представлены конкурирующие предложения от компаний Microsoft и Cisco Systems, касающиеся спецификации протокола, который обеспечивал бы безопасность передачи IP-дейтаграмм по неконтролируемым и небезопасным (untrusted) сетевым доменам. Предложение Microsoft представляло собой попытку

стандартизировать туннельный протокол типа "точка-точка" (Point-to-Point Tunneling Protocol — PPTP), который был создан этой компанией. Корпорация Cisco также предложила протокол, созданный для выполнения аналогичной функции. IETF соединила лучшие черты этих протоколов и определила открытый стандарт L2TP.

Протокол PPP устанавливает на 2-м уровне канал типа "точка-точка", в котором соединения протокола PPP выполняют инкапсуляцию и транспортировку пакетов различных протоколов. Сервер доступа к сети (Network Access Server — NAS) является терминирующим устройством канала типа "точка-точка" на 2-м уровне, установленного пользователями с применением различных технологий, таких как удаленный доступ через общедоступную сеть POTS, ISDN и ADSL. Сервер NAS является терминирующей точкой как каналов 2-го уровня типа "точка-точка", так и сеансов протокола PPP.

При использовании протокола L2TP терминирующие точки канала 2-го уровня и сеанс протокола PPP могут быть отделены друг от друга различными устройствами, соединенными между собой через IP-сети. Иными словами, пользователи могут осуществлять доступ к локальному серверу NAS, а сеанс PPP может быть расширен посредством соединения протокола L2TP через общую инфраструктуру, такую как сеть Internet или Frame Relay, с домашним шлюзом, который обрабатывает сеанс PPP и управляет им. При этом пользователи получают в свое распоряжение те же самые функции, но оплачивают только услуги местной телефонной сети.

Протокол L2TP имитирует соединение типа "точка-точка" путем инкапсуляции дейтаграмм протокола PPP для их транспортировки по маршрутизируемым сетям или по объединенным сетям. Когда дейтаграммы протокола PPP поступают в пункт назначения, инкапсуляция удаляется и дейтаграммы восстанавливаются в своем первоначальном формате. Таким образом, сеанс связи типа "точка-точка" может поддерживаться через не связанные непосредственно сети. Такой метод называется туннелированием.

Ниже описаны ключевые компоненты соединения протокола L2TP.

- Сервер доступа к сети (Network Access Server — NAS). Это устройство предоставляет удаленный доступ по требованию пользователям локальных сетей. Оно является терминирующей точкой для каналов типа "точка-точка", установленных конечными пользователями, обычно с использованием линий PSTN или ISDN.
- Концентратор доступа протокола L2TP (L2TP Access Concentrator — LAC). Этот узел обычно выполняет функции инициатора установки туннеля протокола L2TP к сетевому серверу протокола L2TP. Концентратор LAC пересылает пакеты между конечными пользователями и серверами LNS.
- Сетевой сервер протокола L2TP (L2TP Network Server — LNS). Этот узел функционирует в качестве терминирующей точки сеансов протокола PPP, проходящих по туннелю L2TP, инициированному концентратором LAC.

Концентратор LAC и сервер LNS определяют только логические функции соединения протокола L2TP. Их физическое расположение зависит от конкретных топологий реализации и предъявляемых к ним требований, как описано в последующих разделах.

Топологии реализации

Протокол L2TP может быть реализован в двух различных топологиях:

- принудительное туннелирование или прозрачное для клиента туннелирование;
- добровольное туннелирование или туннелирование, известное клиенту.

Различие между этими двумя топологиями состоит в том, известно ли клиентскому устройству, использующему протокол L2TP для доступа к удаленной сети, что ее соединение туннелируется. Физическое расположение концентраторов LAC в этих топологиях различно.

Принудительное туннелирование

Принудительное туннелирование характеризуется распределением концентраторов LAC в непосредственной близости к удаленным пользователям. Такое географическое разделение предназначено для уменьшения расходов на междугородную и международную телефонную связь, которые в противном случае были бы возложены на удаленных пользователей, осуществляющих удаленный доступ к центрально расположенному местному концентратору LAC.

Как показано на рис. 18.4, удаленным пользователям не требуется непосредственно поддерживать протокол L2TP. Они лишь устанавливают сеанс связи типа "точка-точка" с сервером NAS, который также является концентратором LAC, использующим протокол PPP. При этом пользователь инкапсулирует IP-дейтграммы во фреймы протокола PPP. Концентратор LAC осуществляет обмен сообщениями протокола PPP с удаленным пользователем и устанавливает туннель протокола L2TP с сервером LNS, через который проходят сообщения протокола PPP удаленного пользователя. Концентратор LAC может также выполнять аутентификацию конечных пользователей и использовать информацию конечных пользователей, такую как имя домена, для направления конечных пользователей на соответствующие серверы LNS.

Рис. 18.4. Принудительные туннели протокола L2TP

Сервер LNS представляет собой шлюз пользователя к его домашней сети. Он является выходной точкой туннеля; в его функции входит удаление инкапсуляции протокола L2TP и предоставление удаленному пользователю доступа к сети.

Как видно из этого сценария, у конечного пользователя нет выбора, а туннель протокола L2TP, установленный сервером NAS, поддерживающим L2TP, является прозрачным для конечных пользователей.

Туннелирование по желанию пользователя

Как показано на рис. 18.5, функции концентратора LAC выполняются на клиентском компьютере, а соединение протокола L2TP инициируется конечным пользователем. Клиент сначала получает IP-соединение с сервером NAS от локального Internet-провайдера или подсоединяется к сегменту локальной сети LAN. После этого он инициирует соединение с сервером LNS, который является терминирующей точкой туннеля протокола L2TP и расширенного сеанса протокола PPP.

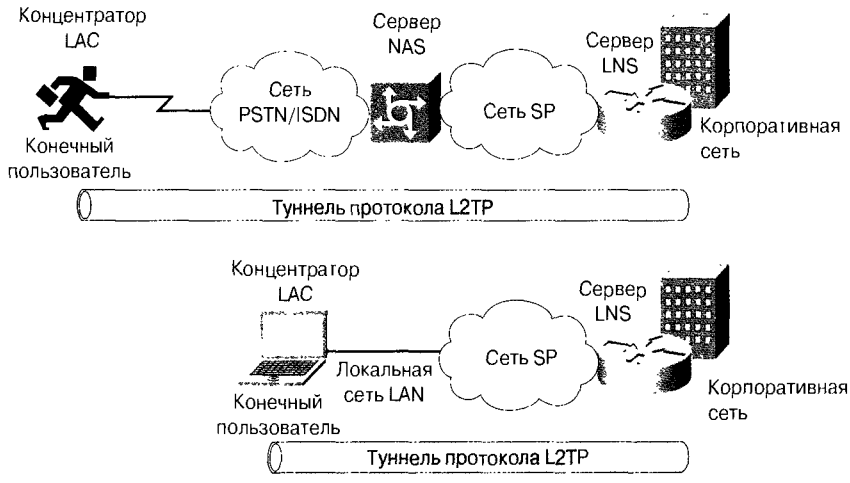


Рис. 18.05. Туннели протокола L2TP, создаваемые по желанию пользователя

Соединения протокола L2TP, защищенные посредством IPSec

Сколь бы полезным ни был протокол L2TP, необходимо признать, что он не является решением всех проблем. Он обеспечивает гибкость удаленного доступа, но не обеспечивает высокой степени безопасности для передаваемых данных. В значительной степени это связано с относительно небезопасной природой самого протокола PPP. Строго говоря, протокол PPP был разработан специально для соединений типа "точка-точка" и безопасность соединения при его разработке не была главным приоритетом.

Дополнительная причина для беспокойства связана с тем, что туннели протокола L2TP не являются криптографическими. Данные, являющиеся полезной нагрузкой, передаются открытым текстом и их упаковкой являются только фреймы протоколов L2TP и PPP. Однако реализация протоколов IPSec в сочетании с протоколом L2TP позволяет обеспечить дополнительный уровень безопасности. Как показано в разделе "Протокол IPSec", протоколы IPSec поддерживают строгую аутентификацию, а также шифрование.

VPN-сети в MPLS-сетях

VPN-сети, использующие протоколы IPSec и L2TP, описанные в предыдущих разделах, часто поддерживаются и управляются промышленными потребителями. Часто их называют VPN-сетями на основе модуля центрального процессора CPE. Однако в последние годы провайдеры служб пытаются использовать уже существующую IP-инфраструктуру для предоставления промышленным пользователя новых служб, таких как обеспечиваемые провайдером VPN-сети (Provider-Provisioned VPN — PPVPN). В настоящее время провайдерами предлагаются следующие службы VPN-сетей на основе многопротокольной коммутации по меткам (Multiprotocol Label Switching — MPLS):

- VPN-сети BGP/MPLS;
- VPN-сети 2-го уровня на базе MPLS.

VPN-сети BGP/MPLS

VPN-сети протоколов BGP/MPLS, описанные в проекте IETF: draft-ietf-ppvpn-rfc2547bis, являются VPN-сетями 3-го уровня. В этом случае промышленные пользователи полностью передают управление этими сетями провайдерам служб, которые управляют как этими сетями, так и маршрутизацией пользователя в этих сетях. Провайдеры служб, предлагающие службы VPN-сетей протоколов BGP/MPLS, уже имеют базовую IP-сеть с функциями MPLS, которая пересылает данные от одного узла пользователя к другому. Протокол BGP используется для распространения информации маршрутизации по базовой сети провайдера.

Как показано на рис. 18.6, VPN-сети MPLS включают в себя приведенные ниже основные компоненты.

- В сети провайдера службы имеются маршрутизаторы провайдера (Provider Router — PR) или P-маршрутизаторы с функциями MPLS. P-маршрутизаторы пересылают данные VPN-сети между граничными маршрутизаторами (Provider Edge Router — PE) провайдера.
- Как ясно из самого названия, граничный PE- маршрутизатор находится на границе сети провайдера. Он имеет соединения с узлами пользователя, по которым происходит обмен информацией маршрутизации с граничными маршрутизаторами пользователя или CE-маршрутизаторами (Customer Edge Router — CE). Как показано на рис. 18.6, PE-маршрутизатор может включать в себя несколько пользовательских VPN-сетей, каждая из которых имеет свою IP-адресацию и схему маршрутизации. Разделение потоков данных этих сетей достигается путем поддержки виртуальной таблицы маршрутизации и пересылки (Virtual Routing and Forwarding — VRF) для каждой отдельной виртуальной VPN-сети. Таблица VRF содержит информацию маршрутизации для каждой отдельной пользовательской сети VPN. Для обмена информацией между PE-маршрутизаторами используется протокол BGP.
- CE-маршрутизаторы обеспечивают доступ пользователя к сети провайдера службы. CE-маршрутизатор может осуществлять обмен информацией маршрутизации с PE-маршрутизатором, используя различные протоколы маршрутизации.

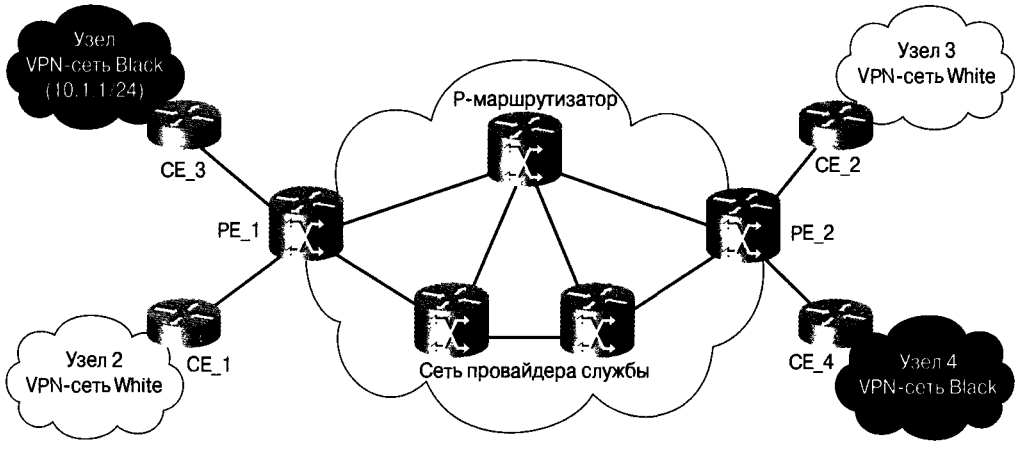


Рис. 18.6. Компоненты VPN-сетей протоколов BGP/MPLS

Проходя по среде провайдера службы MPLS, данные VPN-сетей пересылаются между PE-маршрутизаторами. Решение о пересылке принимается на основе информации от двух источников: таблицы пересылок по меткам, поддерживаемой P-маршрутизатором (также называемом маршрутизатором коммутации по метке или LSR-устройством [Label Switch Router — LSR]), и метки, содержащейся в передаваемых пакетах.

Метки MPLS, используемые для принятия решений о пересылке, представляют собой заголовки, созданные LSR-устройством. Формат метки зависит от используемой технологии канального уровня. Например, протоколы ATM и Frame Relay могут переносить метку как часть своих заголовков канального уровня — в поле VCI или VPI заголовка ячейки ATM, или в поле DLCI заголовка фрейма протокола Frame Relay. Поскольку в технологиях канального уровня, таких как Ethernet, FDDI или Token Ring, метка не может передаваться в заголовках канального уровня, для этой цели используется вспомогательный ("shim") заголовок, который вставляется между заголовками канального и сетевого уровней. Метки MPLS распространяются по сети с помощью протокола распространения меток (Label Distribution Protocol — LDP).

Пакет данных может переносить несколько меток в виде стека меток, устроенного по принципу: "последним пришел — первым вышел" ("Last-In — First-Out — LIFO). В случае использования VPN-сетей с протоколами BGP/MPLS пакеты имеют две метки. Внутренняя метка идентифицирует удаленный PE-маршрутизатор, который объявляет маршрут пользователя, а внешняя метка используется для пересылки пакета данных в среде MPLS к PE-маршрутизатору.

На рис. 18.6 предполагается, что маршрутизатор CE_1, расположенный в узле Site 2 VPN-сети White, объявляет маршрут 10.1.1/24 к маршрутизатору PE_1. Маршрутизатор PE_1 добавляет этот маршрут к своей таблице VRF VPN-сети White и назначает метку этому маршруту. Этот VPN-маршрут и метка распространяются протоколом BGP маршрутизатору PE_2, расположенному на другом конце VPN-сети White. Если узлу Site 3 VPN-сети White требуется осуществить обмен данными с узлом 10.1.1/24, то маршрутизатор CE_2 пересылает пакет маршрутизатору PE_2, опираясь на VPN-маршрут, который он получает от PE_2. После получения этого пакета маршрутизатор PE_2 просматривает свою VRF-таблицу. Этот просмотр показывает, что к узлу 10.1.1/24 можно получить доступ через маршрутизатор PE_1. Поэтому маршрутизатор PE_2 вставляет соответствующую метку, которую он получил от PE_1 для 10.1.1/24, и пытается послать пакет данных маршрутизатору PE_1.

Продолжая обсуждение, отметим, что для достижения PE_1 осуществляется еще один просмотр таблицы для нахождения метки, логически связанной с маршрутом, к маршрутизатору PE_1 в базовой сети MPLS. В конечном итоге маршрутизатор PE_2 посылает пакет данных с двумя метками. P-маршрутизаторы в среде MPLS обменивают внешнюю метку для пересылки пакетов от маршрутизатора PE_2 к маршрутизатору PE_1. Когда маршрутизатор PE_1 получает пакет, он просматривает внутреннюю метку для принятия решения о пересылке пакета требуемому CE-маршрутизатору, такому, например, как маршрутизатор CE_1. Поскольку пользователи VPN-сети могут использовать конфиденциальные IP-адреса из RFC 1918, может оказаться, что PE-маршрутизатор будет управлять двумя пользовательскими VPN-сетями, адресные пространства которых накладываются друг на друга. Это является проблемой при использовании протокола BGP, в котором предполагается, что передаваемые адреса протокола IPv4 являются глобально уникальными. Для решения этой проблемы VPN-сети протоколов BGP/MPLS используют сочетание следующих двух механизмов.

- Введение адресов протокола Ipv4 для VPN-сетей, которые превращают не являющиеся уникальными адреса протокола IPv4 в глобально уникальные адреса

семейства. Адрес протокола IPv4 содержит 8-байтовый определитель маршрута (Route Distinguisher — RD), за которым следует 4-байтовый адрес протокола Ipv4.

- Реализация многопротокольных BGP-расширений для поддержки распространения VPN-адресов протокола IPv4.

Как показано на рис 18.6, в VPN-сетях с коммутацией MPLS CE-маршрутизаторы осуществляют непосредственное одноранговое соединение с PE-маршрутизаторами. Такая модель называется одноранговой. По сравнению с моделью наложения, используемой в VPN-сетях протокола IPSec, в которой маршрутизаторы пользователя осуществляют одноранговое соединение только с другими маршрутизаторами пользователей с образованием туннеля типа "точка-точка", создающего "виртуальную магистраль", при реализации крупной сети одноранговая модель значительно легче масштабируется.

Другим преимуществом VPN-сетей с коммутацией MPLS является поддерживаемая MPLS зона качества обслуживания (Quality of Service — QoS). MPLS поддерживает классификацию пакетов в различные классы обслуживания (Classes of Services — CoS) и обработку пакетов с учетом соответствующих характеристик этих классов CoS.

VPN-сети 2-го уровня на базе коммутации MPLS

PPVPN-группа по виртуальным сетям IETF и группа PWE3 работают над определением общей структуры и стандартов для обеспечиваемых провайдерами VPN-служб 2-го уровня (Provider-Provisioned Layer 2 VPN — L2VPN). Сети L2VPN позволяют провайдеру службы предоставлять транспортные услуги служб 2-го уровня, таких как Ethernet, Frame Relay и ATM, пользователям по магистрали IP/MPLS. Они также предоставляют провайдерам возможность безболезненного перехода от инфраструктур Frame Relay и ATM к полностью основанной на MPLS IP-инфраструктуре без нарушения работы уже существующих служб.

В отличие от VPN-сетей протоколов BGP/MPLS, описанных в предыдущем разделе, пользователи, использующие L2VPN, должны сами управлять маршрутизацией в своих сетях.

Общая структура протокола L2VPN, определенная PPVPN-группой IETF, имеет две модели.

- Служба виртуального частного соединения (Virtual Private Wire Service — VPWS) реализует топологию типа "точка-точка", в которой PE-маршрутизаторы на границах базовой сети провайдера соединены "псевдокабелем" ("pseudo wire" — PW). Полезная нагрузка протоколов 2-го уровня, таких как Frame Relay или ATM, инкапсулируется входным граничным PE-маршрутизатором и пересылается между PE-маршрутизаторами в виде PDU-модулей псевдокабеля. Эта модель предлагает две многообещающие технологии:
  - Произвольная транспортировка по MPLS-сети (Any Transport Over MPLS — AToM), которая поддерживает в базовой сети MPLS любые протоколы, в частности, протоколы Frame Relay, ATM, Ethernet, PPP и HDLC. Механизмы инкапсуляции и распространения меток определены в двух группах проектов IETF: проекты Martini и проекты Kompella
  - В базовых IP-сетях для этой же цели используется протокол L2TP версии 3.
- Служба виртуальных частных локальных сетей (Virtual Private LAN Service — VPLS) реализует имитацию LAN-моста, к которому подсоединены все PE-маршрутизаторы VPLS-сетей.

Резюме

В последние годы технологии VPN-сетей стремительно развивались. Новые VPN-технологии позволяют промышленным пользователям экономить средства за счет использования VPN-сетей для безопасной передачи данных по сети Internet, а провайдерам служб дают возможность предоставлять своим пользователям новые службы.

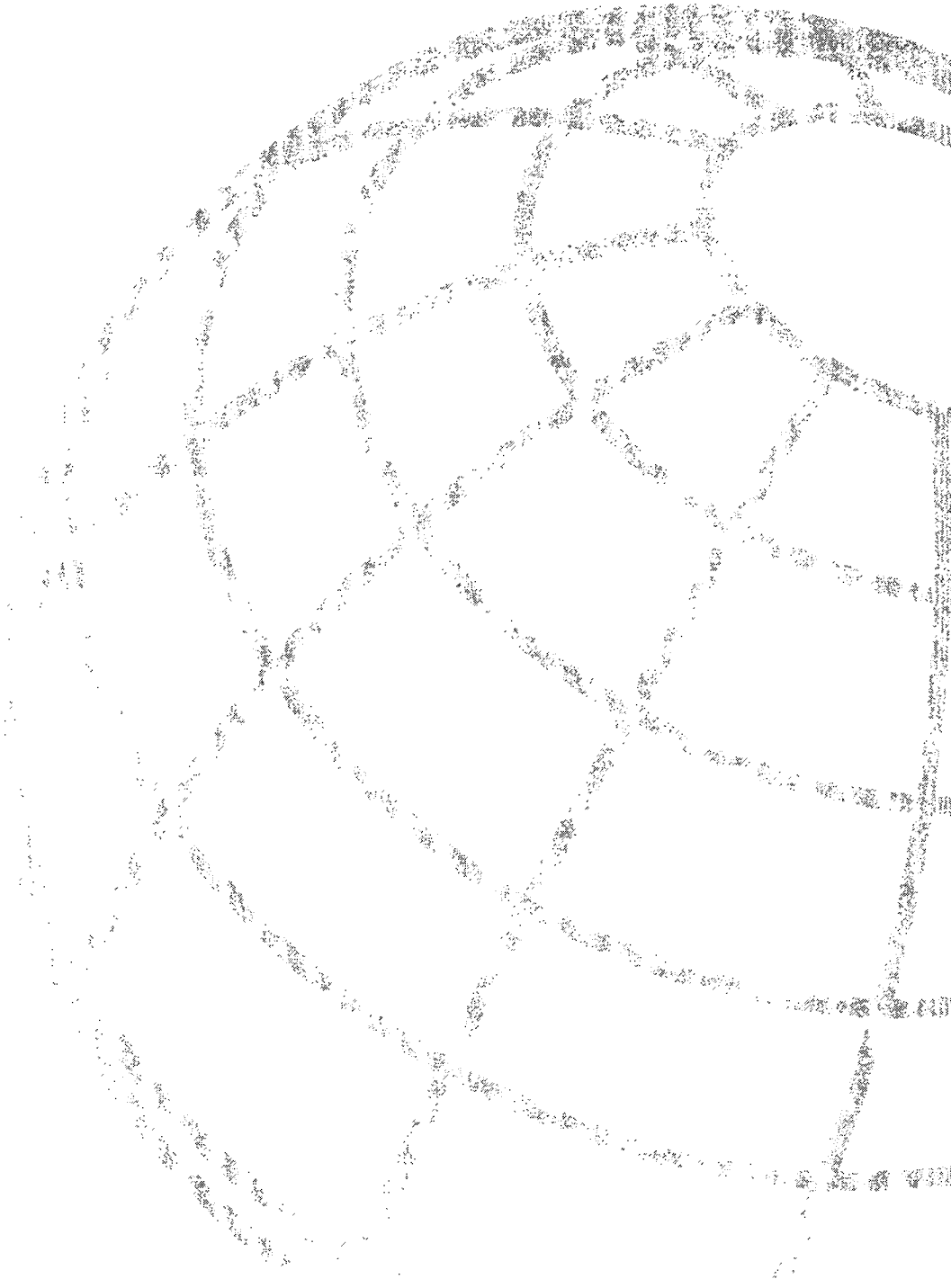
Лежащие в основе VPN-сетей технологии обеспечивают различные характеристики для разных типов VPN-сетей и могут удовлетворить разнообразные требования пользователей. VPN-сети на основе протокола L2TP, использующие протокол IPSec, обеспечивают высокий уровень безопасности и часто управляются самими промышленными пользователями. VPN-сети 2-го и 3-го уровней на основе коммутации MPLS, реализуемые провайдером службы, обеспечивают реализацию крупных сетей и строгое управление качеством обслуживания QOS.

Контрольные вопросы

1. Что представляет собой виртуальная частная сеть VPN?
2. Какие ключевые службы безопасности обеспечивает протокол IPSec?
3. Каковы функции протокола IKE?
4. Протокол IKE включает в себя две фазы. Какие функции характерны для каждой из них?
5. Каковы операционные режимы протокола L2TP?
6. Каким образом коммутация MPLS поддерживает иерархическую маршрутизацию в VPN-сетях протоколов BGP/MPLS?

Дополнительные источники

- Davie, Bruce and Rekhter Y. *MPLS Technology and Applications.*
- Schneier, Bruce. *Applied Cryptography.*
- RFC 2401, *Security Architecture for the Internet Protocol.*
- RFC 2402, *IP Authentication Header.*
- RFC 2406, *IP Encapsulating Security Payload (ESP).*
- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP.*
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP).*
- RFC 2409, *The Internet Key Exchange (IKE).*
- RFC 2661, *Layer Two Tunneling Protocol "L2TP".*
- RFC 3193, *Securing L2TP using IPSec.*
- IETF Draft: draft-ietf-ppvpn-rfc2547bis-02, *BGP/MPLS VPN.*
- IETF Draft: draft-ietf-ppvpn-l2-framework, *L2VPN Framework.*
- Virtual Private Network Consortium, http://vpnc.org.



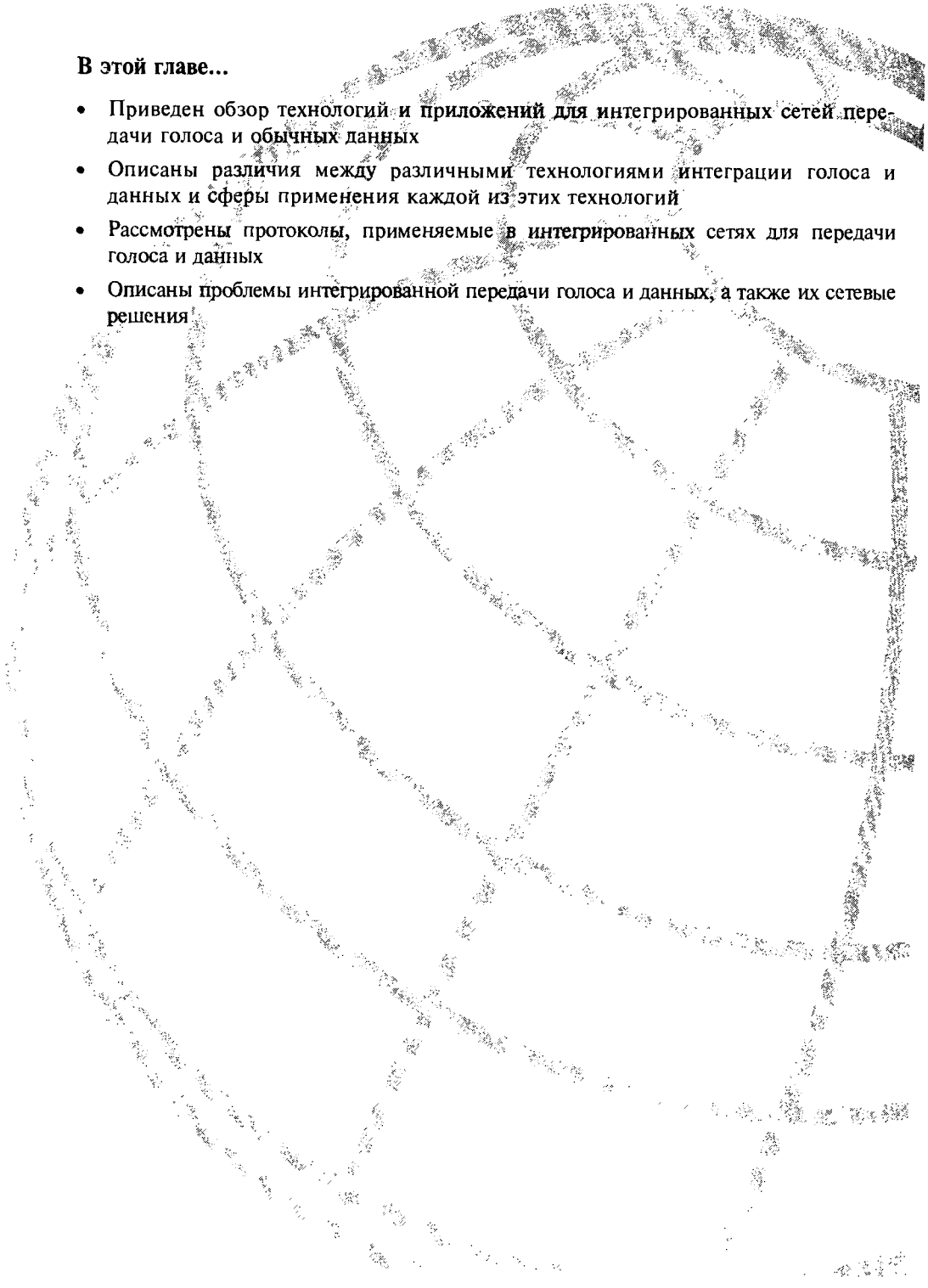
Часть IV

Технологии мультисервисного доступа

Глава 19. Интегрированная передача голосовых и обычных данных
Глава 20. Беспроводные технологии
Глава 21. Цифровые абонентские каналы
Глава 22. Технологии кабельного доступа
Глава 23. Введение в технологии оптических сетей
Глава 24. Технология передачи голосовых данных по протоколу IP
Глава 25. Протоколы динамической транспортировки пакетов и эффективного использования полосы пропускания
Глава 26. Протокол расширяемой аутентификации

В этой главе...

- Приведен обзор технологий и приложений для интегрированных сетей передачи голоса и обычных данных
- Описаны различия между различными технологиями интеграции голоса и данных и сферы применения каждой из этих технологий
- Рассмотрены протоколы, применяемые в интегрированных сетях для передачи голоса и данных
- Описаны проблемы интегрированной передачи голоса и данных, а также их сетевые решения



Глава 19

Интегрированная передача голосовых и обычных данных

Введение

Интегрированная передача голоса и данных важна для разработки как провайдерских, так и корпоративных сетей. Провайдеров привлекает низкая стоимость — в настоящее время стоимость передачи голосовых пакетов составляет от 20 до 50% стоимости передачи по обычным аналоговым голосовым каналам. Разработчики корпоративных сетей заинтересованы в уменьшении затрат, связанных с уплатой пошлин и с транзитной коммутацией. И те, и другие заинтересованы также в так называемой "неявной" экономии, получаемой за счет удешевления обслуживания и более эффективного контроля и управления сетью. Наконец, пакетные голосовые системы открывают доступ к новым, улучшенным службам, таким как Unified Messaging и управление приложениями, а те, в свою очередь, обещают повышение производительности труда пользователей и более разнообразное обслуживание.

В последние годы, благодаря взаимодействию сторон, обеспечивающих спрос и предложение, развитие технологий интегрированной передачи голоса и данных значительно ускорилось. Потребители увеличивают инвестиции в сетевую инфраструктуру, чтобы воспользоваться преимуществами интегрированных приложений, в том числе и голосовых. Производители получили возможность воспользоваться научными достижениями во многих областях, в частности в тех, которые связаны со стандартами, технологиями и производительностью сетей.

Стандарты

Многие стандарты для взаимодействия при передаче голосовых сигналов были ратифицированы и доведены до приемлемой функциональной совместимости. Это уменьшает риск и затраты, с которыми сталкиваются производители компонентов систем интегрированной передачи голоса и данных. Уменьшается и риск потребителя. Такие стандарты, как H.323 (утвержденный ITU в июне 1996 г.), в настоящее время проходят третью и четвертую редакцию, а ранее созданные продукты, хотя и основаны на первоначальных стандартах, тем не менее обладают обширными возможностями и функциональной совместимостью. В свою очередь, общая законченность стандартов привела к появлению надежных

стеков протоколов, которые можно приобрести "со склада" у поставщиков, еще более повысив гарантии функциональной совместимости.

Технология

Недавние технологические достижения также сделали возможной интегрированную передачу голоса и данных. Например, новая технология процессора цифровых сигналов (Digital Signal Processor — DSP) позволила обрабатывать аналоговые сигналы в цифровых доменах, что еще несколько лет назад было затруднительно, если вообще возможно. Эти новые мощные микросхемы работают с огромной скоростью, позволяя квантовать, оцифровывать и осуществлять сжатие голосовых данных в режиме реального времени. Дальнейшие технологические достижения позволяют одной микросхеме обрабатывать до четырех разговоров одновременно, и производительность продолжает повышаться. Такие технологии значительно уменьшают стоимость и сложность разрабатываемых продуктов, а также снижают затраты на внедрение систем интегрированной передачи голоса и данных.

В других областях промышленности также используются достижения технологий голосового кодека (кодера/декодера). Ранее предполагалось, что качество звука пострадает из-за почти линейного уменьшения полосы пропускания. Однако благодаря новым, более сложным алгоритмам, применяемым в современных кодеках, ситуация изменилась. В настоящее время существует возможность получать достаточно качественный звук при значительно меньшей, чем требовалась ранее, полосе пропускания. И, что наиболее важно, эти новые алгоритмы вошли в стандарты, обеспечив тем самым функциональную совместимость для передачи голосовых данных с высокой степенью сжатия данных.

Производительность сети

Кроме вышесказанного, следует отметить, что сетевые технологии передачи данных усовершенствовались до такой степени, что стали обеспечивать надежную передачу голосовых данных. В последние годы рост объема передачи голосовых данных был сравнительно невелик, в то время как объем передачи обычных рос экспоненциально. В результате во многих сетях в настоящее время объем обычных данных превышает голосовой. Кроме того, возросла относительная важность цифровых данных, так как предприятия и организации все чаще опираются в своей работе на повсеместное использование компьютерных сетей. Это повышение важности компьютерных сетей привело к коренным изменениям в способах проектирования, построения и управления такими сетями. Традиционное моделирование по принципу "негарантированной доставки" уступило место созданию усовершенствованных сетей, основанных на политиках, с управляемым качеством обслуживания, поддерживающих еще более широкий спектр приложений. Передача голосовых данных, как приложение в обычных компьютерных сетях, значительно выиграла от применения этих технологий. Например, поддержка чувствительных к задержкам SNA-данных по IP-сетям привела к совершенствованию управления задержками и установки приоритетов в очередях, что впоследствии было применено к передаче голосовых данных.

Как уже отмечалось, внедрение новых технологий и приложений во многом определяется спросом пользователей. Достижения технологии претворяются в жизнь, но только в том случае, если они удовлетворяют реальные потребности пользователей и

не требуют неприемлемых для них затрат. Например, технологии цифровой аудиозаписи на ленту (Digital Audio Tape — DAT) так и остались достоянием горстки любителей из-за своей высокой стоимости и лишь незначительного повышения качества воспроизведения по сравнению с аналоговыми лентами. Однако интегрированная передача голоса и данных предоставляет пользователю весьма реальные преимущества как в настоящее время, так и в будущем. Большинство пользователей этих технологий имеют двойную выгоду: уже сейчас цифровые технологии передачи голосовых пакетов дешевле аналоговых, а в будущем они будут обладать и большими возможностями, чем сегодняшние голосовые каналы.

Экономическая эффективность

По оценкам специалистов, затраты на сети пакетной передачи голоса составляют всего 20–30% соответствующих затрат на обычные голосовые каналы. Это касается как телефонных компаний (провайдеров), так и коммерческих (частных) пользователей. Отсюда следует логический вывод: для корпоративных пользователей службы удаленной передачи голосовых данных могут обходиться дешевле, чем междугородные звонки, и зачастую дело обстоит именно таким образом. Например, многие корпоративные пользователи внедрили технологии интегрированной передачи голоса вместе с обычными данными по распределенным компьютерным сетям между традиционными АТС, расположенными в различных городах. Экономия на междугородных переговорах часто окупает затраты уже через полгода (особенно если речь идет о международных звонках). Использование компьютерных систем в качестве "виртуальных связующих звеньев" между коммутаторами для передачи голоса полезно и для провайдеров служб. По этой причине, по мере дальнейшего развития их первичной сетевой инфраструктуры, многие из них начали использовать технологии пакетной передачи голоса.

Однако экономия от применения технологий пакетной передачи голоса не ограничивается только передачей. Благодаря использованию этих технологий коммутация телефонных звонков в домене компьютерной сети становится дешевле, чем при использовании обычных телефонных коммутаторов. Крупные предприятия с несколькими филиалами могут сэкономить средства за счет использования компьютерных сетей в качестве "транзитных коммутаторов" при маршрутизации звонков между АТС-станциями по принципу "call-by-call". Получающаяся структура голосовой сети проще администрируется и имеет надежную, неблокирующую коммутацию, в основе которой лежит компьютерная система.

Совершенствование приложений

Реальная экономия средств является достаточной причиной для внедрения технологий интегрированной передачи голоса и данных. Но есть и дополнительные преимущества, которые станут более очевидными в будущем. Благодаря интеграции голосовых и компьютерных приложений будет повышаться производительность труда пользователей. Интеграция компьютерной телефонии (Computer Telephony Integration — CTI) была начата производителями АТС в 80-х годах XX века в целях внедрения компьютеров в АТС и применения таких новых функций, как "консультационный центр" (например экранные меню для агентов).

Однако по мере дальнейшей интеграции передачи голоса и данных, различий между голосовыми и цифровыми приложениями будет все меньше. Например, некоторые сис-

темы Unified Messaging уже сейчас позволили объединить голосовую почту, электронную почту и факсимильные сообщения в одну удобную систему. Их пользователи могут читать электронные письма по телефону и прилагать документы к голосовой почте. На уровне предприятия новые приложения, такие как виртуальные консультационные центры, позволяют помещать агентов в любой точке компьютерной сети, сохраняя все функции и свойства консультационного центра. Агенты даже могут получать вызовы на своих компьютерах вместо традиционных телефонных аппаратов, организовать "комбинированный консультационный центр" и отвечать на вопросы пользователей через Web, используя электронный чат и электронную почту наравне с телефонными звонками. Эти возможности выходят далеко за рамки обычной экономии. Они, безусловно, сделают работу организаций гораздо эффективнее и выгоднее.

Острая потребность в сетях с интегрированной передачей голоса и данных привела к различным вариантам решения этой проблемы, у каждого из которых есть свои преимущества и недостатки. Существует три основных подхода к этому вопросу:

- передача голоса по сетям ATM;
- передача голоса по сетям Frame Relay;
- передача голоса по IP-сетям.

Существуют также смешанные решения, в которых комбинируются варианты передачи голоса по IP, Frame Relay и т.д. Как показано на рис. 19.1, передача голоса по сетям ATM и Frame Relay применяется в основном между АТС, а передача голоса по протоколу IP — между компьютерами. Подробнее эти механизмы будут рассмотрены ниже.

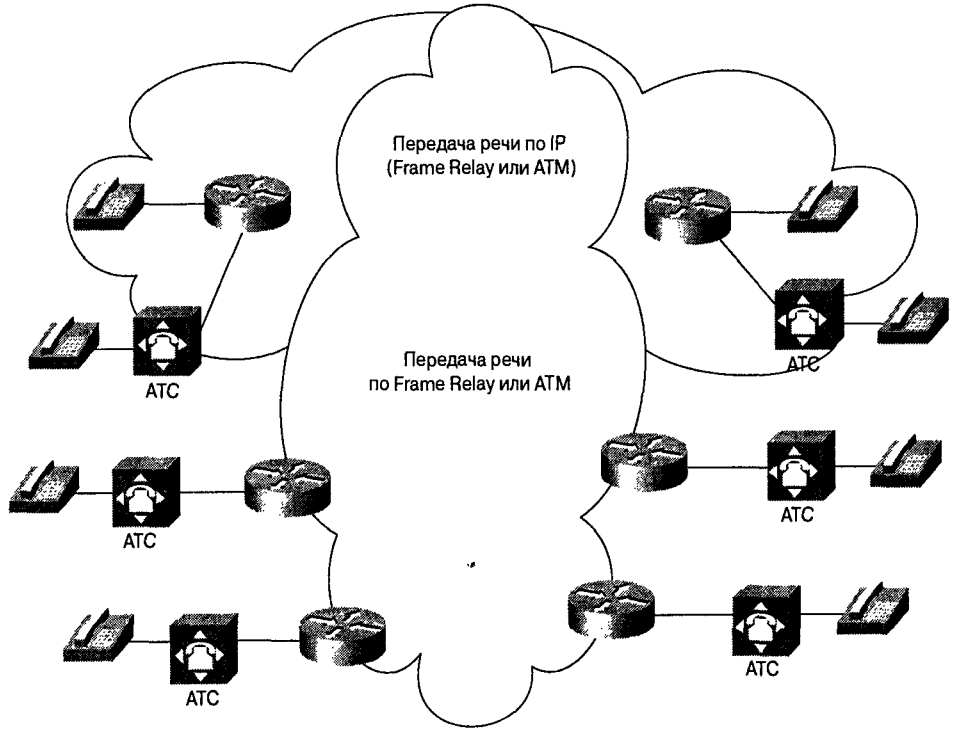


Рис. 19.1. Смешанные варианты передачи голоса по сетям IP, Frame Relay и т.д.

Современные технологии передачи голосовых данных

Передача голоса по сетям ATM (Voice Over ATM — VoATM) может осуществляться как стандартная эмуляция голосового канала с импульсно-кодовой модуляцией (AAL1, рассматривается ниже) или как передача голоса в ячейках ATM с переменной битовой скоростью (AAL2, также рассматривается ниже). Использование коммутации ATM имеет много преимуществ при передаче и коммутации голосовых данных. Прежде всего, это гарантированное качество обслуживания (Quality Of Service — QoS), определяемое провайдером для пользователя или для каждого звонка в отдельности. Кроме того, в основе сигналов настройки вызова для коммутируемых виртуальных каналов ATM (Switched Virtual Circuits — SVC), Q.2931, лежат сигналы настройки вызова для голосового ISDN, Q.931. Администрирование сходно с обычными телефонными каналами.

Однако применение технологии VoATM страдает от излишней сложности, недостаточной поддержки и слабого взаимодействия между производителями. Наблюдается тенденция к удорожанию из-за ориентации исключительно на оптические сети. И, что наиболее важно, ATM обычно внедряется как протокол 2-го уровня распределенных сетей и потому не распространяется на всю сеть, вплоть до настольных ПК. Тем не менее, ATM достаточно эффективно выполняет функции магистрали и транзитного коммутатора между существующими голосовыми коммутаторами и АТС.

Передача голоса по сетям Frame Relay получила широкое распространение. Как и технология VoATM, она обычно применяется в качестве связующей магистрали или транзитного коммутатора между удаленными АТС. Ее преимущество заключается в более простом администрировании и в относительно невысокой по сравнению с VoATM стоимости, особенно при использовании в частных распределенных сетях. Ее масштабирование также экономичнее, чем у VoATM, благодаря поддержке различных каналов — от T1 до 56 Кбит/с. Если сеть Frame Relay тщательно спроектирована, то технология VoFR работает очень надежно и обеспечивает высокое качество. Однако качество голоса в сетях Frame Relay может страдать из-за нестабильности и задержек. Несмотря на то, что требования к минимальной полосе пропускания и всплескам постоянно снижаются, нестабильность и задержки часто не включаются в соглашения об уровне обслуживания (Service Level Agreements — SLA), заключаемые с провайдерами. В результате скорость передачи голоса непостоянна. Даже если поначалу качество удовлетворительно, со временем, по мере насыщения сети провайдера различными потоками данных, оно может ухудшиться. По этой причине многие крупные корпоративные потребители начинают указывать в своих требованиях к провайдеру допустимый уровень нестабильности и задержки вместе со средней пропускной способностью, обеспечиваемой сетью провайдера. В таких ситуациях обеспечивается высококачественная передача голоса по сети Frame Relay.

В последние годы начала внедряться передача голоса по IP-сетям. В отличие от передачи голоса по сетям Frame Relay и ATM, передача голоса по IP-сетям является решением 3-го уровня (сетевого). Она более значима и полезна, так как протокол IP распространяется вплоть до настольных персональных компьютеров. Это означает, что, кроме обеспечения основной магистральной связи и транзитной коммутации для АТС, технология VoIP может начать заменять АТС в качестве приложения. Как решение 3-го уровня, VoIP маршрутизируется и может прозрачно передаваться в любой сетевой инфраструктуре, включая сети Frame Relay и ATM. Из всех технологий пакетной

передачи голоса для VoIP характерны, вероятно, наибольшие проблемы в обеспечении качества, потому что качество обслуживания при использовании этой технологии не гарантируется. Обычные приложения, такие как протокол TCP, работающие в IP-сетях, не чувствительны к задержкам. Они лишь должны повторно отправлять пакеты, потерянные из-за коллизий и перегрузок. Передаваемая речь более чувствительна к задержкам пакетов, чем к их потере. Кроме обычной перегрузки сети, качество обслуживания в сетях VoIP часто зависит от нижних уровней, которые не различают голосовые и цифровые потоки данных.

Сети для передачи голосовых данных

Основы голосовых технологий были заложены более 100 лет назад. За это время они развились настолько, что стали вездесущими и часто невидимыми для большинства пользователей. Это наследие медленной эволюции во многом продолжает влиять и на современные усовершенствованные голосовые сети, поэтому важно сначала освоить основы традиционной голосовой технологии, и только потом переносить ее на компьютерные сети.

В традиционных аналоговых телефонных аппаратах, применяемых в обычных телефонных сетях, для подключения к сети используется простой двухпроводной интерфейс. Комбинация входящих и исходящих сигналов в них определяется внутренним двух- и четырехпроводным гибридным каналом. Такой экономичный подход эффективен, но требует принятия специальных мер по борьбе с отраженным звуком. Следует отметить, что стоимость и необходимость прокладки новых кабелей практически исключают возможность создания четырехпроводной цепи от пользователя к телефонной станции.; вследствие этого локальное ответвление к абоненту проходит через гибридные фильтрующие каналы, которые позволяют передавать дуплексные сигналы в обоих направлениях по одному и тому же двухпроводному каналу.

Гибридное эхо является первичным источником общего эха, генерируемого общедоступной телефонной сетью (public switched telephone network — PSTN). Это электрически генерируемое эхо создается по мере того, как голосовые сигналы передаются по сети через гибридное соединение в точках преобразования двухпроводного канала PSTN в четырехпроводной, при котором электрическая энергия отражается от четырехпроводного канала в направлении абонента. На маршруте прохождения сигнала между двумя телефонными аппаратами, в том числе и при удаленном вызове, требуется усиление сигнала с использованием четырехпроводного канала в сети PSTN.

Основы телефонии

Для традиционной телефонии требуется три типа сигналов: слежения, уведомления и адресации. Сигнал слежения позволяет наблюдать за состоянием устройств — например, сообщает центральному офису или АТС о том, что снята трубка и набирается номер, или что разговор окончен. Сигнал уведомления предназначен для того, чтобы сообщать пользователю о входящем звонке или о состоянии вызова ("занято", "перезвоните" и т.п.). Наконец, сигнал адресации дает возможность пользователю набрать добавочный номер.

Кроме сигналов, телефонные службы предоставляют защищенную среду для передачи голоса, обеспечивают аналого-цифровое преобразование, соединение и заземление, электропитание и, при необходимости, выполнение других функций.

За годы развития аналоговые голосовые интерфейсы стали обеспечивать эти основные функции для определенных приложений. Поскольку основные двухпроводные аналоговые интерфейсы телефонных сетей работают по модели "ведущий/ведомый", компьютерное оборудование должно имитировать два основных типа аналоговых интерфейсов: пользовательский и сетевой. Пользовательский интерфейс (телефон) должен получать от сети питание и сигнал слежения.

Для соединения с аналоговым телефоном, факсом, модемом или другим устройством, которое может быть подключено к телефонной линии, используется интерфейс внешней службы обмена (Foreign Exchange Service — FXS). С его выхода снимается постоянное напряжение 48 В, сигнал звонка и т.п., а на вход поступают цифры набираемого номера. Противоположностью интерфейса FXS является интерфейс офиса внешнего обмена (Foreign Exchange Office — FXO). Он используется для соединения с системой коммутации, обеспечивая обслуживание и слежение, и предполагает, что коммутатор обеспечивает слежение и другие элементы. (У читателя может возникнуть вопрос: почему используется термин "внешний" обмен? Дело в том, что термины *FXS* и *FXO* первоначально использовались в сетях телефонных компаний для описания телефонных услуг, предоставляемых другим центральным офисом, а не тем, на который эти обязанности обычно возлагаются.)

В интерфейсах FXS и FXO необходимо также имитировать варианты слежения. Обычные телефоны работают в режиме циклического старта. Обычно в телефоне имеется высокое сопротивление между двумя проводами. Когда на приемнике снимают трубку, между двумя проводами замыкается цепь с низким сопротивлением. Затем коммутатор, на который поступил ток, определяет, что трубка снята, и посылает сигнал набора. Кроме того, коммутатор, прежде чем послать звонок, проверяет, не снята ли трубка на приемнике. Эта система хорошо работает в простых телефонах, но может вызвать проблемы на магистралях между АТС и СО с высокой активностью. В такой ситуации удаленная система и коммутатор СО могут попытаться занять линию одновременно. Подобная ситуация, называемая "бликом" (glare), может "заморозить" магистраль до того момента, пока одна из сторон ее не освободит. Решение проблемы заключается в коротких предупреждениях или звонках на "землю", оповещающих о занятии линии, а не зацикливании. Такой метод называется "*стартом от земли*" ("ground start").

После того как линия занята, необходимо набрать номер. Человеческие пальцы не могут сделать это быстрее, чем срабатывают приемники набора в современных коммутаторах, но при автоматическом наборе АТС такое возможно. В этом случае многие аналоговые магистрали используют метод задержки старта, или "мерцающий старт", чтобы уведомить вызывающее устройство о том, что коммутатор готов принять цифры набора.

Еще одним аналоговым интерфейсом, часто используемым для магистралей, является интерфейс E&M. Он представляет собой четырех- или шестипроводной интерфейс, в котором, кроме голосовой пары, предусмотрены отдельные провода для слежения. Аббревиатура *E&M* означает "ear and mouth" ("ухо и рот") или "earth and magneto" ("земля и индуктор"). Провода интерфейса E&M используются для подачи сигналов о состоянии трубки: снята или повешена.

Аналоговая передача голоса полноценно работает для основных магистральных соединений между коммутаторами или АТС, но неэкономична, если количество соединений превышает 6–8 каналов. На этой стадии, как правило, более эффективно использование цифровых магистралей. В Северной Америке применяется магистраль T1 (со скоростью 1,544 Мбит/с), которая может поддерживать 24 оцифрованных аналоговых

разговора. В других частях света используется E1 (2,048 Мбит/с), поддерживающая 30 голосовых каналов. (Применение линий E1 и T1 в разных странах инженеры называют "правилом бейсбола" — обычно линии T1 распространены там же, где популярна игра в бейсбол: крупнейшие сети T1 находятся в Соединенных Штатах, Канаде и Японии, а в других странах используется E1.)

Первым шагом в оцифровке является квантование голосовых данных. Согласно теореме Найквиста, частота квантования должна быть вдвое больше наивысшей желаемой частоты. Некогда специалисты по телефонии решили, что диапазон в 4000 Гц будет достаточным для того, чтобы можно было разобрать человеческую речь (что соответствует производительности длинных аналоговых петель). Поэтому голосовые каналы квантуются со скоростью 8000 раз в секунду, или один раз в 125 мс. Размер кванта определяется 8-разрядным числом, что в итоге обеспечивает передачу 64000 битов в секунду. В заключение выполняется настройка громкости (компандирование) для повышения точности низко-амплитудных компонент. В Северной Америке для этого применяется u-закон (или mu-закон), а в остальных странах — обычно A-закон. При передаче по объединенным сетям, согласно действующему соглашению, Северная Америка выполняет соответствующее преобразование.

При создании линии T1 объединяются 24 канала с общей пропускной способностью 1,536 Мбит/с, к которым каждые 125 мс добавляются еще 8 битов для создания фрейма, что требует скорости передачи 1,544 Мбит/с. Часто фреймы T1 объединяются в более крупные структуры, называемые суперфреймами (12 фреймов) и расширенными суперфреймами (24 фрейма). Дополнительные сигналы могут передаваться "заимствованными битами" (robbing bits) из внутренних фреймов.

Основные интерфейсы T1 и E1 имитируют набор аналоговых голосовых магистралей и используют для передачи информации слежения, подобно аналоговой модели E&M, заимствование сигнального бита. Таким образом, каждый канал передает свои собственные сигналы. Такой интерфейс называется канально-ассоциированной сигнальной системой (Channel Associated Signaling — CAS). Более эффективный метод использует общие сигналы для всех голосовых каналов. Наиболее типичным примером такой общеканальной сигнализации (Common Channel Signaling — CCS) является первичный интерфейс обмена (Primary Rate Interface — PRI) в сетях ISDN.

Для успешной интегрированной передачи голоса и данных, а также обеспечения максимально широкого диапазона приложений необходима поддержка всех этих голосовых интерфейсов. За последние годы пользователи привыкли к определенному уровню производительности, надежности и обслуживания телекоммуникационных систем, который должен поддерживаться и далее. Все эти вопросы сегодня решаются различными системами пакетной передачи речи, поэтому пользователи могут получить тот уровень обслуживания, к которому они привыкли.

Передача голоса по сетям ATM

Для того чтобы представить различные типы потоков данных в сетях VoATM, форум ATM и ITU определили различные классы служб.

Разработанные в основном для голосовых коммуникаций, классы с постоянной битовой скоростью (Constant Bit Rate — CBR) и с переменной битовой скоростью (Variable Bit Rate — VBR) позволяют передавать данные в реальном времени и гарантировать определенное качество обслуживания. В частности, класс CBR позволяет

определить во время вызова полосу пропускания, величину сквозной задержки и пределы ее изменения.

Неопределенная битовая скорость (Unspecified Bit Rate — UBR) и доступная битовая скорость (Available Bit Rate — ABR) были определены для потоков данных переменной интенсивности и больше подходят для приложений, работающих с цифровыми данными. В частности, класс UBR не дает гарантий доставки цифровых данных.

Выбор метода передачи голосовых каналов по сетям ATM зависит от природы передаваемых данных. Для различных типов данных были разработаны разные типы адаптаций ATM, со своими преимуществами и недостатками. Наиболее распространенным является первый уровень адаптации ATM (ATM Adaptation Layer 1 — AAL1), используемый в службах класса CBR.

Неструктурированный уровень адаптации AAL1 принимает непрерывный битовый поток и помещает его в ячейки ATM. Это распространенный метод поддержки полного сквозного байтового потока E1. При его использовании проблема заключается в том, что полный E1 может быть отправлен независимо от количества действительно используемых голосовых каналов. (E1 является схемой глобальной цифровой передачи, используемой главным образом в Европе и обеспечивающей передачу данных со скоростью 2,048 Мбит/с.)

Структурированный AAL1 содержит среди полезных данных указатель, позволяющий поддерживать структуру нулевого уровня цифровых сигналов (Digital Signal level 0 — DS0) в последующих ячейках. Это обеспечивает эффективную работу сети без использования пропускной способности свободных DS0. (DS0 представляет собой фреймовую спецификацию, применяемую при передаче цифровых сигналов по отдельному каналу T1 со скоростью 64 Кбит/с.)

Функция переназначения позволяет сети ATM прервать передачу структурированных ячеек AAL1 и переслать DS0 другому получателю. Это ликвидирует потребность в постоянных виртуальных каналах (Permanent Virtual Circuits — PVC) между всеми возможными комбинациями источник/получатель. Главным отличием от предыдущих подходов является отсутствие PVC-каналов через всю сеть.

Сигнализация в сетях VoATM

На рис. 19.2 представлена схема метода прозрачной передачи голосовых сигналов по сети. Для передачи голосовых сигналов создаются PVC-каналы. Сначала от одной конечной станции к другой по сигнальному PVC-каналу прозрачно передается сигнальное сообщение. Затем координация конечных систем позволяет выбрать PVC-канал для обмена голосовыми данными между конечными станциями.

Сеть ATM не участвует в интерпретации сигналов, передаваемых между конечными станциями. Однако в состав некоторых продуктов входит дополнительная функция распознавания канально-ассоциированных сигналов (Channel Associated Signaling — CAS), предотвращающая посылку пустых голосовых ячеек, если на конечной станции трубка не снята.

На рис. 19.3 изображена модель преобразования. В этой модели сеть ATM интерпретирует сигналы, поступающие как с сетевых устройств ATM, так и с других сетевых устройств. В отличие от предыдущей модели, где PVC передаются по сети прозрачно, в данном случае между конечными станциями и сетью ATM созданы каналы PVC.

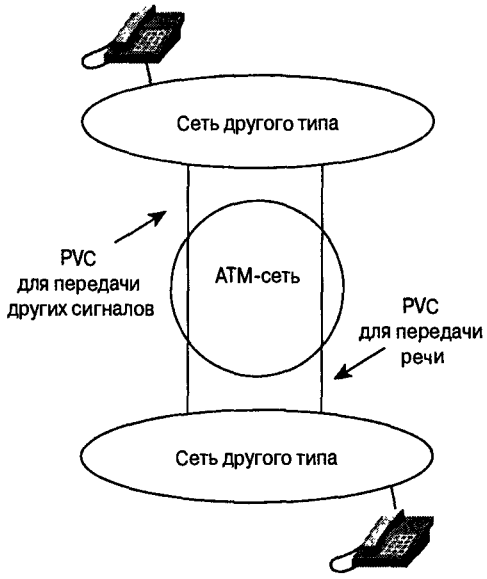


Рис. 19.2. Модель передачи сигналов VoATM описывает метод прозрачной передачи голосовых сигналов по сети

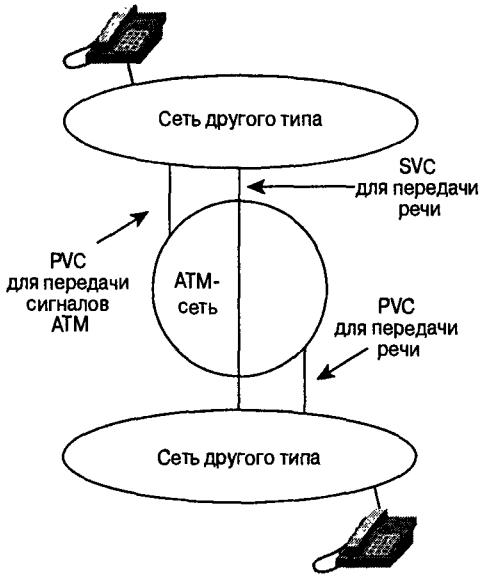


Рис. 19.3. В модели преобразования сигналов VoATM сеть ATM интерпретирует сигналы, поступающие как с сетевых устройств ATM, так и с других сетевых устройств

По сигнальному запросу конечной станции ATM-сеть создает для этой конечной станции SVC-канал с соответствующим качеством обслуживания QoS. Создание SVC-каналов выгоднее, чем предварительное открытие PVC, по следующим трем причинам.

- Каналы SVC используют полосу пропускания эффективнее, чем PVC-каналы.
- Качество обслуживания SVC-соединений не обязательно должно быть постоянным, как для PVC-каналов.
- Возможность коммутации вызовов внутри сети может привести к исключению транзитных, а возможно, и конечных мини-АТС.

Адресация в сетях VoATM

Стандарты ATM поддерживают частную и открытую схемы адресации. Обе они работают с адресами длиной в 20 байтов (рис. 19.4). Дополнительная информация о стандартных форматах адресации ATM приведена на рис. 31.9 в главе 31 "Коммутация в режиме ATM".

Идентификатор полномочий и формата AFI (Authority and Format Identifier — AFI) определяет используемый формат адресации. В настоящее время определены три идентификатора AFI: код страны (Data Country Code — DCC), международный код (International Code Designator — ICD) и E.164. Каждый из них определяется стандартами. Вторая часть адреса представляет собой начальный идентификатор домена (Initial Domain Identifier — IDI). Этот адрес однозначно определяет сеть клиента. IDI схемы E.164 длиннее и соответствует 15-значному номеру сети ISDN. Последняя часть является внутридоменным адресом (Domain-Specific Part — DSP) и определяет логические группы и конечные станции ATM.

Рис. 19.4. Коммутация ATM поддерживает 20-байтовые адреса

В транспортной модели не требуется знать скрытую адресацию, используемую голосовой сетью. Но в модели преобразования возможность соединения сетевого устройства, не принадлежащего сети ATM, с сетевым устройством ATM требует преобразования адресов. К счастью, ATM поддерживает схему адресации E.164, которая используется телефонными сетями во всем мире.

Маршрутизация VoATM

В технологии ATM применяется *частный межсетевой интерфейс (Private Network-to-Network Interface — PNNI)* — иерархический протокол маршрутизации состояния канала, который можно масштабировать для глобального использования. Кроме определения досягаемости и маршрутизации в пределах сети ATM, он также позволяет производить вызовы.

Запрос вызова виртуального канала (Virtual Circuit — VC) создает соединение с определенными требованиями к QoS, выдвигаемыми сетью ATM. Маршрут в сети определяется исходным коммутатором ATM на основании определенного им по протоколу PNNI и запросу QoS наилучшего сетевого пути. Каждый встречающийся на маршруте коммутатор проверяется на наличие требуемых для соединения ресурсов.

Когда соединение установлено, голосовые данные передаются между конечными станциями так, как если бы между ними существовал выделенный канал. Эта спецификация определяет маршрутизацию в частных сетях. В сетях провайдера межкоммутаторным протоколом является B-ICI. Последние исследования и разработки интегрированной маршрутизации в и других сетях откроют новые возможности построения голосовых сетей и сетей ATM уровня трансляции.

B-ICI представляет собой интерфейс между двумя провайдерами или операторами сетевых служб по общедоступной сети. Он является точкой демаркации, обозначающей границу между сетями таких провайдеров. Физический уровень интерфейса между двумя операторами основан определенном CCITT интерфейсе сетевого узла (Network Node Interface — NNI), к которому добавляются физические уровни DS3 и E3. Спецификация B-ICI также включает в себя специфические для службы функции, находящиеся над уровнем ATM, которые требуются для транспортировки, функционирования и управления рядом межоператорных служб через B-ICI.

Задержки в VoATM

В ATM существует несколько механизмов управления задержкой и ее вариацией. Возможности QoS позволяют ATM осуществлять запрос на передачу данных с постоянной

битовой скоростью, гарантированной полосой пропускания и диапазоном задержки. Использование очередей виртуальных каналов VC дает возможность обрабатывать каждый поток отдельно. Голосовым потокам при передаче может быть установлен более высокий приоритет. Использование малых ячеек фиксированного размера сокращает задержки, вызванные установкой в очередь и их вариации, вызванные переменным размером пакетов.

Передача голоса по сетям Frame Relay

Технология передачи голоса по сети Frame Relay позволяет передавать речь в прямом эфире (например, телефонные разговоры и факсы). Frame Relay — распространенный и недорогой способ передачи, предоставляемый большинством крупных телекоммуникационных компаний.

Сигнализация VoFR

Исторически сложилось так, что для установки вызова в сетях Frame Relay использовались фирменные протоколы производителя. Это приводило к тому, что продукты разных производителей оказывались несовместимыми друг с другом. На форуме Frame Relay FRF.11 были стандартизированы установка вызова, типы кодирования и форматы пакетов VoFR, что стало базой взаимодействия между различными производителями.

Адресация VoFR

Преобразование адресов производится по статическим таблицам, при этом набранные цифры соответствуют определенным каналам PVC. Маршрутизация голосовых потоков зависит от того, какой протокол маршрутизации был выбран для установки канала PVC и какое оборудование применяется в сети Frame Relay. Маршрутизация может быть основана на ограничении полосы пропускания, количестве переходов, на величине задержки или некоторой комбинации этих параметров, однако большинство типов маршрутизации основано на максимальном использовании полосы пропускания.

Для обеспечения минимального количества промежуточных сетевых узлов и максимальной возможности выбора различных типов QoS применяется полное объединение каналов PVC для голоса и данных. Такая сеть обеспечивает минимальную задержку и повышает качество речи, но является наиболее дорогостоящей.

Расценки большинства провайдеров Frame Relay основаны на количестве используемых каналов PVC. Для уменьшения затрат можно настроить сегменты голоса и данных таким образом, чтобы использовать один и тот же PVC, тем самым сократив количество требуемых каналов PVC. В этой структуре голосовые вызовы маршрутизируются коммутатором центрального узла. У нее есть потенциал для создания промежуточных узлов на случай, если речь должна передаваться между удаленными офисами. Однако в этом случае удается избежать компрессии и декомпрессии, возникающей при использовании транзитной АТС.

В сетях Frame Relay имеется ряд механизмов, которые могут минимизировать задержку и ее вариацию. Наличие длинных фреймов данных в низкоскоростных каналах Frame Relay может привести к задержкам, неприемлемым для голосовых фреймов. Для частичного решения этой проблемы некоторые производители применяют мень-

шие размеры фреймов, чтобы уменьшить задержку и ее вариацию. На форуме FRF.12 было предложено внести эту процедуру в промышленный стандарт для обеспечения функциональной совместимости продуктов разных производителей и для того, чтобы потребители знали, какое качество голоса можно ожидать.

Назначение голосовым фреймам более высокого приоритета по сравнению с фреймами данных тоже помогает уменьшить задержку и ее вариацию. Различные производители используют разные сочетания этого подхода с уменьшением размера фреймов. Для обеспечения хорошего качества речи на каждом канале PVC должна быть определена согласованная скорость передачи информации (Committed Information Rate — CIR) таким образом, чтобы исключить отбрасывание голосовых фреймов. В перспективе сети Frame Relay будут обеспечивать передачу сигналов установки вызова по каналам SVC и, возможно, устройства DTE Frame Relay смогут запрашивать QoS для вызова. Все это должно повысить качество VoFR.

Передача голоса по протоколу IP

Как уже отмечалось, передача голоса по протоколу IP (voice over IP — VoIP) является решением скорее 3-го уровня OSI, а не 2-го уровня. Данная функция позволяет VoIP работать автономно в сетях Frame Relay и ATM. Но, что наиболее важно, VoIP работает в обычных локальных сетях, вплоть до настольных ПК. В этом смысле VoIP является скорее приложением, чем службой и это учитывалось в процессе эволюции протоколов VoIP.

Все протоколы VoIP делятся на две категории: централизованные и распределенные. Централизованные модели придерживаются архитектуры клиент/сервер, а распределенные основаны на взаимодействии узлов одноранговой сети. Все технологии VoIP используют общую среду для передачи голоса в виде пакетов RTP по протоколу IP, а также поддерживают множество кодеков для сжатия данных. Разница заключается в способе передачи сигналов и месте обслуживания логики и режима вызова: в конечных точках или на центральном сервере. У обеих архитектур есть свои достоинства и недостатки. Распределенные модели хорошо масштабируются и являются более гибкими (надежными), так как у них отсутствует центральный узел, который может выйти из строя. И наоборот, централизованные модели управления вызовами отличаются более простым управлением и поддержкой традиционных дополнительных услуг (таких как конференции), но могут иметь ограничения по масштабируемости, определяемые мощностью центрального сервера. В настоящее время разрабатываются гибридные и межсетевые модели, где реализуются преимущества этих подходов.

Самая старая архитектура, H.323, и самая новая — протокол инициирования сеанса (Session Initiation Protocol — SIP), принадлежат к распределенным схемам управления вызовами VoIP. К методам централизованного управления вызовами относится протокол управления шлюзами среды передачи (Media Gateway Control Protocol — MGCP) и фирменные протоколы, такие как Skinny Station Protocol, разработанный Cisco Systems. Краткое описание каждого из этих протоколов приводится ниже.

Обзор голосовых кодеков

Технология голосовых кодеров/декодеров (кодеков) за последние несколько лет значительно продвинулась вперед благодаря достижениям в области архитектуры построения цифровых систем обработки сигналов (Digital Signal Processor — DSP),

а также исследованиям в области распознавания человеческой речи. Новые кодеки не просто выполняют аналого-цифровое преобразование. В них применяются сложные прогнозирующие модели для анализа входного голосового сигнала и последующей передачи голоса с использованием минимальной полосы пропускания. В этом разделе будет приведено несколько примеров голосовых кодеков и используемой ими полосы пропускания. Во всех случаях речь передается RTP-пакетами по протоколу IP.

Простая импульсно-кодовая модуляция голоса (Pulse Code Modulated — PCM) описывается стандартом ITU-T G.711. Он допускает две основные разновидности PCM со скоростью 64 Кбит/сек: по mu-закону и по A-закону. В обоих этих методах для достижения 12-13-битового линейного качества PCM на 8 битах используется логарифмическое сжатие. Однако они отличаются менее значительными особенностями сжатия (mu-закон имеет небольшое преимущество при низкоуровневом соотношении "сигнал-шум"). Исторически сложилось так, что использование указанных методов соответствовало географическим границам: в Северной Америке используют модуляцию по mu-закону, а в Европе — по A-закону. Преобразование mu-закона сжатия в A-закон выполняет страна, использующая модуляцию по mu-закону. При поиске неисправностей в системах PCM несовпадение видов модуляции приводит к неестественно звучащей, но, тем не менее, внятной речи.

Другим часто применяемым методом сжатия является адаптивная дифференциальная импульсно-кодовая модуляция (Adaptive Differential Pulse Code Modulation — ADPCM). Типичным случаем использования ADPCM является кодирование по стандарту ITU-T G.726 с использованием 4-битовых квантов, обеспечивающих скорость передачи 32 Кбит/сек. В отличие от PCM, 4 бита кодируют не амплитуду речи, а только разницу в амплитуде и скорость изменения амплитуды, используя довольно примитивное линейное прогнозирование.

PCM и ADPCM являются примерами кодеков *по форме сигнала*, в методах сжатия которых применяются избыточные характеристики формы сигнала. В новых способах сжатия, разработанных за последние 10-15 лет, используется, кроме того, знание исходных особенностей формирования речи. В таких методах применяются способы обработки сигналов, которые сжимают речь, посылая только упрощенную параметрическую информацию об исходной форме звукового сигнала и голосового тракта. Для передачи этой информации требуется меньшая полоса пропускания. Эти способы могут быть объединены в общую группу кодеков *по источнику*. В нее входят такие разновидности, как линейное прогнозируемое кодирование (Linear Predictive Coding — LPC), линейный прогноз, возбуждаемый кодовым словом (Code Excited Linear Prediction — CELP) и многоимпульсное многоуровневое квантование (Multipulse, Multilevel Quantization — MP-MLQ).

Перечисленные выше виды кодеков можно разделить на подкатегории. Например, к методам CELP можно отнести версию с малой задержкой, называемую LD-CELP (low delay CELP), а также более сложные методы моделирования голосового тракта с алгебраическими преобразованиями сопряженных структур. Такие кодеки обозначаются как CSA-CELP (conjugate structure algebraic CELP). Данный список можно продолжать до бесконечности, но сетевым разработчикам важно знать только области применения этих подходов в сетях и приложениях.

Сложные предсказывающие кодеки опираются на математическую модель человеческого голосового аппарата и вместо того, чтобы отправлять сжатую речь, посылают ее математическое представление, позволяющее получателю ее сгенерировать. Однако для отладки такого оборудования требуются серьезные исследования. Например, некоторые из первых кодеков хорошо воспроизводили голоса своих разработчиков и активно

внедрялись — до тех пор, пока не обнаружилось, что они не очень хорошо воспроизводят женскую речь и азиатские диалекты. Тогда в конструкцию этих кодеков были внесены изменения с учетом более широкого диапазона типов человеческого голоса.

Союз ITU стандартизировал наиболее распространенные методы в телефонии кодирования и пакетирования речи, приняв приведенные ниже стандарты.

- **G.711.** Кратко описанный ранее PCM-метод голосового кодирования со скоростью передачи 64 Кбит/сек. Кодирование голоса по стандарту G.711 всегда обеспечивает правильный формат для передачи голоса в цифровом виде по открытой телефонной сети или через мини-АТС.
- **G.726.** Метод кодирования ADPCM со скоростями передачи 40, 32, 24 и 16 Кбит/сек. Речь, кодированная методом ADPCM, также может передаваться между сетями с пакетной передачей речи, открытыми телефонными сетями и сетями на основе мини-АТС при условии, что последние поддерживают ADPCM.
- **G.728.** Разновидность CELP-сжатия голоса с малой задержкой и скоростью передачи 16 Кбит/сек. Речь, кодированная методом CELP, должна преобразовываться в формат открытых телефонных сетей для передачи по ним.
- **G.729.** Метод CELP-сжатия, позволяющий кодировать речь в потоки со скоростью передачи 8 Кбит/сек. Две разновидности этого стандарта (G.729 и G.729 Annex A) значительно различаются по сложности вычислений, но оба обеспечивают примерно такое же хорошее качество речи, как и метод ADPCM со скоростью 32 Кбит/сек.
- **G.723.1.** Метод, который может быть использован для сжатия голоса и других аудиокомпонентов мультимедийных сообщений с очень низкой битовой скоростью передачи. Являясь частью общего семейства стандартов H.324, этот кодер имеет две битовые скорости передачи: 5,3 и 6,3 Кбит/сек. Более высокая скорость основана на технологии MP-MLQ и обеспечивает более высокое качество; более низкая основана на методе CELP и обеспечивает хорошее качество, а также предоставляет системным разработчикам дополнительную гибкость.

Поскольку кодеки все больше полагаются на субъективно настраиваемые методики сжатия, стандартные объективные показатели качества, такие как суммарное искажение гармоник и отношение сигнал/шум, имеют меньшее отношение к качественным показателям кодека. Распространенным тестом для определения эффективности голосовых кодеков является средняя экспертная оценка (Mean Opinion Score — MOS). Из-за того, что качество голоса и звука обычно оценивается субъективно и зависит от слушателя, в этом методе важен широкий диапазон слушателей и образцов речи. Тесты MOS проводятся на группе слушателей, которые дают голосовым образцам оценки от 1 (плохо) до 5 (отлично). Затем оценки усредняются и получается средняя экспертная оценка. MOS-тестирование также применяется для сравнения качества работы одного и того же кодека в различных условиях, таких как уровни фоновых шумов, способы кодирования и декодирования и т.п. Впоследствии эти данные могут использоваться для сравнения с другими кодеками.

В табл. 19.1 приведены оценки по методу MOS для нескольких кодеков ITU-T, а также показана связь между несколькими низкоскоростными кодеками и стандартом PCM.

Таблица 19.1. Относительная сложность обработки и средние экспертные оценки распространенных голосовых кодеков

Метод сжатия	Битовая скорость, Кбит/с	Сложность обработки[1], млн. Операций/с	Размер фрейма	Оценка MOS
G.711 PCM	64	0,34	0,125	4,1
G.726 ADPCM	32	14	0,125	3,85
G.728 LD-CELP	16	33	0,625	3,61
G.729 CS-ACELP	8	20	10	3,92
Кодировки G.729 x2	8	20	10	3,27
Кодировки G.729 x3	8	20	10	2,68
G.729a CS-ACELP	8	10,5	10	3,7
G.723.1 MPMLQ	6,3	16	30	3,9
G.723.1 ACELP	5,3	16	30	3,65

[1] Для Texas Instruments DSP 54x.

В этой таблице приведена информация, полезная для сравнения различных реализаций распространенных голосовых кодеков. Относительная полоса пропускания и сложность обработки, выраженная в миллионах операций в секунду (Millions of Instructions Per Second — MIPS) определяют области применения различных кодеков. В целом, высшая средняя экспертная оценка соответствует более сложным кодекам или большей полосе пропускания.

Ограничения при разработке сетей VoIP

После сжатия и преобразования в цифровой вид голосовые данные помещаются в поток протокола реального времени (Real Time Protocol — RTP) для передачи по сети IP. При реализации VoIP сетевые разработчики должны учитывать полосу пропускания и задержку. Требования к полосе пропускания являются критичными и определяются не только выбранным кодеком, но и дополнительной нагрузкой на сеть, вызываемой IP-заголовками и другими факторами. Особенно важное значение полоса пропускания приобретает при соединении по дорогостоящим распределенным сетям. На общую задержку влияет задержка распространения (ограничение по скорости света), последовательная задержка (обычно вызывается буферизацией в промежуточных устройствах по пути следования) и задержка пакетирования.

Требования к полосе пропускания

На полосу пропускания при передаче голоса по протоколу IP влияет множество факторов. Прежде всего, как уже отмечалось, скорость передачи используемого кодека может изменяться в широком диапазоне — от менее чем 3-4 Кбит/с до более чем 64 Кбит/с. Дополнительное время затрачивается на передачу заголовков 2-го (Ethernet) и 3-го (IP) уровней. Обычно голосовые пакеты очень малы и зачастую содержат не более 20 байтов информации. Отсюда очевидно, что такие служебные сигналы могут быстро превысить ограничения по полосе пропускания.

У системных разработчиков есть несколько средств для уменьшения последствий этой проблемы. Прежде всего, в источнике применяется обнаружение голосовой активности (Voice Activity Detection — VAD) для регулирования потока пакетов. Данный метод позволяет остановить передачу, если уровень аналогового голосового сигнала упадет ниже пороговой величины. В результате требования к полосе пропускания снижаются примерно в два раза, так как большинство разговоров наполовину состоит из молчания — в то время, когда говорит собеседник (за исключением ожесточенных споров...).

Однако это решение может привести к возникновению нескольких проблем. Прежде всего, во избежание потерь, необходимо тщательно настроить время включения/выключения. В Cisco такая проблема решается путем постоянного квантования и кодирования, а затем отбрасывания пакета в последний момент, если голосовая энергия падает ниже определенного минимума в течение отведенного времени. На самом деле большинство пустых голосовых пакетов ставятся в очередь и готовятся к передаче и при необходимости будут предшествовать первым фразам. Другой проблемой VAD является отсутствие шума на приемнике. Пользователи первых подобных систем часто жаловались на то, что из-за отсутствия шума кажется, будто связь оборвалась посреди разговора. Этот факт лишь подтверждает, что VAD работает, но явно неудобен для пользователя.

Cisco и другие производители решили вышеуказанную проблему путем введения на приемнике "*комфортного шума*". Когда буфер приемника пуст (что означает отсутствие принимаемых пакетов), система генерирует низкоуровневый сигнал "розового" или "белого" шума, чтобы убедить слушателей в наличии соединения. Более совершенные системы фактически извлекают фоновый шум окружающей среды на противоположном конце и воспроизводят его в периоды молчания.

Другим средством, часто используемым сетевыми разработчиками, является сжатие заголовков RTP. В этих заголовках много избыточной информации, повторяющейся в других местах потока. Маршрутизаторы Cisco сжимают заголовки протокола RTP от узла к узлу, что значительно уменьшает требуемую полосу пропускания.

Конечный результат таких действий показан в табл. 19.2. В ней содержатся требования к относительной полосе пропускания для различных реализаций кодеков с учетом дополнительных расходов, связанных с обычными сетевыми транспортными уровнями.

Задержка

Сетевые разработчики, планирующие внедрение технологии VoIP, должны учитывать допустимые задержки, которые определяются требованиями к качеству системы, выдвигаемыми пользователями. Обычно суммарная сквозная задержка не должна превышать 150 мс.

Задержка распространения сигнала определяется средой передачи. Скорость света в вакууме составляет 186000 миль в секунду, а скорость перемещения электронов в меди — примерно 100000 миль в секунду. Волоконно-оптический кабель длиной в пол-экватора (13000 миль) теоретически создает одностороннюю задержку около 70 мс. Хотя для человеческого уха такая задержка почти незаметна, но вместе с задержками, вызванными передачей заголовков, задержки распространения могут привести к заметному ухудшению качества речи. Пользователи, разговаривающие по спутниковой телефонной связи, ощущают задержку, достигающую в некоторых случаях 1 с, в то время как обычно приемлемая задержка составляет около 250 мс. Задержки, превышающие 250 мс, нарушают естественный темп разговора, как если бы разговаривающие перебивали друг друга.

Таблица 19.2. Требования к полосе пропускания для VoIP

Метод сжатия	Полоса пропускания голосового канала, Кбит/с	Оценка MOS	Задержка кодирования, мс	Размер фрейма, байт	Дополнительная нагрузка Cisco, байт	Скорость, пакетов в с	Размер заголовков IP/UDP/ /RTP, байт	Размер заголовка CRTP, байт	L2	Размер заголовка уровня 2, байт	Ширина общей полосы пропускания, Кбит/с, без VAD	Ширина общей полосы пропускания, Кбит/с, с VAD
G.729	8	3,9	15	10	20	50	40		Ether	14	29,6	14,8
G.729	8	3,9	15	10	20	50		2	Ether	14	14,4	7,2
G.729	8	3,9	15	10	20	50	40		PPP	6	26,4	13,2
G.729	8	3,9	15	10	20	50		2	PPP	6	11,2	5,6
G.729	8	3,9	15	10	20	50	40		FR	4	25,6	12,8
G.729	8	3,9	15	10	20	50		2	FR	4	10,4	5,2
G.729	8	3,9	15	10	20	50	40		ATM	2 яч.	42,4	21,2
G.729	8	3,9	15	10	20	50		2	ATM	1 яч.	21,2	10,6
G.711	64	4,1	1,5	160	160	50	40		Ether	14	85,6	42,8
G.711	64	4,1	1,5	160	160	50		2	Ether	14	70,4	35,2
G.711	64	4,1	1,5	160	160	50	40		PPP	6	82,4	41,2
G.711	64	4,1	1,5	160	160	50		2	PPP	6	67,2	33,6
G.711	64	4,1	1,5	160	160	50	40		FR	4	81,6	40,8
G.711	64	4,1	1,5	160	160	50		2	FR	4	66,4	33,2
G.711	64	4,1	1,5	160	160	50	40		ATM	5 яч.	106,0	53,0
G.711	64	4,1	1,5	160	160	50		2	ATM	4 яч.	84,8	42,4

Окончание табл. 19.2

Метод сжатия	Полоса пропускания голосового канала, Кбит/с	Оценка MOS	Задержка кодирования, мс	Размер фрейма, байт	Дополнительная нагрузка Cisco, байт	Скорость, пакетов в с	Размер заголовков IP/UDP/RTP, байт	Размер заголовка CRTP, байт	L2	Размер заголовка уровня 2, байт	Ширина общей полосы пропускания, Кбит/с, без VAD	Ширина общей полосы пропускания, Кбит/с, с VAD
G.729	8	3,9	15	10	30	33	40		PPP	6	20,3	10,1
G.729	8	3,9	15	10	30	33		2	PPP	6	10,1	5,1
G.729	8	3,9	15	10	30	33	40		FR	4	19,7	9,9
G.729	8	3,9	15	10	30	33		2	FR	4	9,6	4,8
G.729	8	3,9	15	10	30	33	40		ATM	2 яч.	28,3	14,1
G.729	8	3,9	15	10	30	33		2	ATM	1 яч.	14,1	7,1
G.723.1	6,3	3,9	37,5	30	30	26	40		PPP	6	16,0	8,0
G.723.1	6,3	3,9	37,5	30	30	26		2	PPP	6	8,0	4,0
G.723.1	6,3	3,9	37,5	30	30	26	40		FR	4	15,5	7,8
G.723.1	6,3	3,9	37,5	30	30	26		2	FR	4	7,6	3,8
G.723.1	6,3	3,9	37,5	30	30	26	40		ATM	2 яч.	22,3	11,1
G.723.1	6,3	3,9	37,5	30	30	26		2	ATM	1 яч.	11,1	5,6
G.723.1	5,3	3,65	37,5	30	30	22	40		PPP	6	13,4	6,7
G.723.1	5,3	3,65	37,5	30	30	22		2	PPP	6	6,7	3,4
G.723.1	5,3	3,65	37,5	30	30	22	40		FR	4	13,1	6,5
G.723.1	5,3	3,65	37,5	30	30	22		2	FR	4	6,4	3,2
G.723.1	5,3	3,65	37,5	30	30	22	40		ATM	2 яч.	18,7	9,4
G.723.1	5,3	3,65	37,5	30	30	22		2	ATM	1 яч.	9,4	4,7

Задержки, вызванные передачей заголовков, могут влиять на традиционные телефонные сети с коммутацией каналов, но настоящие проблемы они вызывают в среде с пакетной передачей — из-за буферизации пакетов. Необходимо рассчитать задержку, чтобы определить, не превышает ли она порога в 150–200 мс.

В G.729 имеется алгоритмическая задержка на прогнозирование, составляющая примерно 20 мс. Обычно в продуктах для передачи голоса по IP-протоколу DSP генерируют фрейм каждые 10 мс. Затем эти голосовые фреймы помещаются в пакет (по два); таким образом, задержка пакета составляет 20 мс.

В сетях с пакетной передачей есть и другие причины для задержек: время помещения текущего пакета в выходную очередь и задержка в самой очереди. В Cisco IOS проблема перемещения и определения адреса назначения пакета решена достаточно хорошо. (Данный факт необходимо отметить потому, что в иных решениях на основе пакетной передачи — как на основе ПК, так и других — это сделано не столь удачно.) Иной причиной задержки является фактическая задержка в выходной очереди. Ее следует по возможности удерживать в пределах 10 мс при помощи любых методов управления очередью, оптимальных для данной сети.

В табл. 19.3 приводятся величины задержек, вносимые разными кодеками.

Таблица 19.3. Задержки, вносимые различными кодеками

Метод сжатия	Битовая скорость, Кбит/с	Задержка сжатия, мс
G.711 PCM	64	0,75
G.726 ADPCM	32	1
G.728 LD-CELP	16	3–5
G.729 CS-ACELP	8	10
G.729a CS-ACELP	8	10
G.723.1 MPMLQ	6,3	30
G.723.1 ACELP	5,3	30

Кроме описанных выше стационарных задержек, приложения VoIP чувствительны к изменениям задержки. В отличие от коммутируемых сетей, в сетях с пакетной передачей сквозная задержка может изменяться в широких пределах, в зависимости от загрузки сети. Кратковременные отклонения задержки называют *дребезжанием (jitter)*, который определяется как разница между ожидаемым и реальным временем получения пакета. Голосовые устройства должны компенсировать дребезг путем настройки буфера воспроизведения на сглаживание речи, предотвращение разрывов в голосовом потоке. Это увеличивает суммарную задержку (и сложность) системы. Такой приемный буфер может иметь фиксированную или настраиваемую длину, как в некоторых современных устройствах производства Cisco Systems.

Обратите внимание, что дребезг является главным препятствием для использования VoIP в Internet. Типичный вызов VoIP по Internet пройдет через множество транспортных систем, с широким диапазоном времени ожидания и различными способами управления QoS. В результате использование VoIP для передачи по Internet приводит к плохому качеству и часто отпугивает производителей устройств VoIP. Тем не менее, существует множество программных продуктов, предоставляющих возможность бесплатной передачи голоса по Internet. Общей особенностью этих систем являются очень большие приемные буферы, которые приводят к задержкам значительно

более продолжительным, чем 1 с. Бесплатная передача голоса привлекательна, но для бизнесменов из-за плохого качества она не подходит. Впрочем, для бытовых разговоров многие находят такие системы вполне пригодными — особенно учитывая стоимость международных телефонных переговоров.

В будущем, по мере улучшения провайдерами услуг Internet, передача голоса по сети приобретет большую популярность. На самом деле, многие аналитики предсказывают, что в один прекрасный день передача голоса станет бесплатной и будет входить в стандартный пакет услуг, предоставляемых вместе с доступом к Internet.

Качество обслуживания для VoIP

Как следует из сказанного выше, на качество передаваемого голоса сильно влияет время ожидания и дребезг в сетях с пакетной передачей. Поэтому сетевым разработчикам следует применять политики QoS. Кроме отделения передаваемого голоса от цифровых данных, они предоставляет дополнительные преимущества по обеспечению полосы пропускания для важных данных приложений, несмотря на обилие голосовых вызовов.

Элементами хорошего стиля разработки QoS является управление потерями пакетов, задержками, дребезгом и эффективное распределение полосы пропускания. Для достижения этих целей применяются следующие средства.

- **Политики**. Обычное ограничение частоты передачи пакетов, часто путем простого отбрасывания пакетов, не удовлетворяющих условиям пропускной способности различных элементов сети. Политики могут применяться как на входе, так и на выходе устройства. Примерами применения политик является раннее случайное обнаружение (Random Early Detection — RED) и взвешенное раннее случайное обнаружение (Weighted RED — WRED). С помощью этих методик можно, при необходимости, идентифицировать пакеты, подлежащие отбрасыванию в первую очередь.
- **Формирование потоков данных**. Буферизация и выравнивание входящих и исходящих информационных потоков на пакетной основе. В отличие от политик, целью выравнивания потоков данных является предотвращение отбрасывания пакетов; однако, поскольку пакеты помещаются в буфер для последующей передачи, при этом увеличивается время ожидания и дребезг.
- **Управление правом вызова**. Отклонение запросов приложений на полосу пропускания сети. В случае VoIP можно привести пример использования протокола резервирования ресурсов (Resource Reservation Protocol — RSVP) для резервирования полосы пропускания перед завершением вызова. Аналогичным образом для управления частями полосы пропускания, доступными для каждого вызова, может использоваться драйвер управления пропуском через шлюз (gatekeeper) H.323.
- **Очереди и расписание**. Применяются наряду с буферизацией для определения приоритета передаваемых пакетов. Организация отдельных очередей для голоса и данных, например, позволяет передавать чувствительные к задержкам голосовые пакеты раньше, чем пакеты данных. В качестве примеров для VoIP, в частности, можно привести взвешенную равноправную очередность и приоритетные очереди протокола RTP стека IP.

- **Присоединение тегов и маркировка**. Различные способы идентификации пакетов для специальной обработки. Пакеты VoIP, к примеру, могут идентифицироваться по формату RTP, предшествующим битам IP (биты ToS) и т.п. Присоединение тегов к пакетам важно также для сохранения QoS при переходе из одной сети в другую. Например, коммутация по тегам сохраняет теги протокола IP при пересечении пакетами VoIP сети ATM.
- **Фрагментация**. Под фрагментацией понимается возможность некоторых сетевых устройств делить большие пакеты на меньшие перед прохождением участков с узкой полосой пропускания. Это важно во избежание "замораживания" голосовых пакетов, пока не пройдут большие пакеты данных. Благодаря фрагментации можно вставить меньшие голосовые пакеты в промежутки между большими пакетами данных. Затем маршрутизатор снова собирает большие пакеты, поэтому данные приложения восстанавливаются в исходном виде.

Обзор стандарта H.323

Стандарт H.323 является производным от стандарта видеоконференций H.320, однако он предполагает объединение компонентов конференции не по сети ISDN, а по локальной сети, поэтому он не поддерживает QoS. При использовании H.323 для поддержки приложений VoIP вызовы рассматриваются как аудиокомпоненты видеоконференций.

Стандартизированные видеоконференции в целом описываются рекомендациями "серии H" Международного союза телекоммуникаций (International Telecommunications Union — ITU). В их состав входят H.320 (протокол ISDN), H.323 (протокол LAN) и H.324 (протокол для обычной телефонной сети). Эти стандарты определяют способ передачи аудио-, видео- и цифровой информации в режиме реального времени для различных топологий. Совместимость стандартов обеспечивает общность функций и функциональную совместимость между сетевыми мультимедийными компонентами разных производителей.

Стандарт H.323, утвержденный в 1996 году, состоит из следующих компонентов.

- **H.225.** Определяет сообщения для управления вызовами, в том числе передачу сигналов, регистрацию и полномочия, а также пакетирование и синхронизацию информационных потоков разных форматов.
- **H.245.** Определяет сообщения открытия и закрытия каналов для потоков разных форматов, другие команды, запросы и признаки.
- **H.261.** Видеокодек для аудиовизуальных служб со скоростью передачи P×64 Кбит/с.
- **H.263.** Новый видеокодек для передачи видео по телефонной сети.
- **G.711.** Аудиокодек, 3,1 кГц; 48, 56 и 64 Кбит/с (для обычных телефонных каналов).
- **G.722.** Аудиокодек, 7 кГц; 48, 56 и 64 Кбит/с; утвержденный стандарт.
- **G.728.** Аудиокодек, 3,1 кГц; 16 Кбит/с.
- **G.723.** Аудиокодек для 5,3 и 6,3 Кбит/с.
- **G.729.** Аудиокодек (G.729a — упрощенный вариант).

Ниже описаны устройства стандарта H.323.

- **Термиал.** По стандарту H.323, терминал представляет собой конечную точку локальной сети, обеспечивающую двусторонний обмен данными в реальном времени с другим терминалом, шлюзом или многопортовым управляющим модулем H.323. Этот обмен данными заключается в обмене управляющими, индикаторными и аудиосообщениями, цветными видеофильмами и данными между двумя терминалами. Терминал может ограничиваться только приемом и передачей речи, голоса и данных, голоса и видео или речи, данных и видео.
- **Шлюз.** По стандарту H.323, шлюз (gateway — GW) представляет собой конечную точку локальной сети, которая обеспечивает двусторонний обмен данными в реальном времени между терминалами H.323 локальной сети и другими ITU-терминалами распределенной сети либо иным шлюзом H.323. Под другими ITU-терминалами подразумеваются терминалы, соответствующие рекомендациям H.310 (H.320 для B-ISDN), H.320 (ISDN), H.321 (ATM), H.322 (GQOS-LAN), H.324 (GSTN), H.324M (мобильная связь) и V.70 (DSVD).
- **Прокси-система.** Специальный тип шлюза, который, в сущности, ретранслирует один сеанс H.323 на другой такой же сеанс. Прокси-системы Cisco являются ключевым элементом инфраструктуры конференций, которые обеспечивают QoS, формируют потоки данных и управляют политиками информационного потока H.323.
- **Драйвер шлюза (gatekeeper).** Дополнительный элемент системы H.323. Предоставляет услуги по управлению вызовами с конечных точек H.323. Драйверов шлюза может быть несколько, причем способ их соединения не определен. Логически драйверы шлюза отделены от конечных точек, но физически они могут встраиваться в терминалы, многопортовые управляющие модули, шлюзы, многопортовые контроллеры, а также другие устройства локальной сети, не обязательно соответствующие H.323.
- **Многопортовый управляющий модуль** (Mutipoint Control Unit — MCU). Конечная точка локальной сети, позволяющая трем и более терминалам и шлюзам участвовать в многосторонней конференции. Кроме того, он может соединять два терминала для проведения конференции в режиме "точка-точка", которая позже может быть развернута в многостороннюю конференцию. Обычно MCU работает по стандарту H.231, но аудиопроцессор не является обязательным. MCU состоит из двух частей: обязательный многопортовый контроллер и дополнительные многопортовые процессоры. В простейшем случае MCU может состоять из одного контроллера, без процессоров.
- **Многопортовый контроллер** (Multipoint Controller — MC). Объект H.323 в локальной сети, предназначенный для управления тремя и более терминалами, участвующими в многосторонней конференции. Кроме того, он может соединять два терминала для проведения конференции по схеме "точка-точка", которая позже может быть развернута в многостороннюю конференцию. MC обеспечивает возможность согласования со всеми терминалами для достижения общего уровня связи. Он может также выполнять такие функции в конференции, как назначение управляющего рассылкой многоадресного видео. MC не выполняет смешивания и коммутации аудио- и видеосигналов или данных.
- **Многопортовый процессор** (Multipoint Processor — MP). Объект H.323 в локальной сети, обеспечивающий централизованную обработку аудио- и видеопотоков, а

также потоков данных в многосторонней конференции. MP обеспечивает смешивание, коммутацию и другую обработку потоков разных форматов под управлением MC. MP может обрабатывать один или несколько потоков разных форматов, в зависимости от типа конференции.

- **Конференция по схеме "точка-точка".** Это конференция между двумя терминалами H.323 или одним терминалом H.323 и одним терминалом SCN через шлюз.
- **SCN.** Открытые или частные коммутируемые телекоммуникационные сети, такие как GSTN, N-ISDN или B-ISDN.

Стандарт H.323 предусматривает достаточно интеллектуальные конечные устройства для обслуживания режима собственного вызова. В простейшем случае H.323 является системой передачи сигналов между узлами одноранговой сети. Конечные точки могут вызывать одна другую непосредственно, используя предлагаемые стандартом процедуры, если им известны IP-адреса друг друга. Сигнальные сообщения начальной настройки вызова соответствуют традиционной модели ISDN Q.931, использующей передачу пакетов формата ASN.1 по протоколу TCP. Поэтому для обеспечения QoS протокол передачи сигналов опирается на повторные передачи TCP. После настройки вызова обе конечные точки обмениваются характеристиками для согласования стандарта аудиокодека, который будет использоваться, и наконец выбирают номер порта RTP, который будет применяться самой средой передачи речи. Обратите внимание, поскольку номера портов RTP назначаются конечными точками динамически в широком диапазоне, при работе через брандмауэры, если только они сами не выполняют настройку вызова, возможны некоторые затруднения.

Поток вызовов H.323 и взаимодействие протоколов

Обмен данными происходит поэтапно, как показано на рис. 19.5.

Как видно из рис. 19.5, протокол H.323 обладает высоким уровнем гибкости и надежности, однако это достигается за счет определенного снижения эффективности.

Кратко о протоколе MGCP

Протокол MGCP (Media Gateway Control Protocol) представляет собой относительно новый набор клиент-серверных протоколов обмена сигналами VoIP, разработанный в ответ на требования устойчивого централизованного управления сравнительно малоинтеллектуальными конечными устройствами. Такая возможность значительно расширяет применимость системы VoIP, делая ее более простой для разработки, настройки и управления благодаря тому, что все главные изменения осуществляются на сервере.

Когда писалась эта книга, протокол MGCP был только в проекте IETF. Может быть, IETF его так окончательно и не утвердит. Возможно, окончательным решением станет более совершенный производный протокол, получивший название MEGACO. Тем не менее, требования рынка побудили нескольких производителей (включая Cisco Systems) объявить о поддержке MGCP в достандартном виде. Что, в свою очередь, привело к появлению неофициального стандарта с функциональной совместимостью для сетей различных производителей. Вообще-то, это положительно сказалось на рынке, так как подтолкнуло разных производителей выпустить продукты, в которых потребители действительно нуждаются.

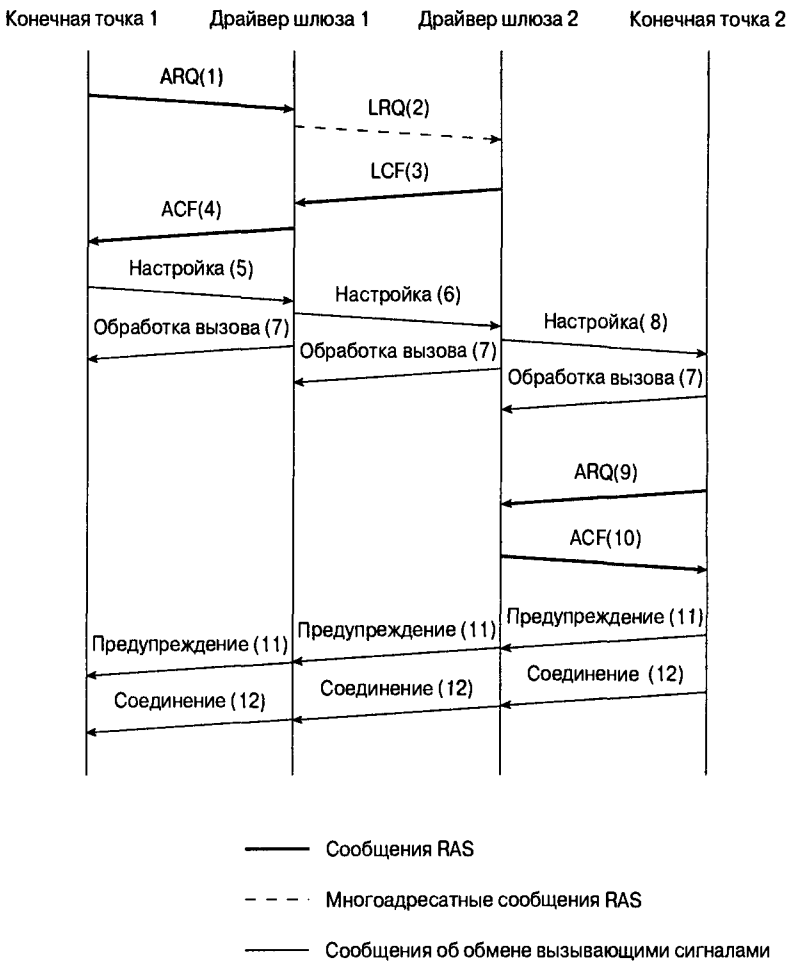


Рис. 19.5. Поток вызовов между устройствами H.323

Подобно большинству протоколов, MGCP имеет интересную историю. Первоначально это был клиент-серверный протокол, названный Simple Gateway Control Protocol и предложенный совместно Bellcore (сейчас — Telcordia) и Cisco Systems. Это был первый шаг на пути к действительно универсальному клиенту. В то же время Cisco Systems и другие производители разрабатывали другой клиент-серверный протокол 3-го уровня, названный IPDC (Internet Protocol Device Control). Протокол IPDC задумывался как более общая система управления для различных мультимедийных IP-устройств. Через некоторое время эти два протокола были объединены, в результате чего появился протокол MGCP.

Основные понятия MGCP

Как уже отмечалось, в протоколе MGCP используются простые конечные точки, называемые шлюзами среды передачи (Media Gateways — MG). Обслуживание обеспечивает интеллектуальный контроллер шлюза среды передачи (Media Gateway Controller —

MGC) или агент вызова (Call Agent — CA). Конечная точка обеспечивает интерфейс и взаимодействие между пользователями, а MGC — централизованную обработку вызова. Между MGC и MG поддерживаются отношения "ведущий/ведомый". В действительности все изменения состояния передаются на MGC в виде серии относительно простых сообщений. Затем MG выполняет простые действия по командам MGC.

Важно понимать, что состояние конечных точек MG не изменяется. Они не выполняют локальную обработку вызова. Например, в случае интерфейса типа FXS, поддерживающего аналоговую телефонную связь, когда пользователь снимает трубку, шлюз уведомляет об этом MGC, который затем инструктирует MG дать сигнал набора. Когда пользователь набирает номер (DTMF), цифры по очереди пересылаются на MGC, потому что MG "не понимает" правил набора номера. Он "не знает", когда пользователь набрал достаточное количество цифр. В известном смысле MG становится логическим расширением MGC. В случае предоставления новых услуг (например, ожидание звонка) изменениям подвергается только MGC.

Как правило, сообщения MGCP передаются между MG и MGC по протоколу IP/UDP. Любые специальные телефонные сигнальные интерфейсы (такие, как D-канал для интерфейса первичной скорости ISDN) непосредственно передаются MGC для обработки, а не остаются в MG. Это означает, что для обычных приложений необходимо поддерживать обмен данными между MG и MGC, для того, чтобы не разорвать связь.

Собственно соединение среды передачи (голосовой маршрут) обычно производится по IP/RTP, но возможно непосредственное применение VoATM и VoFrame Relay. (Фактически MGCP не предъявляет определенных требований к среде передачи.) Для защиты сигнальной информации в MGCP используется IPSec.

Преимущества MGCP

Протокол MGCP имеет определенные преимущества перед типичными реализациями H.323. Хотя протокол MGCP не был утвержден как официальный стандарт, он обеспечивает функциональную совместимость достаточно большого количества производителей, так что потребители могут свободно применять его, не рискуя замкнуться в своей сети. Он сохраняет возможности уже существующих протоколов IETF, таких как SDP, SAP, RTSP. Но самым важным, вероятно, является то, что модель централизованного управления вызовами в MGCP является гораздо более эффективной средой для создания служб, включая выписку счетов, агентов вызова, службы обмена сообщениями и т.п. В зависимости от производителя, MGC может поддерживать интерфейсы интеграции стандартной компьютерной телефонии (Computer Telephony Integration — CTI), такие как применяемый в мини-АТС интерфейс прикладного программирования (Telephony Application Programming Interface — TAPI).

Терминология протокола MGCP

В модели MGCP используются следующие определения.

- **Конечная точка.** Отдельная магистраль, порт или сервис, такой как сервер уведомлений.
- **Соединение.** То же, что и сеанс. Есть несколько режимов соединений: отправка, прием, отправка/прием, неактивный, возвратная петля и тест соединения.
- **Вызов.** Группа соединений.
- **Агент вызова.** Контроллер шлюза среды передачи (MGC).

Сообщения MGCP составляются из следующих элементов.

- **NotificationRequest** (RQNT). Инструкция шлюзу следить за специальными сообщениями.
- **Notify** (NTFY). Сообщает MGC, когда произойдет запрос.
- **CreateConnection** (CRCX). Устанавливает соединение с конечной точкой внутри шлюза.
- **ModifyConnection** (MDCX). Изменяет параметры, связанные с установленным соединением.
- **DeleteConnection.** Удаляет существующее соединение. В ответ приходит статистика вызова.
- **AuditEnpoint** (AUEP). Аудит конечной точки.
- **AuditConnection** (AUCX). Аудит соединения.
- **RestartInProgress** (RSIP). Шлюзовое уведомление MGC о перезапуске или отключении MG или конечной точки.

Особый интерес представляют уведомляющие сообщения. Шлюз среды передачи использует их, чтобы сообщить MGC об изменении состояния. Обычно это сигналы или события, несколько примеров которых приводится ниже.

- **Сигналы.** Звонок, особый звонок (от 0 до 7), тональный обратный звонок, сигнал набора, сигнал отбоя, сигнал перегрузки сети, сигнал "занято", сигнал подтверждения, сигнал ответа, сигнал ожидания вызова, сигнал предупреждения о том, что трубка снята, сигнал прерывания, сигнал продолжения, проверка связи, сигналы DTMF.
- **События.** Сигналы факса, модема, непрерывный сигнал, сообщение о непрерывности связи (как результат проверки связи), события "трубка лежит" и "трубка снята", прием номера DTMF.

Благодаря некоторым функциям, MGCP является привлекательным для разработчиков систем VoIP. Прежде всего, это обмен сообщениями на основе UDP, а не TCP, что делает его более эффективным. Централизованная модель управления обеспечивает единственную точку сбоя, поэтому шлюзы среды передачи можно спроектировать с учетом возможности переключения на резервный MGC в случае отказа основного контроллера. В результате эта модель становится такой же надежной, как и любая другая модель управления вызовом. MGCP хорошо масштабируется: его степень масштабирования обычно определяется только производительностью MGC. Когда она достигает предела, сеть можно разделить на MGC-домены. Поэтому модель управления вызовом MGCP можно расширять до миллионов конечных точек.

Протокол также надежен, так как предусматривает три варианта подтверждений для каждого запроса: успешный, неустойчивая ошибка и постоянная ошибка. Неподтвержденные запросы могут быть отправлены повторно. Для преобразования имен IP-адресов MGCP использует DNS. Это означает, что один IP-адрес может соответствовать нескольким узлам, а также что один узел может иметь несколько IP-адресов. Все эти функции также повышают гибкость протокола.

На рис. 19.6 показан типичный поток вызова MGCP.

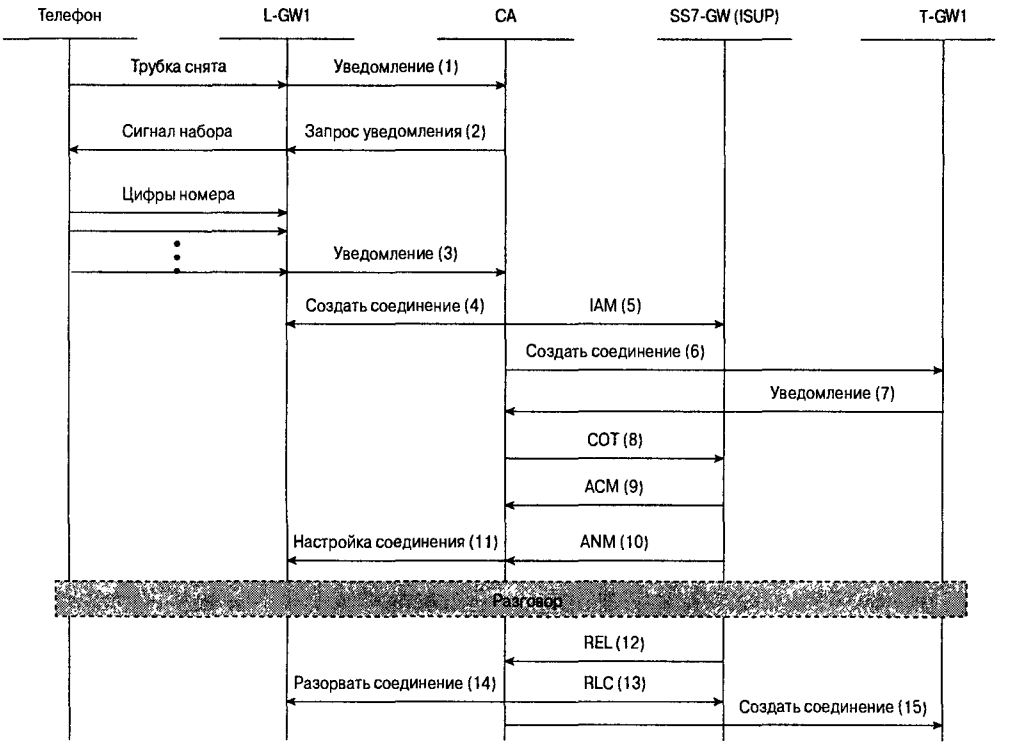


Рис. 19.6. Типичный поток вызовов протокола MGCP

Основы SIP

Протокол инициирования сеанса (Session Initiation Protocol — SIP) представляет собой один из новых протоколов для передачи сигналов в одноранговых сетях, подобных H.323. Но, в отличие от H.323, по своей сущности и целям SIP является протоколом Internet. Он описан в документации RFC 2543, выпущенной рабочей группой IETF MMUSIC в сентябре 1999 года. Многие технологи считают SIP конкурентом H.323 и дополнением к таким клиент-серверным протоколам, как MGCP. Он, вероятно, получит распространение в смешанных средах, представляющих собой комбинацию конечных точек SIP и устройств MGCP.

Протокол SIP зависит от относительно интеллектуальных конечных точек, которым необходимо незначительное взаимодействие с сервером (если вообще требуется). Каждая конечная точка имеет собственный набор сигналов как для пользователей, так и для других конечных точек. По существу, протокол SIP обеспечивает управление сеансом, а протокол MGCP — управление устройством. Это наделяет протокол SIP рядом преимуществ. Прежде всего, простая структура сообщений позволяет выполнить настройку вызова за меньшее количество шагов, чем это происходит в устройствах H.323, поэтому на аналогичном оборудовании производительность MGCP выше, чем у H.323. Затем, протокол SIP лучше масштабируется, чем H.323, так как в его основе лежит распределенная и универсальная модель вызова. Но, вероятно, основным отличием (и преимуществом) протокола SIP является тот факт, что по своей природе он является настоящим протоколом Internet.

В нем используется обмен простыми сообщениями ASCII (а не ASN.1), основанный на HTTP/1.1. Это означает, что сообщения SIP легко декодируются и корректируются, а также, что более важно, Web-приложения могут поддерживать службы SIP с минимальными изменениями. В самом деле, кроме стандарта E.164 North American Numbering Plan (NANP), протокол SIP полностью поддерживает адресацию URL (с DNS). А значит, в модели SIP адрес электронной почты пользователя и его номер телефона могут быть одинаковыми. Кроме того, это означает абстрагированность сеанса, возможность обмена данными между самыми разными конечными точками.

SIP рассчитан на поддержку некоторых или каждого из представленных ниже пяти аспектов установки и разрыва мультимедийного соединения. Каждый из этих аспектов может быть согласован в ходе сеанса SIP между двумя конечными точками:

- местонахождение пользователя;
- возможности пользователя;
- доступность пользователя;
- настройка вызова;
- обработка вызова.

Хотя по своей сущности SIP является протоколом для одноранговых сетей, он состоит из логических клиентов и серверов, обычно расположенных в пределах конечной точки. Например, типичным клиентом SIP может быть IP-телефон, ПК или PDA; SIP состоит из клиента агента пользователя (User Agent Client — UAC) для создания SIP-запросов и сервера агента пользователя (User Agent Server — UAS) для ответа на SIP-запросы. Также поддерживаются прокси-серверы SIP, серверы переадресации SIP, серверы-регистраторы и размещения. Все эти серверы не являются обязательными, но имеют большое значение в реальных реализациях SIP.

Такие SIP-серверы описаны ниже.

- **Прокси-сервер.** Действует и как сервер, и как клиент; инициирует SIP-запросы от имени UAC.
- **Сервер переадресации** (Redirect Server — RS). Получает SIP-запрос, определяет пункт назначения — один или несколько адресов — и передает данные по этим адресам.
- **Сервер-регистратор.** Принимает запросы от UAC для регистрации текущего расположения. Обычно совмещается с сервером переадресации.
- **Сервер размещения.** Предоставляет информацию о вероятном местоположении вызываемого, обычно связываясь для этого с сервером переадресации. Совместно с сервером размещения SIP, может сосуществовать обычный сервер или служба размещения.

Сообщения SIP

Словарь запросов и ответов SIP-сообщений очень прост. Используются следующие запросы (или *методы)* протокола SIP:

- **REGISTER.** Регистрирует текущее расположение сервера.
- **INVITE.** Посылается вызывающим устройством для инициирования вызова.
- **ACK.** Посылается вызывающим устройством, чтобы узнать, принят ли вызов. Это сообщение не требует ответа.

- **BYE.** Посылается любой стороной для завершения вызова.
- **CANCEL.** Посылается для завершения несостоявшегося вызова.
- **OPTIONS.** Посылается для запроса возможностей.

Адресация SIP

Как уже отмечалось, модель адресации SIP повторяет URL. Например, типичный SIP-адрес может выглядеть следующим образом.

```
sip:"einstein" aeinstein@smartguy.com; transport=udp
```

Однако может поддерживаться и стандартная адресация E.164 путем внедрения в URL.

```
+14085553426@smartguy.com; user=phone
```

В структуре адреса указываются также такие параметры, как тип передачи и групповые адреса.

Поток вызова SIP

Как видно из рис. 19.7, настройка вызова в SIP намного проще, чем в H.323, даже с участием прокси-сервера. В противном случае, без прокси-сервера, конечные точки должны "знать" о существовании друг друга. Но настройка вызова выполняется при помощи сообщения INVITE, посылаемого непосредственно из одной конечной точки в другую.

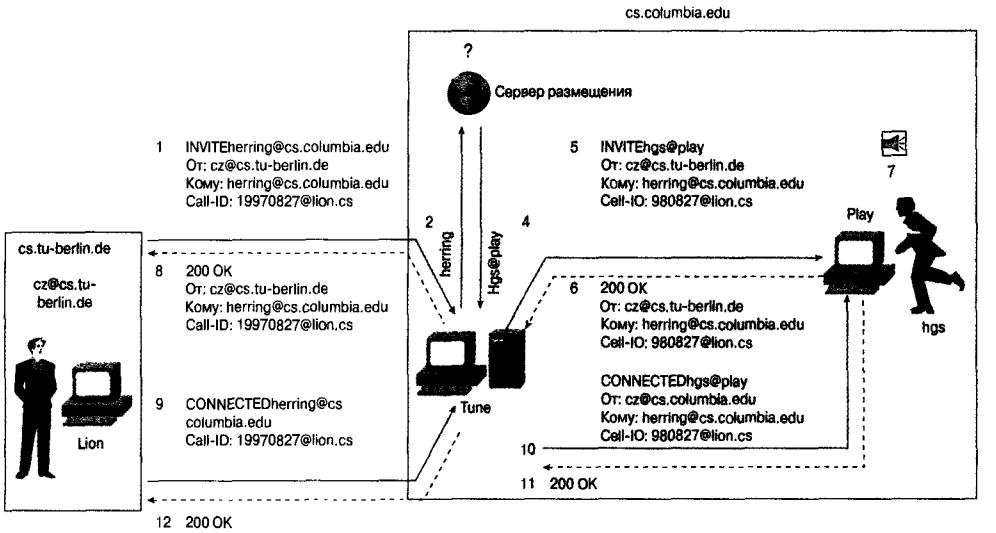


Рис. 19.7. Поток вызова для протокола SIP

Протокол управления работой пользователя

Протокол управления работой пользователя (Skinny Client Control Protocol — SCCP), иронически называемый "тонким", представляет собой фирменный протокол

сигнализации и управления корпорации Cisco, используемый для установки и ликвидации вызова, а также для управления им в среде VoIP. Он является ядром решения AVVID Cisco. Это протокол широко используется в корпоративных сетях VoIP и все чаще поддерживается другими производителями в среде провайдеров служб.

Этот простой и компактный протокол обладает богатым набором функций и реализуется вместе с протоколом Cisco IP Phones. Маршрут сигнализации использует порт 2000 протокола TCP, а маршрут передачи мультимедийных данных использует протокол UDP. Набор сообщений для управления работой клиентского приложения включает в себя три основных сферы: регистрация и управление, управление вызовом (установка, прекращение и статистика) и контроль мультимедийного потока (аудио). Первоначально этот протокол был спроектирован и реализован в технологии Cisco Call Manager, однако за прошедшее время привлек внимание многих других производителей. Call Manager или SoftSwitch управляют конечными точками, установкой прекращением и учетом вызовов, однако потоки мультимедийных данных управляются непосредственно конечными точками.

Сравнение альтернатив передачи сигналов VoIP

У различных вариантов передачи сигналов есть свои достоинства и недостатки с точки зрения системных разработчиков. Некоторые из них описаны ниже.

Первое, что следует отметить, сравнивая MGCP и H.323, — это различия в их возможностях. MGCP — простой протокол управления устройствами, а H.323 — полнофункциональный мультимедийный протокол для конференций. У H.323 уже появилась 3-я версия, а MGCP, возможно, даже не будет окончательно утвержден; это лишь неофициальный стандарт, принятый некоторыми производителями. Поэтому MGCP, хоть и обеспечивает функциональную совместимость, не является промышленным стандартом. С другой стороны, функциональной совместимости H.323 мешает его сложность.

Протокол MGCP устанавливает соединение всего за два прохода, а H.323 для этого обычно требуется семь или восемь проходов. (Примечание: в H.323v2 есть функция ускоренного запуска, позволяющая устанавливать некоторые соединения за два прохода, но такой протокол не очень широко распространен.) Управление вызовом в MGCP ненамного лучше управления устройствами, в то время как в H.323 оно унаследовано от системы сигнализации Q.931 ISDN как протокол управления передачей информации. Для MGCP эта управляющая информация передается по UDP, а для H.323 — по TCP.

Протокол SIP и H.323 являются мультимедийными протоколами полнофункциональных одноранговых систем, SIP представляет собой IETF RFC, а H.323v3 утвержден ITU. Как уже отмечалось, данные протоколы функционально совместимы. SIP эффективнее, чем H.323, так как устанавливает некоторые вызовы всего за один проход. Кроме того, SIP использует существующие протоколы Internet, а для H.323 продолжают появляться новые элементы для приспособления к модели Q.931 ISDN.

Сравнение протоколов SIP с MGCP подобно сравнению протоколов H.323 с MGCP, потому что SIP (как и H.323) является протоколом управления средой передачи, а MGCP — протоколом управления устройствами. Поэтому проявляются те же отличия, что и между клиент-серверными протоколами и одноранговыми протоколами. Основное отличие состоит в том, что одноранговые протоколы, такие как H.323 и SIP, обычно лучше масштабируются, а клиент-серверные протоколы наподобие MGCP проще для разработки и обслуживания.

Развитие систем интегрированной передачи голоса и данных

Первые продукты для интегрированной передачи голоса и данных были предназначены для того, чтобы избежать оплаты междугородных телефонных переговоров путем соединения телефонных сетей через инфраструктуру. Эти продукты, как правило, встраивались в маршрутизатор или другое компьютерное устройство и обеспечивали прямое соединение "точка-точка", используя обычные аналоговые магистральные порты. По мере их совершенствования появилась поддержка разных типов интерфейсов, в том числе цифровых, E&M и других.

Затем, с расширением возможностей, появилась поддержка аналоговых телефонных аппаратов. Данное приложение первоначально предназначалось для резервных расширений мини-АТС по частным автоматическим каналам прямого вызова (Private Line Automatic Ringdown — PLAR), но позже в таких шлюзовых устройствах появилось распознавание DTMF и поддержка основных вариантов автоматического набора. В конце концов это привело к тому, что сетевые устройства WAN стали обеспечивать не только передачу, но и транзитную коммутацию для подключенных к ним мини-АТС.

Со временем логику корпоративных вызовов стали переносить на устройства распределенной компьютерной сети. Мини-АТС, подключенным к WAN, оставалось только передавать межузловые вызовы шлюзу WAN, не заботясь о дальнейших подробностях вычисления маршрута. Варианты автоматического вызова, предоставляемые такими шлюзами, как маршрутизаторы Cisco Systems с интегрированной передачей речи, обеспечивали магистральную связь между многими узлами.

Данная модель работала очень хорошо, особенно для небольших сетей, размером до 10 узлов. Однако по мере появления все более крупных систем с гораздо большим количеством узлов, их стало трудно администрировать. Каждый раз, когда добавлялся новый узел или изменялась схема связи, сетевым инженерам приходилось вручную регистрироваться на каждом маршрутизаторе в сети и вносить в схему связи соответствующие изменения. Это был громоздкий процесс, порождавший ошибки. В конце концов это привело к появлению утилит, облегчающих такую работу. Например, CVM (Cisco Voice Manager) имеет графический интерфейс для настройки и управления схемой связи, который позволяет сетевым инженерам управлять сотнями голосовых шлюзов.

Эти решения вполне соответствовали требованиям многих приложений, но дальнейшее увеличение масштабов сетей вызвало появление систем с сотнями и даже тысячами узлов. Крупные предприятия и провайдеры, оценивая технологию, обнаружили две основные проблемы масштабирования — это управление полномочиями соединения (Connection Admission Control — CAC) и централизация схемы связи.

По мере роста объемов передачи голосовых данных повысилось значение управления полномочиями соединения. Стало очевидным, что даже если один шлюз "видит" другой шлюз в логически плоской связной сети, то он не всегда в состоянии выполнить вызов. Необходимо было некое центральное управляющее средство, выполняющего функции дорожного регулировщика, регламентирующего количество вызовов между основными узлами. Вызовы, поступившие после того, как было превышено их предельное количество, должны отбрасываться или, если нужно, направляться по другим маршрутам.

Схемы связи тоже стали слишком громоздкими для администрирования малыми сетевыми элементами. Плоская связная топология, в сущности, привела к необходимости хра-

нить в каждом узле информацию схемы связи со всеми узлами. Ограниченность ресурсов памяти и процессоров скоро стала тормозить дальнейший рост.

Решением указанных двух проблем стало введение централизованного управления вызовами. Для передачи голоса по Frame Relay и ATM были внедрены виртуальные коммутирующие системы контроллерного типа, позволяющие централизировать логику и информацию о вызове. В VoIP для этого появился драйвер шлюза H.323. В Cisco Systems, например, был разработан драйвер шлюза Multimedia Conferencing Manager (MCM) H.323 для поддержки как голосовых сетей, так и видеоконференций, для которых он, в сущности, и был создан.

Необходимо обратить внимание на то, что централизованная логика управления вызовами не означает централизацию голосовых маршрутов. Централизованы только администрирование схем связи и управление вызовами. Собственно коммутация голосовых пакетов происходит, как всегда, в элементах компьютерной сети, поэтому сохраняются экономичность и эффективность, присущая продуктам, связанным с обработкой голосовых пакетов.

Будущие приложения для телефонии

По мере дальнейшего совершенствования решений интегрированной передачи голоса и данных, различные производители начали создавать приложения нового типа. Вместо простой передачи и коммутации между мини-АТС системы пакетной передачи голоса теперь начинают заменять мини-АТС решениями "точка-точка". Это означает, что технологии пакетной передачи голоса уже являются не сетевой службой, а приложением, работающим в сети. Разница между данными терминами существенна, когда речь идет о сбыте и администрировании продуктов. По архитектуре их можно разделить на следующие типы.

- **мини-АТС — мини-АТС.** В этой архитектуре сервер на базе PC имеет как порты магистральных шлюзов, так и аналоговые телефонные порты. Обычно специальные программы и драйверы, работающие под управлением NT, обеспечивают все основные стандартные системные функции для аналоговых телефонов. Дополнительные функции, такие как **hold** и **transfer**, подаются путем нажатия на рычаг аппарата или на кнопку Flash. Системы обычно масштабируются до 48 телефонов. Обратите внимание, что в системе нет избыточности, но ее полная стоимость может быть намного ниже, чем у большинства старых систем. В состав многих продуктов входит интегрированная голосовая почта, позволяющая сохранять оцифрованные голосовые сообщения на жестком диске.
- **LAN-АТС.** В эту категорию входят продукты, основанные на LAN-телефонии и распространяющиеся вплоть до настольных ПК. Некоторые из них позволяют использовать службы LAN-телефонии через компьютерные программы на ПК пользователя; другие фактически представляют собой телефоны, подключаемые к локальной компьютерной сети. Со временем возможно создание таких продуктов на базе MAC-уровня (Ethernet), ATM или IP. Продукты 3-уровня (на базе IP) обеспечивают большую гибкость и масштабируемость благодаря тому, что IP является маршрутизируемым протоколом. Следовательно, их можно применять в различных сегментах LAN. Продукты на базе низкоуровневых протоколов имеют привлекательную цену, вследствие меньшей сложности их клиентской части.

Как показал опыт, основными проблемами LAN-телефонии являются надежность и масштабируемость. Для того чтобы интегрированная передача голоса и данных од-

нажды заменила традиционную архитектуру мини-АТС, их необходимо решить. В разных продуктах эти проблемы решаются разными способами. Например, в системе IP-телефонии производства Cisco Systems имеется дополнительный сервер обработки вызовов, так что если на одном сервере произойдет сбой, то IP-телефоны переключатся на резервный. Кроме того, модели обработки вызовов, упрощающие структуру сервера, обеспечивают лучшую масштабируемость. Для этого в продуктах Cisco Systems используется клиент-серверная модель обработки вызовов, подобная MGCP, которая называется Skinny Station Protocol. Она позволяет одному серверу обслуживать тысячи конечных телефонных точек (телефоны и порты шлюзов).

Стимулы создания приложений пакетной телефонии

Современные решения LAN-телефонии предлагают потребителям привлекательные бизнес-модели. Обычные системы "АТС-АТС" стоят дешевле, чем большинство замещаемых ими систем, а системы "LAN-АТС" окупаются быстрее, чем традиционные мини-АТС. Несмотря на сравнимую стоимость базового оборудования, установка систем "LAN-АТС" обычно обходится намного дешевле, так как они используют существующую инфраструктуру компьютерной сети (кабель категории 5), а не требуют прокладки специальных проводов. Администрирование таких систем также не столь обременительно, поскольку администраторы LAN и сервера могут управлять системой без помощи специально приглашенных телефонистов. Наконец, источником дополнительной экономии являются звонки между офисами, потому что они не выходят за пределы компьютерной сети. Со временем оказывается, что системы LAN-телефонии значительно экономичнее, чем обычные мини-АТС.

Это не означает, что мини-АТС обречены. Чтобы такого не произошло, производители традиционных мини-АТС активно переводят свои продукты на пакетную передачу. Начав с простых информационных магистральных плат, позволяющих избежать платы за междугородные переговоры, сейчас производители мини-АТС устанавливают также платы H.323 VoIP, чтобы мини-АТС могли управлять клиентами H.323. Мини-АТС постепенно превращаются в голосовые серверы, как и системы "LAN-АТС", полностью перестраиваясь. Только время покажет, какое из решений лучше, но одно ясно уже сейчас: у потребителей появился более широкий выбор, чем когда-либо.

Вероятно, наиболее привлекательной стороной IP-телефонии является перспектива интеграции приложений с речью. За последние годы была выполнена значительная работа в области CTI (интеграции телефона и компьютера) в традиционных мини-АТС. У этих систем появились программируемые интерфейсы, такие как TAPI (Telephony API), TSAPI (Telephony Services API) и JTAPI (Java Telephony API), что привело к появлению расширенных функций центра обработки вызовов, в том числе экранных меню для агентов и активной маршрутизации вызовов между центрами.

Однако технологи считают, что это только начало. Приложения с интеграцией голоса и данных "произведут революцию" в способах применения таких систем. Например, Unified Messaging обеспечивает доступ к голосовой почте, электронной почте и факсу с одного сервера, используя любую среду передачи. Пользователь может получить голосовую почту на ПК (в виде wav-файлов) или, наоборот, письменные сообщения по телефону, воспользовавшись функцией преобразования текста в речь.

Основная цель этих примеров — переосмысление способов получения информации и ее использования. Способ передачи сможет определять не отправитель сообщения, а получатель. Кроме того, интеграция с интеллектуальным программным обеспечением, таким как электронный секретарь, производимым различными фирмами, позволит пользователям создавать наборы правил для управления всеми входящими звонками. В центре обработки вызовов сложные коммерческие правила (например, проверка кредита перед принятием новых заказов) могут применяться ко входящим сообщениям всех видов (речь, электронная почта и т.п.). В результате у организаций, перешедших на данную технологию, не только уменьшатся затраты, но и возрастет эффективность работы.

Резюме

В этой главе представлен обзор технологий и приложений для интегрированной передачи голоса и данных. Описаны протоколы и элементы архитектуры для передачи голоса по сетям Frame Relay, ATM и IP. Но основное внимание было уделено причинам распространения таких технологий. Эти технологии поддерживают ряд приложений, внедрение которых дает значительный экономический эффект, заключающийся в экономии за счет отказа от междугородных телефонных звонков и замены мини-АТС технологией VoIP. Но главное: новые интегрированные приложения обеспечивают экономический эффект от пакетной передачи речи.

С появлением этих технологий приходится выбирать, какая из них наиболее приемлема для конкретной ситуации. В данной главе обсуждаются возможности различных вариантов. Передача голоса по сетям ATM и Frame Relay больше подходят для простого соединения между разными FNC и транзитной коммутации; передача голоса по IP-сети обеспечивает поддержку сквозных голосовых приложений на настольных ПК и дальнейшее усложнение системы.

Контрольные вопросы

1. Назовите три основные технологии пакетной передачи речи.
2. Каким образом обеспечивается экономия на междугородных звонках при помощи технологии голосовых пакетов?
3. Назовите основные сигнальные протоколы передачи речи.
4. Чем одноранговые сигнальные протоколы передачи голоса отличаются от клиент-серверных протоколов?

Дополнительные источники

- Davidson, Jonathan. *Voice over IP Fundamentals.* Indianapolis: Cisco Press,March 2000.
- Newton, Harry. *Newton's Telecom Dictionary*, New York, March 2003.
- Dodd, Annabel Z. *The Essential Guide to Telecommunications*, New York,September 2001.

В этой главе...

- Вводятся концепции беспроводной передачи и используемая при этом терминология
- Обсуждается беспроводная связь вне пределов прямой видимости (Non-Line-of-Sight — NLOS)
- Описаны компоненты полного решения задачи беспроводной связи
- Приводятся начальные сведения о беспроводных локальных сетях (wireless local-area network — WLAN)
- Обсуждаются преимущества беспроводных систем связи

Глава 20

Беспроводные технологии

Введение

В той или иной форме беспроводные технологии существуют с конца 19-го века. Все технологии, используемые для передачи данных, начиная с дуговых передатчиков и заканчивая сложнейшими беспроводными коммуникационными системами, имеют одну цель — они предназначены для передачи информации в пространстве с помощью электромагнитных волн. Для этого используются самые различные методы, но все они управляются одними и теми же физическими законами и подчиняются их ограничениям.

В настоящей главе описаны основы радиосвязи, начиная с общих теоретических положений и понятий, с последующим рассмотрением типичных современных беспроводных систем. Далее более подробно рассмотрен наиболее популярный тип беспроводных сетей — беспроводные локальные сети.

Основы беспроводной связи

В последующих разделах описываются физические явления, на которых основана радиосвязь, компоненты радиосистем и основные типы используемых в настоящее время беспроводных систем.

Основной целью любой коммуникационной системы является передача информации, в беспроводной связи обычно называемой интеллектуальной (в отличие от служебной), от источника получателю. Эти данные могут быть представлены либо аналоговыми синусоидальными сигналами, либо цифровыми импульсами. Беспроводная связь основана на базовых физических законах, которые управляют передачей, приемом и поведением электромагнитных волн, по мере того как они создаются, распространяются и, в конечном итоге, принимаются получателем вместе с той интеллектуальной информацией, которую они в себе заключают.

Основы радиосвязи

При обсуждении современных сетевых вопросов удивительно часто приходится возвращаться к основным физическим законам, которые изучались еще в школе. Такие разделы физики, как теория передачи сигналов, теория модуляции, передача

энергии в пространстве и чувствительность при приеме применяются в той или иной мере практически в любой используемой в настоящее время технологии. Поэтому при рассмотрении любого вида связи между передатчиком и приемником, включая цифровые абонентские каналы, оптические и кабельные каналы, удаленный доступ и даже простую связь по кабелю RS-232 принципиально важно понимать основные концепции, лежащие в их основе и присущие им ограничения.

С точки зрения обучения беспроводная связь, вероятно, является наилучшим методом изучения и понимания основ коммуникации.

Компоненты беспроводной системы связи

Простейшая беспроводная система состоит из передатчика, подсоединенного проводом к антенне, которая, в свою очередь, образует интерфейс с принимающей антенной, сигнал с которой по проводу подается на приемник. Хотя в таком описании беспроводная связь кажется достаточно простой, в действительности технология этой системы весьма сложна и постоянно совершенствуется. Но в конечном итоге, независимо от уровня сложности современных систем, все они в базовых чертах описываются схемой радиосистемы, показанной на рис. 20.1.

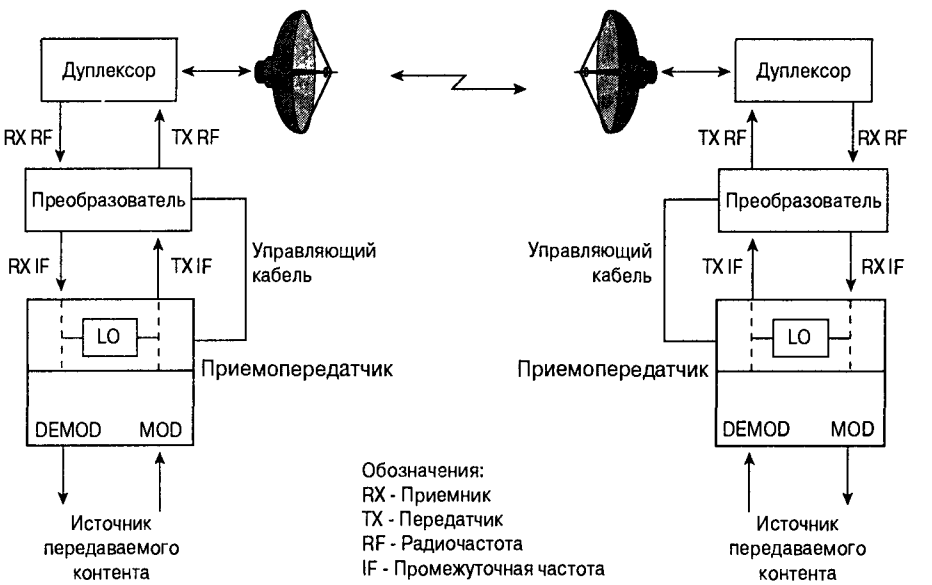


Рис. 20.1. Система беспроводной связи

Ниже описаны основные компоненты систем радиосвязи.

- **Полезная (интеллектуальная) информация источника**—Информация, которую необходимо промодулировать и передать по беспроводному каналу для доставки на принимающий узел. Эта информация может представлять собой голосовые данные, обычные цифровые или видеоданные и в первоначальной форме может быть цифровой или аналоговой.
- **Передатчик/приемник**—Это устройство обычно называют просто "радио". Оно обладает функциями передатчика (transmitter — TX) и приемника (receiver — (RX).

- **Модулятор/демодулятор**—Это устройство преобразует первоначальную информацию в форму сигнала, который генерируется гетеродином (локальным колебательным контуром с определенной частотой, называемой несущей частотой или просто несущей).
- **Локальный гетеродин (Local oscillator — LO)**—Смысловая информация и сигнал, частота которого определяется локальным гетеродином, объединяются в фильтре, который создает суммарный сигнал, разность сигналов и два исходных сигнала. С помощью полосового фильтра сигнал суммарной частоты выделяется и копируется в канал передачи, по которому он поступает на повышающий преобразователь частоты. Результатом этого является так называемый сигнал промежуточной частоты (intermediate frequency — IF). Он представляет собой сигнал с частотой, задаваемой локальным гетеродином, на котором модулируется сигнал, содержащий полезные данные. Частота локального генератора (local oscillator — LO) обычно представляет собой частоту кристалла или синтезированную частоту, которая последовательно увеличивается в 2,3 или 4 раза, до тех пор пока не будет достигнута частота локального гетеродина.
- **Повышающий преобразователь частоты**— Приемопередатчик (трансивер) подсоединен к повышающему преобразователю частоты или внешнему модулю (outdoor unit — ODU) с помощью линии передачи, которая обычно реализуется с помощью коаксиального кабеля. Имеется большое количество различных коаксиальных кабелей. Выбор кабеля зависит от рабочих частот, уровня мощности сигнала и требуемой длины. Линии передачи будут рассмотрены далее в настоящей главе.
- **Кабель для передачи управляющих сигналов**—В зависимости от типов внешнего модуля ODU и приемника/передатчика, в системе может присутствовать кабель для передачи управляющих сигналов между этими двумя устройствами. Возможно, читателю не приходилось встречаться с радиосистемами, в которых блоки промежуточной частоты (IF) и радиочастоты (RF) находятся в отдельных "коробках". В некоторых радиосистемах физические соединения осуществляются непосредственно с антенной. Использование отдельных блоков IF и RF целесообразно в тех случаях, когда источник полезной нагрузки находится на значительном расстоянии от антенны. Свойства передающего канала для IF-сигнала, имеющего частоту 70 МГц и RF-сигнала с частотой 5,7 ГГц принципиально различны. При проектировании системы беспроводной связи необходимо свести протяженность передающего канала для радиочастоты к минимуму, особенно при использовании высоких частот.
- **Дуплексор**—Это устройство позволяет поддерживать дуплексные беспроводные соединения, в которых у каждой системы имеется только одна антенна. При этом в антенне объединяются две разных частоты — одна для приема, другая — для передачи, которые, однако, не смешиваются друг с другом. Такой метод называется мультиплексированием с разделением частот (frequency-division multiplexing — FDM). Типичным способом дуплексирования является использование полостей, которые получаются фрезерованием металла, такого, например, как алюминий. Эти полости выполняют функции полосового фильтра, выделяя требуемые частоты и значительно ослабляя все остальные. В традиционных голосовых радиосистемах, в которых использовались симплексные каналы передачи, сигнал с антенны подавался на приемник до тех пор пока радист на передатчике работал ключом, что приводило к тому, что реле RF дублировало вывод с передатчика на антенну.

- Имеются системы беспроводной связи, которые не являются дуплексными. Симплексной или полудуплексной называется система, в которой связь между двумя конечными точками осуществляется на одной и той же радиочастоте. Поскольку обе станции во время разговора передают на одной и той же частоте, каждой стороне требуется удостовериться в том, что его собеседник сделал паузу, в противном случае никто из них не услышит друг друга.
- Выше были приведены первичные сведения о беспроводных системах связи. Конечно, в реализациях этой схемы существуют множество различий, однако все они базируются на описанных выше компонентах и целью беспроводной связи всегда является получение данных или полезной нагрузки от источника, модуляция их в сигнал промежуточной частоты IF, с последующим преобразованием в сигнал радиочастоты RF и доставкой получателю через атмосферное пространство. Используемые при этом методы и лежащие в их основе физические явления будут описаны в последующих разделах, однако до этого целесообразно рассмотреть спектр электромагнитных волн.

Электромагнитный спектр

Под электромагнитным спектром (Electromagnetic — EM spectrum) понимается совокупность всех возможных форм электромагнитного излучения. Излучение представляет собой энергию, которая перемещается в пространстве теоретически со скоростью света; по мере распространения она рассеивается.

Существует много типов электромагнитного излучения:

- Видимый свет, например, свет от домашней электролампы;
- Радиоволны, которые поступают от передающей радиостанции;
- Микроволновое излучение, используемое в радиоканалах типа "точка-точка" и в микроволновых печах;
- Инфракрасное и ультрафиолетовое излучение, рентгеновское излучение и гамма-излучение.

В зависимости от сферы применения электромагнитный спектр делится на несколько диапазонов. Важно отметить, что большая часть спектра используется *лицензированными пользователями (licensed users)*, которыми являются провайдеры служб, правительственные органы и т.д, для таких целей, как управление авиаполетами или оборона страны.

Выделением частот лицензированным пользователям обычно занимаются правительственные органы, такие как Федеральная комиссия по коммуникациям США (Federal Communications Commission — FCC) или Канадская комиссия по радио, телевидению и телекоммуникациям (Canadian Radio-Television and Telecommunications Commission — CRTC) в Канаде. Оба этих органа предоставляют большое количество справочного материала.

Радиочастоты измеряются в герцах; эти значения частоты эквивалентны количеству циклов в секунду. Для более высоких частот электромагнитного спектра в качестве единицы измерения чаще используется длина волны. В частности, это типично для оптических технологий, в которых базовыми длинами оптических волн являются значения 850, 1310, и 1550 нанометров (нм). Эта система измерений более удобна при практическом применении.

Для вычисления частоты в герцах используется следующая формула:

$\lambda = c / F$

где

- λ — длина волны в метрах;
- c — скорость света в вакууме ($3{,}0 * 10^8$ м/с);
- F — частота в герцах.

Особый интерес в настоящем обсуждении беспроводных технологий представляет часть электромагнитного спектра, называемая радиочастотами. Основные диапазоны этой части спектра приведены в табл. 20.1.

Таблица 20.1. Основные диапазоны беспроводной связи

Сфера применения	Диапазон частот	Примечания
AM-радио	От 535 до 1705 КГц	Коммерческие радиочастоты
Аналоговые телевизионные каналы 2-6 (VHF)	От 54 до 88 МГц	Широковещательное телевидение
FM-радио	От 88 до 108 МГц	Коммерческие радиочастоты
Аналоговые телевизионные каналы 7-13 (VHF)	От 174 до 216 МГц	Эти диапазоны частот были выделены комиссией FCC для поддержки цифрового телевидения начиная с 2007г.
Аналоговые телевизионные каналы 14-69 (UHF)	От 470 до 806 МГц	Эти диапазоны частот были выделены комиссией FCC для поддержки цифрового телевидения начиная с 2007г.
Сотовая телефония	От 825 до 894 МГц	Аналоговая общедоступная телефонная сеть (POTS)
Промышленные, научные и медицинские системы (industrial, scientific and medical — ISM)	От 902 до 928 МГц	Нелицензируемые фирменные системы
PCS	От 1850 до 1990 МГц	Беспроводная связь 2G
ISM	От 2,4 до 2,4835 ГГц	Не лицензируется; системы спецификации 802.11 и фирменные системы
Многоканальная многоточечная служба распределения (Multichannel Multipoint Distribution Service — MMDS)	От 2,1 до 2,7 ГГц	33 канала с полосой частот 6 МГц; выделенные для беспроводной связи 3G
Нелицензируемая Национальная Информационнная инфраструктура (Unlicensed National Information Infrastructure — U-NII)	От 5,15 до 5,35 ГГц, от 5,725 до 5,825 ГГц	Не лицензируется; системы спецификации 802.11 и фирменные системы
Локальная многоточечная система распределения (Local Multipoint Distribution System — LMDS)	От 27,4 до 31,3 ГГц	Два блока частот, с общей полосой частот 1,3 ГГц

Окончание табл. 20.1

Сфера применения	Диапазон частот	Примечания
Космическая оптика	W-диапазон 60 ГГц	Широкая полоса пропускания; оптическая замена
Космическая оптика	IR 765 нм	Широкая полоса пропускания; оптическая замена

В табл. 20.1 описана лишь небольшая часть электромагнитного спектра, однако в ней указаны основные области, в которых в настоящее время используются беспроводные сетевые технологии. Более подробную информацию об остальных частях ЕМ-спектра можно получить на Web-сайте комиссии FCC.

Теория передачи сигналов в диапазоне радиочастот RF

Выше были кратко описаны беспроводные системы, электромагнитный спектр и основные диапазоны частот, которые используются в беспроводных сетях. Далее рассматриваются теоретические основы радиосвязи.

Энергия электромагнитных волн

Для того, чтобы понять, каким образом функционирует беспроводная связь, необходимо изучить вопрос о том, как генерируются и распространяются в пространстве электромагнитные волны. При прохождении тока по металлическому проводу создается электрическое поле, которое, в свою очередь, порождает магнитное поле. У переменного тока, в отличие от постоянного, электрическое поле создается и исчезает с той же частотой, с какой меняется направление тока. Магнитное поле порождается и исчезает с той же скоростью, как и электрическое поле. При таком изменении полей возникает электромагнитная волна, которая излучается проводом, выступающим в данном случае в роли антенны.

Возникающая электромагнитная волна или импульс имеет синусоидальную форму и, соответственно, имеет три основных характеристики волнового процесса — амплитуду, фазу и частоту. Эти характеристики наследуются волной от первоначального электрического сигнала, который дублируется в антенне после того, как он был сгенерирован передатчиком.

Наиболее важными факторами, определяющими эффективность функционирования системы беспроводной связи, являются мощность конечного усилителя радиочастоты и уровень сигнала на входе приемника. Составными элементами передачи на радиочастотах являются передающие каналы, антенны и атмосферный интерфейс.

Измерение мощности

Первым элементом радиопередачи являются передающие каналы. Однако перед обсуждением этих каналов необходимо подчеркнуть важность мощности сигнала и ее измерения, поскольку эта мощность является одним из наиболее важных факторов, определяющих успешную работу системы связи. Назначение передающего канала состоит в том, чтобы надежно передать сигнал на антенну, сведя при этом к минимуму потери в среде передачи. Канал передачи должен иметь соответствующие электрические спецификации, такие как импеданс, коэффициент передачи мощности и уровень потерь. Эти

характеристики связаны между собой и весьма важны для разработчика системы. Однако их рассмотрение выходит за рамки настоящего вступительного обзора.

В беспроводной связи мощность сигнала обычно измеряется в ваттах или в дБм. Исходной величиной является мощность 1 мВт, которая принимается за значение 0 дБм. В мощных радиопередатчиках мощность обычно измеряется в ваттах, однако в устройствах с небольшой выходной мощностью удобнее измерять мощность в дБм.

В табл. 20.2 показано соотношение величин мощности в дБм и Вт.

Таблица 20.2. Ватты и дБм

Мощность в дБм (относительно мощности 1 мВт)	Мощность в ваттах
50 ДБм	100 Вт
40 ДБм	10 Вт
30 ДБм	1 Вт
20 ДБм	100 мВт
10 ДБм	10 мВт
0 ДБм	1 мВт
–10 ДБм	100 uВт
–20 ДБм	10 uВт
–30 ДБм	1 uВт

Для быстрого вычисления мощности в ваттах при наличии значений в дБм следует выполнить следующие действия:

- При увеличении мощности на 1 дБм значение в ваттах необходимо умножить на 1,25;
- При увеличении мощности на 2 дБм значение в ваттах следует умножить на 1,5;
- При увеличении мощности на 3 дБм значение в ваттах следует умножить на 2.

Эти правила можно применять и для обратного преобразования. Например, уменьшение мощности на 3 дБм приводит к уменьшению мощности в ваттах в 2 раза. Для сигнала мощностью 20 дБм или 100 мВт при увеличении мощности на 5 дБм значение в ваттах надо сначала умножить на 2, а затем на 1,5, что дает значение 300 мВт.

Под *затуханием* понимается потеря мощности сигнала при его прохождении по физической среде, независимо от ее природы — в атмосфере, в физическом передающем канале или в электрической цепи, такой как фильтр. Подобно тому как измеряется *усиление (gain)* сигнала, так же измеряется и его ослабление или *затухание (attenuation)*. Учет этих потерь необходим для того, чтобы после передачи сигнал поступал на принимающую станцию с достаточным уровнем мощности. Приемник должен быть достаточно чувствительным для того, чтобы он смог выделить требуемую частоту. Если приемник не сможет этого сделать, то невозможно будет выполнить обратное преобразование сигнала и выделить из него передаваемую полезную информацию.

Передающие каналы

Назначение передающего канала состоит в обеспечении физического соединения между передающим и принимающим устройствами. Передающие каналы могут быть реализованы в различных формах и с использованием разных материалов. В беспроводных сетях обычно используются следующие типы каналов:

- коаксиальные кабели;
- волноводы.

Каждый из этих типов передающих каналов имеет множество разновидностей, однако независимо от выбранного типа канал обладает следующими характеристиками, которые должны быть учтены при проектировании:

- затухание радиочастот;
- импеданс;
- потери по постоянному току (если этот канал используется также для подачи постоянного тока на преобразователь частоты);
- физические характеристики, такие как вес и радиус изгиба;
- стоимость.

Первые три характеристики в определенной степени взаимосвязаны, а также зависят от частот, которые передаются по каналу. Чем выше частота, тем больше затухание и, соответственно, потери.

Критически важным является также значение импеданса, поскольку он должен быть одним и тем же на обоих концах канала. Несовпадение импеданса приводит к ухудшению передачи электрической энергии в точках механического соединения. Другой проблемой, которая возникает при несовпадении импедансов, является возникающее отражение сигналов. Если не все 100% передаваемой энергии передаются через механическое соединение в цепь получателя, то часть энергии направляется в окружающее пространство (такое явление называется утечкой) или отражается в направлении передающего устройства.

Эта энергия может вызвать серьезные проблемы, если фаза отраженного сигнала не совпадает с первоначальной. Если на первоначальный сигнал накладывается его собственное отражение, равное по амплитуде, но с фазой, измененной на 180 градусов, то первоначальный сигнал фактически становится равным нулю. Конечно, трудно представить ситуацию 100%-го отражения сигнала с точно противоположной фазой, однако в определенной степени отражение с измененной фазой всегда имеет место. Результирующий сигнал может увеличиться по сравнению с первоначальным, если имеет мест полное совпадение фаз, но в случае несовпадения фаз происходит ослабление сигнала.

В беспроводных системах такое ослабление замеряется и называется коэффициентом стоячей волны (Voltage Standing Wave Ratio — VSWR). Это значение VSWR характеризует степень несоответствия импедансов передающего канала и его нагрузки, которой в данном случае является антенна. Чем больше это значение, тем больше несоответствие импедансов.

Антенны

Вторым компонентом системы RF-передачи является антенна. Выше была рассмотрено функционирование базового приемника/передатчика и подсоединенного к нему передающего канала. Далее следует рассмотреть другой конец передающего канала, на котором находится антенна. Антенна выполняет две основные функции. Первая из них состоит в приеме энергии радиочастоты от передатчика и ее излучения в требуемом направлении, т.е. в направлении принимающей антенны. Второй функцией является прием энергии от передатчика и передача ее приемнику. Работа антенны определяется несколькими ключевыми факторами, которые обсуждаются далее.

Одновременная дуплексная передача

Рассмотрим понятие одновременной дуплексной передачи. Некоторые радиосистемы позволяют осуществлять постоянную дуплексную (двустороннюю) передачу сигналов. В принципе для такой передачи необходимы две антенны или какое-либо устройство, которое может обеспечить одновременное прохождение сигналов принимающей и передающей частот при использовании одной антенны. Такое устройство называется дуплексором.

Главной функцией дуплексора является разделение и объединение сигналов, что позволяет использовать две различных частоты при наличии лишь одной антенны. Приемная и передающая частоты передаются по одному каналу с одними и теми же RF-характеристиками, поэтому они должны быть достаточно близки друг к другу. Такое использование дуплексора называется *мультиплексированием с разделением частот (frequency division multiplexing — FDM).*

Много лет назад автору пришлось работать с микроволновой радиорелейной системой, в которой использовались квадруплексоры. Это позволяло использовать две передающих и две принимающих частоты при наличии лишь одной антенны. Квадруплексор был фиксированным, т.е. он не допускал настройки частот и был изготовлен из алюминия путем фрезерования. Его электрические характеристики были аналогичны характеристикам полости и он функционировал как волновод, обеспечивающий прохождение требуемых сигналов и существенно ослабляющий все остальные.

Изотропной антенной называется теоретическая антенна, которая излучает электромагнитные волны равномерно во всех направлениях. Такая антенна используется в качестве эталона при рассмотрении свойств направленных антенн. При оценке антенн используется такая характеристика, как коэффициент усиления антенны, который часто измеряется в dBi и отражает принимающие или излучающие свойства конкретной антенны по сравнению с изотропной. Измерение этой величины позволяет сравнивать различные антенны. На рис. 20.2 проиллюстрированы некоторые положения теории антенн.

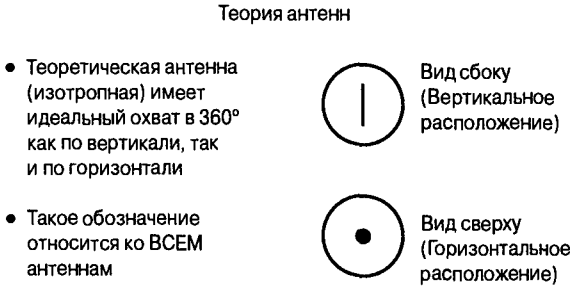


Рис. 20.2. Некоторые понятия теории антенн

Эффективная изотропная мощность излучения (Effective Isotropic Radiated Power — EIRP)

Эффективная изотропная мощность излучения (Effective Isotropic Radiated Power — EIRP) равна мощности сигнала радиочастоты, поданного на антенну, умноженной на коэффициент усиления, соответствующий изотропному излучателю.

EIRP вычисляется по формуле:

EIRP (dBW) = Ptx (dBW) + Gant (dBi) − Ltlc (dB)

где

- Ptx — выходная мощность передатчика в дБВт ;
- Gant — усиление в антенне, обычно вдоль главного лепестка антенны;
- Ltlc — потери в канале передачи, включая потери в соединениях.

Мощность EIRP обычно выражается в дБВт , однако может быть вычислена в дБм или просто в ваттах. Ниже приводится пример вычисления EIRP в дБм:

EIRP (dBm) = Ptx (dBm) + Gant (dB) − Ltlc (dB)

Например, предположим, что выходная мощность передатчика равна 8,5 Вт, коэффициент антенны равен 11 дБ, потери в кабеле 1,2 дБ и в разъемах 0,25 дБ. Выходная мощность передатчика должна быть сначала преобразована из Вт в ДБм.

EIRP равна

EIRP = 39,29 дБм + 11,0 дБ − 1,45 дБ = 48,84 дБм (EIRP)

Типы антенн

Существует много различных типов антенн. Выбор типа антенны определяется видом излучения, частотой и радиочастотными характеристиками покрытия беспроводной сети. Именно при выборе антенны должна быть оценена принятая концепция EIRP, поскольку она является критически важным фактором при выборе антенны.

Для беспроводных систем существует много типов антенн. Основным критерием при выборе антенны является ее направленность. В этом отношении антенны делятся на два основных типа:

- Всенаправленные;
- Однонаправленные или просто направленные антенны.

Всенаправленными называются антенны, в которых излучаемая энергия распространяется равномерно во всех направлениях. В однонаправленной антенне энергия распространяется преимущественно в одном направлении.

Перед тем, как продолжить обсуждение, целесообразно более подробно проанализировать понятие "во всех направлениях".

При описании антенны необходимо также рассмотреть такую ее характеристику, как поляризация. Под поляризацией понимается физическое расположение активного элемента относительно Земли. Активным элементом антенны называется та ее часть, на которую подается сигнал, и с которой, соответственно, происходит излучение энергии. Антенны могут иметь горизонтальную или вертикальную поляризацию. Различие между изотропной и всенаправленной антеннами состоит в том, что всесторонняя антенна излучает электромагнитные волны на весь сектор 360^0, однако реальный характер излучения определяется поляризацией активного элемента.

Физические компоненты антенны включают в себя один или несколько активных элементов, рефлекторы (отражатели) и пассивные вибраторы. Активным элементом называется часть антенны, с которой происходит излучение энергии или прием электромагнитных волн от других источников излучения. Это элемент соединен с приемником/передатчиком через передающий канал.

Односторонняя антенна направляет излучаемую энергию в конкретном направлении и, следовательно, концентрирует ее. Это осуществляется с помощью рефлекторов. Основными типами направленных антенн являются параболические антенны, полупараболические, зеркальные, панельные и антенны типа "волновой канал". Они имеют высокий коэффициент усиления и могут иметь очень узкую направленность. Эти антенны используются

как в каналах типа "точка-точка", так и в многоточечных каналах. При использовании соответствующей конструкции они могут иметь частичную направленность, в том смысле, что их диапазон излучения представляет собой сектор. Например, в мобильной связи или в широкополосной многоточечной связи приемопередатчик концентратора может использовать три антенны, каждая из которых охватывает сектор 120^0, что позволяет сконцентрировать излучаемую энергию в требуемом секторе (рис. 20.3). При этом в каждом секторе необходимо обеспечить эффективное использование доступных частот. Если имеется несколько смежных областей и их сотовые ячейки используют схожие разделения частот, то становится возможным интерференция между ними, поэтому необходимо установить такое разделение частот, которое исключало бы наложение частот различных сигналов.

Рис. 20.3. Три сектора антенны, каждый из которых охватывает диапазон 120 градусов

Важным понятием, которое используется при выборе типа однонаправленной конической (или зеркальной) антенны, является ширина луча. Излучаемая энергия концентрируется при помощи конуса, который выполняет функции рефлектора. Аналогичный принцип используется в карманных фонариках типа Maglite. В этом фонарике при повороте обоймы фактически происходит перемещение лампочки по оси, что приводит к сужению или расширению светового пучка. Такое же явление имеет место для электромагнитных волн, излучаемых зеркальной антенной. Действительный уровень излучаемой энергии (в данном случае световой) остается неизменным, однако эта энергия распространяется на большей площади. Вследствие этого зона, в которой может быть принят сигнал, становится более широкой. При такой концентрации излучения можно использовать сигнал меньшей мощности или достигать большей дальности передачи. На рис. 20.4 показан один из типов направленной антенны.

На рис. 20.5 показана типичная всенаправленная антенна. Такие антенны используются в тех случаях, когда желательно распространять передаваемый сигнал от базовой станции или передатчика во всех направлениях, т.е. в полном круговом секторе 360^0. Типичными системами, в которых это требуется, являются широковещательные радиостанции и

навигационные системы. Однако даже при использовании всенаправленной антенны следует иметь в виду, что из-за внешних по отношению к антенне факторов на практике равномерного кругового охвата получить все же не удается. Это связано как с особенностями излучения антенны, так и с различиями в среде распространения сигналов.

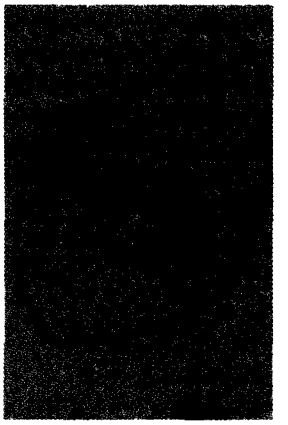


Рис. 20.4. Типичная направленная антенна

Выше были рассмотрены некоторые основные положения теории антенн. Читатель, вероятно, обратил внимание, что до сих пор речь шла только о характеристиках антенн при передаче сигналов. Конечно, антенны должны быть также способны принимать и сигналы от других источников. Сигналы, принимаемые антенной и передаваемые на приемник, имеют амплитуду в несколько микровольт, а в некоторых системах и меньшую. Для того чтобы антенна обеспечивала эффективную беспроводную связь, она должна обладать особыми качествами и характеристиками. Эти качества позволяют антенне принимать очень слабые сигналы и передавать их приемнику с уровнем, достаточным для восстановления модулированной информации.

Рис. 20.5. Типичная всенаправленная антенна

Распространение радиочастот в пространстве

Третьим компонентом передачи сигналов радиочастоты является воздушное пространство, т.е. пространство между передающей и принимающей антенными системами. После того, как электромагнитные волны излучаются передающей антенной, они распространяются в этом пространстве, сохраняя достаточную энергию для того, чтобы достичь принимающей антенны и обеспечить достаточную мощность сигнала

при поступлении на приемник. Однако среда распространения электромагнитных волн может оказывать весьма неблагоприятное воздействие на их энергию. Существует много факторов, которые должны быть учтены при проектировании беспроводных систем. Ниже приведены некоторые из них.

- Потери в атмосфере;
- Дальность прямой видимости;
- Зона Френеля;
- Кривизна поверхности Земли.

После того, как радиоволны покидают передающую антенну и начинают распространяться в направлении принимающей антенны, на них воздействуют атмосфера, физические процессы и географические особенности местности. При оценке их перемещения в пространстве первым фактором являются потери в свободном пространстве (free space loss — FSL). Эта величина является наилучшей оценкой потерь мощности сигнала на пути к принимающей станции. Значение потерь в свободном пространстве является теоретической величиной; при ее вычислении предполагается, что отсутствуют дифракция, рефракция, а на пути перемещения радиоволн нет препятствий или рассеивания. Величина FCL отражает лишь потери, которые испытывает сигнал при удалении от источника вследствие дивергенции лучей. Эта величина может быть вычислена по формуле:

Lp = 36,6 + 20 LogF + 20LogD

где

- Lp — потери в свободном пространстве или ослабление между антеннами в дБ;
- Константа 36,6 используется для сухопутной мили. При использовании морской мили значение этой константы равно 37,8;
- F — частота передаваемого сигнала в МГц;
- D — расстояние передачи в сухопутных милях.

Большое количество FSL-калькуляторов имеется на различных сайтах сети Internet (WWW). При их использовании для получения ответа достаточно ввести конкретные значения параметров. Для нахождения таких калькуляторов можно использовать любую поисковую машину.

При рассмотрении распространения радиоволн весьма важной характеристикой является расстояние прямой видимости (line of sight — LOS). Для радиочастот расстояние прямой видимости означает большее, чем просто возможность видеть принимающую антенну из места расположения передающей антенны. В данном случае для прямой видимости необходимо, чтобы в так называемой зоне Френеля не было никаких объектов, таких как деревья, дома или поверхность земли. Под зоной Френеля понимается область, прилегающая к зоне прямой видимости, в которой распространяются радиоволны после выхода с передающей антенны. Эту область необходимо точно определить, поскольку вне ее качество сигнала резко падает из-за дополнительного ослабления.

Зоны Френеля представляют собой области излучаемой энергии. Теоретически количество таких областей бесконечно, однако на практике рассматривается только первая зона Френеля. Эти зоны имеют эллипсоидальную форму и располагаются вдоль маршрута прямой видимости LOS.

В первой зоне Френеля необходимо, чтобы большая часть имеющейся энергии достигла принимающей антенны, несмотря на потери в свободном пространстве, которые ожидаются на основании расчетов, учитывающих частоту и дальность передачи. Чтобы передать максимальное количество энергии, необходимо добиться того, чтобы препятствия распространению волн занимали не более 40% зоны LOS. Необходимо также учесть кривизну Земли, которая является следствием того, что Земля представляет собой эллипсоид. Совместный эффект этих двух факторов, влияющих на прохождение сигнала, часто требует использования антенны максимальной высоты. На рис. 20.6 проиллюстрирован эффект кривизны Земли и понятие зоны Френеля.

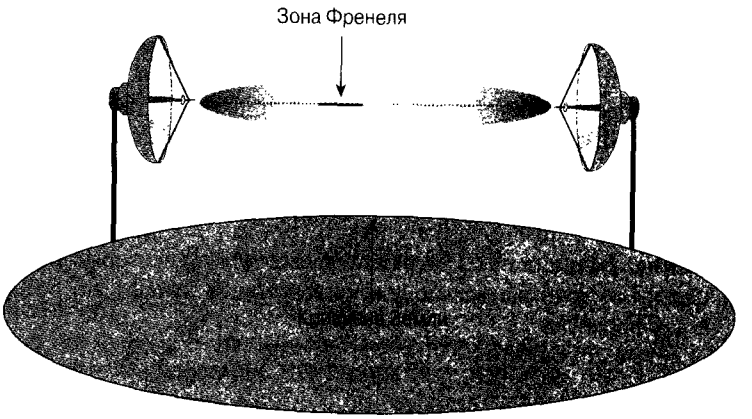


Рис. 20.6. Зона Френеля и кривизна Земли

Для вычисления радиуса зоны Френеля используется следующая формула:
Rft= 72.1 *квадратный корень из D1 * D2 / FD
где

- Rft — радиус первой зоны Френеля в футах;
- D1 — расстояние от передатчика до препятствия на маршруте передачи сигнала;
- D2 — расстояние от препятствия на маршруте передачи сигнала до приемника;
- F — частота сигнала в ГГц;
- D = D1 + D2 — расстояние передачи в милях.

Для вычисления эффекта кривизны Земли используется следующая формула:
Кривизна Земли в футах = D^2 / 8
где

- D^2 — квадрат расстояния между антеннами

В табл. 20.3 приведены стандартные значения для типичных расстояний передачи сигналов.

Для эффективной передачи сигнала необходимо найти способ добиться того, чтобы зона Френеля была достаточно свободна от препятствий и учесть кривизну Земли. Возможно, что для этого придется поднять антенну на мачте. Необходимо также принять во внимание географические особенности местности. Для того, чтобы беспроводная система работала в соответствии с предъявляемыми требованиями, необходимо

выбрать подходящий маршрут распространения сигнала и проанализировать иные факторы, влияющие на качество передачи.

Таблица 20.3. Значения кривизны Земли

Расстояние в милях	Кривизна в футах
2	0.5
4	2.0
6	4.5
8	8.0
10	12.5
12	18.0
14	24.5
16	32.0

Беспроводная связь вне пределов видимости: уменьшение влияния наложения сигналов в высокоскоростных линиях

В настоящей главе рассматривается одна из основных проблем, возникающих при использовании беспроводной связи и способы ее смягчения. В ней также обсуждаются методы модуляции сигналов и их кодирования.

Наложение сигналов

Под *наложением сигналов* (multipath) понимается суммирование первичного сигнала и эхо-сигналов, появившихся в результате отражения сигналов от объектов, расположенных между передатчиком и приемником. На рис. 20.7 приемник принимает основной сигнал, идущий непосредственно от передатчика, а также вторичные сигналы, отраженные от близлежащих объектов.

Отраженные сигналы поступают на приемник позже основного сигнала. В результате такого запаздывания " выбившиеся " из фазы сигналы вызывают межсимвольную интерференцию и искажение принимаемого сигнала. Обычно наложение сигналов происходит из-за отражения от высоких объектов, однако оно может появляться и в результате отражения от низко расположенных объектов, например озер или дорожного покрытия.

В действительности принимаемый сигнал представляет собой комбинацию основного сигнала и нескольких эхо-сигналов. Поскольку расстояние, пройденное основным сигналом, короче того, которое прошли отраженные сигналы, они принимаются не одновременно. Подобные сигналы накладываются друг на друга и сливаются в один общий сигнал. Обычно время между приемом исходного и последнего отраженного сигнала составляет до 4 мс.

В примере, показанном на рис. 20.8, эхо-сигнал имеет временную задержку и меньшую мощность. Это связано с дополнительным расстоянием, которое прошел отраженный

сигнал по сравнению с исходным. Чем больше расстояние, тем больше задержка и меньше мощность отраженного сигнала. На первый взгляд, чем больше задержка, тем лучше прием. Но если задержка слишком велика, прием отраженного символа S1 может наложиться на основной сигнал символа S2. Поскольку в системах, не требующих прямой видимости, основной сигнал не всегда распространяется по прямой, мощность исходного сигнала может оказаться меньше мощности вторичных сигналов.

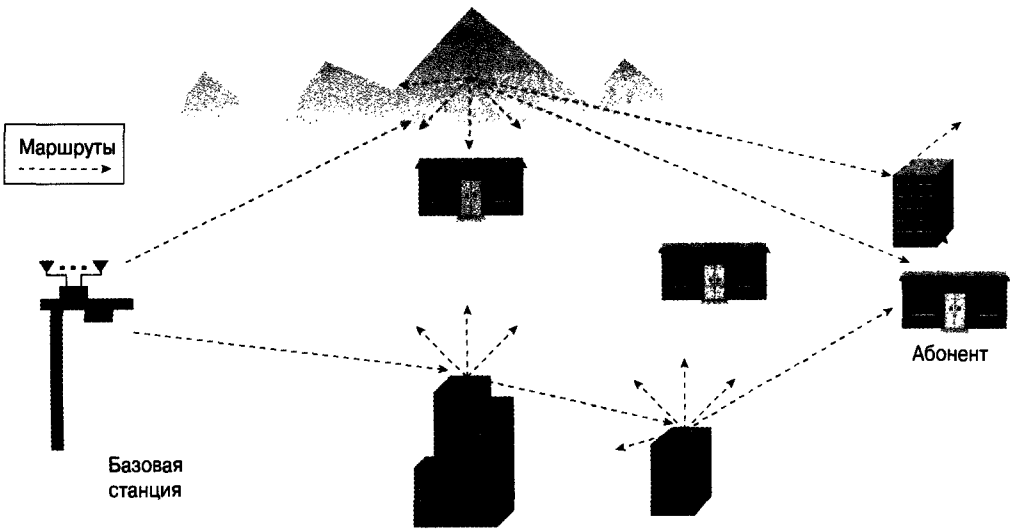


Рис. 20.7. Наложение сигналов

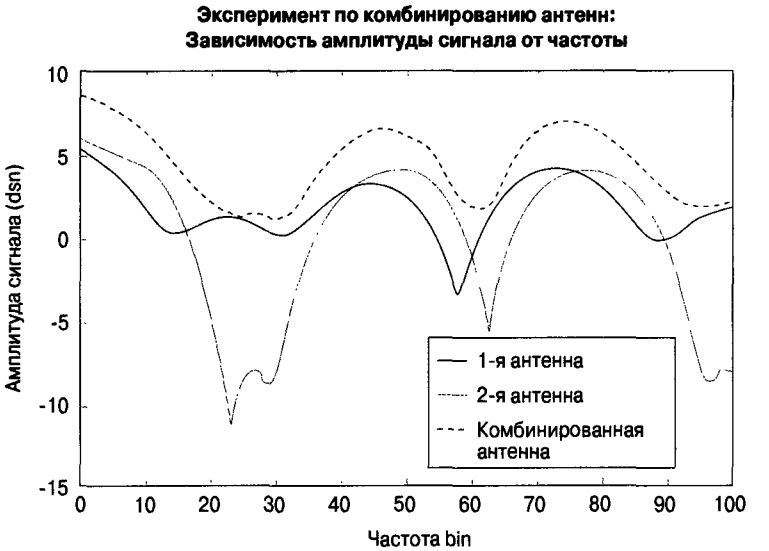


Рис. 20.8. Прием наложения сигналов

В аналоговых системах, таких как телевидение, наложение сигналов можно заметить невооруженным глазом. Иногда на экране появляется "призрачное" изображение, которое невозможно устранить настройкой. В аналоговых системах такое явление

вызывает лишь раздражение. В цифровых системах это обычно приводит к повреждению потоков данных, их потере и снижению производительности. Для коррекции наложения сигналов, из-за которого происходят потери данных, применяются специальные корректирующие алгоритмы.

В цифровых системах входящий сигнал представляет собой набор символов. Отраженный сигнал фактически накладывается на следующий принимаемый символ, вследствие чего возникает межсимвольная интерференция (InterSymbol Interference — ISI). Основной причиной ISI является наложение сигналов, что необходимо учитывать в конструкции цифровых систем.

Каналы микроволновой связи

С самого начала производства оборудования для беспроводной связи производители и операторы связи прилагали усилия для ослабления неблагоприятного влияния эффекта отражения сигналов, связанного с их распространением и называемого наложением сигналов (multipath signals). В современных микроволновых системах в процессе проектирования используются совершенные методы ослабления эффекта наложения сигналов. Большинство используемых подходов позволяют добиться высокой степени надежности передачи информации в беспроводных системах. В настоящем разделе рассматривается процесс создания микроволновых цифровых систем передачи, которые не только ослабляют неблагоприятное воздействие наложения сигналов, но и извлекают из этого эффекта определенные преимущества.

Цифровые микроволновые системы делятся на два типа: с длиной волны менее 10 ГГц и с длиной волны более 10 ГГц (такие волны называются миллиметровыми). Для высокоскоростной передачи используются несколько диапазонов с длиной волны менее 10 ГГц. Среди них есть лицензируемые диапазоны, такие как диапазон MMDS (2,5 ГГц) и нелицензируемые, такие как диапазон U-NII (5,7 ГГц). Использование диапазонов с частотами менее 10 ГГц позволяет добиться большой дальности передачи (до 30 миль). На распространение таких волн почти не влияют климатические явления, такие как дождь. Они также практически не поглощаются окружающей средой. Однако такие волны часто испытывают отражение, что приводит к появлению нескольких аналогичных сигналов, которые накладываются друг на друга.

Дальность распространения сигналов с частотами свыше 10 ГГц, такими как частоты диапазонов 24 ГГц, LMDS (28 ГГц) и 38 ГГц, весьма ограничена и не превышает 5 миль. Они также подвержены ослаблению, в частности при дождливой погоде. Проблема наложения для таких сигналов значительно менее остра, поскольку их дальность распространения относительно невелика и большая часть энергии отраженных сигналов поглощается окружающей средой. Однако если такие частоты используются в плотно застроенной городской среде, то часто возникает эффект отражения, в частности от таких объектов как металлические строительные конструкции или металлические рамы окон. Применение повторителей может увеличить эффект наложения при распространении сигнала, поскольку сигнал принимается с задержкой.

Наложение сигналов в системах без прямой видимости

В системах с прямой видимостью наложение сигналов обычно невелико и легко подавляется. Амплитуда отраженных сигналов значительно ниже амплитуды основного

сигнала, поэтому они могут быть эффективно отфильтрованы с помощью стандартных эквалайзеров. Однако в системах без прямой видимости эхо-сигналы могут быть не менее мощными, чем основной, поскольку последний может быть сильно ослаблен, в основном из-за большого количества наложений, поэтому в данном случае требуются эквалайзеры более сложной конструкции.

До сих пор в настоящем изложении предполагалось, что наложение сигналов носит условно-постоянный характер. Однако это не всегда так: некоторые объекты движутся, что иногда играет важную роль. Иногда условия наложения сигналов изменяются с течением времени. Такое явление называется временными отклонениями. Цифровые системы должны выдерживать быстрые изменения условий наложения сигналов, называемые *быстрым замиранием* (fast fading). Для этого им требуются быстродействующие схемы AGC. Адаптивные эквалайзеры, которые будут описаны ниже, должны обладать способностью к быстрому самообучению.

Методы модулирования и кодирования сигналов с использованием QAM

Многие современные системы СВЧ-связи фиксированной частоты основаны на квадратурно-амплитудной модуляции (Quadrature Amplitude Modulation — QAM). Существуют разные уровни сложности таких систем.

Простейшие системы, например, системы фазовой модуляции (Phase Shift Keying — PSK), очень надежны и просты в реализации из-за низкой скорости передачи данных. В системах с фазовой модуляцией волна не изменяет ни частоты, ни амплитуды, а только фазу. Фаза волны изменяется во времени.

При использовании двоичной фазовой модуляции (binary phase shift keying — BPSK) фаза синусоидальной волны начинается или с 0 или с 1/4. При двоичной фазовой модуляции за один цикл (называемый символом) передается только 1 бит. В более сложных схемах модуляции за один цикл передаются несколько битов. Схема квадратурно-фазовой модуляции (Quadrature Phase Shift Keying — QPSK) аналогична схеме двоично-фазовой модуляции, однако вместо двух значений фазы в алгоритме квадратурно-фазовой модуляции используется четыре (0, $\pi/2$, π и $3\pi/2$), что обеспечивает передачу 2 битов за символ. Подобно двоично-фазовой, квадратурно-фазовая модуляция широко применяется вследствие ее надежности. Однако, поскольку квадратурно-фазовая модуляция позволяет передать только 2 бита за символ, она является недостаточно эффективной для высокоскоростной передачи данных. Чтобы повысить скорость передачи, требуется значительно более широкая полоса пропускания.

Несмотря на то, что при квадратурно-фазовой модуляции амплитуда не изменяется, ее иногда называют четырехуровневой квадратурно-амплитудной модуляцией (4-QAM). При соединении четырех уровней изменения амплитуды с четырьмя значениями фазы, возникает 16-уровневая квадратурно-амплитудная модуляция (16-QAM). При ее использовании 2 бита передаются изменениями фазы и 2 — изменениями амплитуды, что обеспечивает передачу четырех битов за символ.

На рис. 20.10 приведены амплитудно-фазовые диаграммы модуляции для трех типичных схем — QPSK, 16-QAM и 64-QAM. Различные значения фазы и амплитуды образуют равномерную систему координат с осями I и Q. Угол поворота задает фазу, а расстояние до центральной точки — амплитуду. Такой подход можно распространить

до 64-уровневой, 256-уровневой модуляции и выше. Модуляция 64-QAM очень широко распространена как в проводных, так и в беспроводных широкополосных сетях; исследования в этом направлении продолжаются и технология 256-QAM также прошла тестирование. Однако чем выше плотность QAM, тем более высокое отношение сигнал/шум (signal-to-noise — SNR) должно обеспечиваться для поддержания требуемой частоты ошибок по битам (Bit-Error Rate — BER).

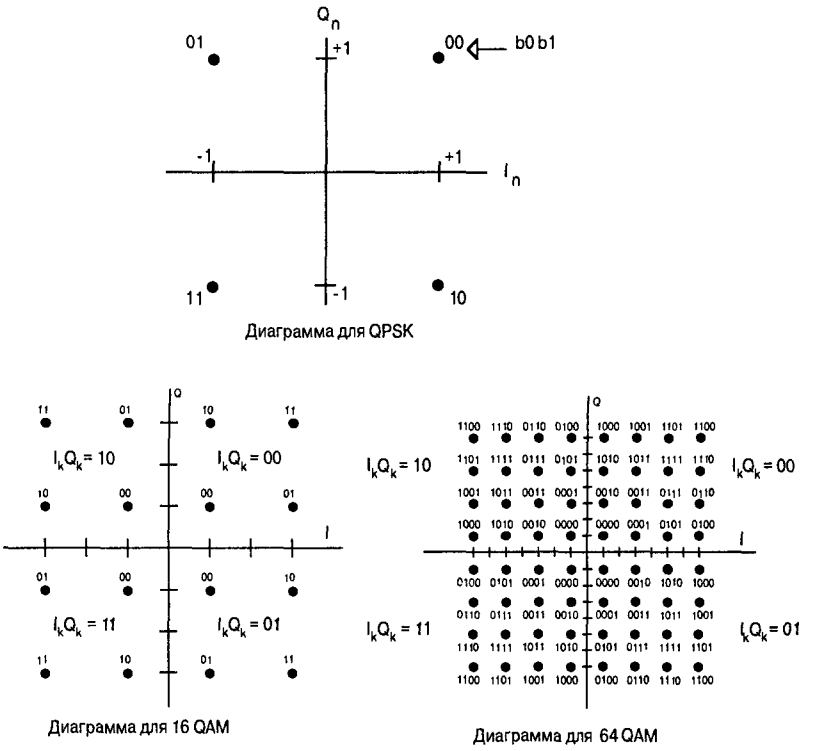


Рис. 20.09. Амплитудно фазовые диаграммы для QPSK, 16-QAM и 64-QAM

Способ кодирования данных также играет существенную роль. Обычно данные шифруются и передается дополнительная информация для упреждающей коррекции (Forward Error Correction — FEC). Благодаря этому система может восстанавливать биты, потерянные из-за шумов, помех и наложения сигналов. Упреждающая коррекция ошибок для данного уровня SNR на приемнике позволяет значительно улучшить BER (рис. 20.11.).

Улучшенные технологии сигнализации для уменьшения наложения сигналов

Есть несколько способов повышения надежности схем цифровой модуляции: квадратурно-амплитудная модуляция с обратной связью (decision feedback equalization — DFE), широкополосная передача с прямой последовательностью (direct sequence

spread spectrum — DSSS), мультиплексирование с разделением частот (frequency-division multiplexing — FDM) и ортогональное мультиплексирование с разделением по частоте (orthogonal frequency-division multiplexing — OFDM).

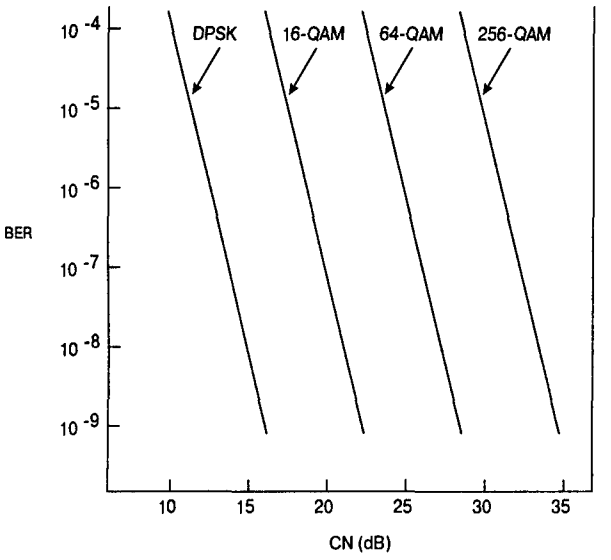


Рис. 20.10. Уравни ашибак при передаче для систем PSK и QAM

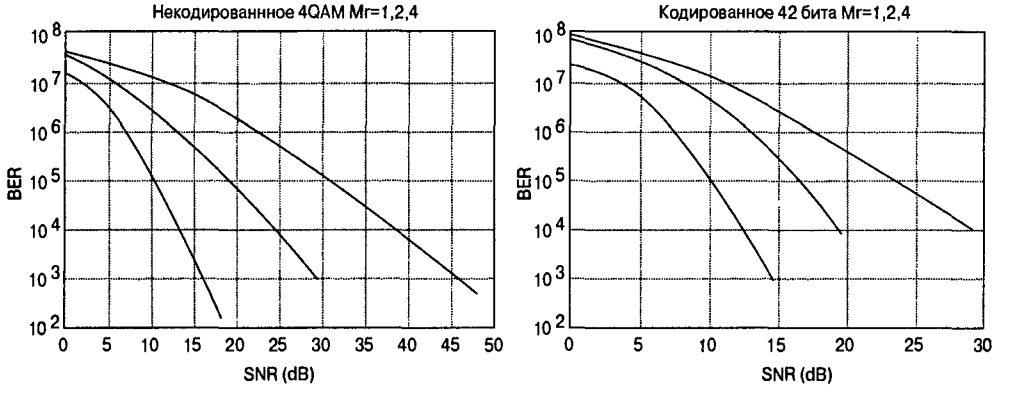


Рис. 20.11. График зависимасти BER ат отнашения сигнал/шум при использовании упреждающей коррекции и без нее

Квадратурно-амплитудная модуляция с обратной связью

Для уменьшения влияния межсимвольных помех (InterSymbol Interference — ISI), вызванных наложением сигналов, в беспроводных системах с квадратурно-амплитудной модуляцией используется обратная связь. Если время задержки распространения сигнала неодинаково, то эхо предыдущих символов искажает передаваемый

символ. Фильтр обратной связи (Decision Feedback Equalizer — DFE) восстанавливает принимаемый сигнал, фильтруя эхо. Из-за своей сложности схемы амплитудной модуляции с обратной связью не позволяют масштабирования при расширении полосы пропускания. Сложность фильтров DFE (количество отводов) пропорциональна времени задержки. Требуемое количество отводов пропорционально времени задержки (в секундах), умноженному на частоту.

Для беспроводной системы на основе квадратурно-амплитудной модуляции, передающей в полосе частот MMDS (канал шириной 6 МГц) при задержке 4 мс требуется 24 отвода. Для того чтобы выровнять систему с 24 отводами, необходима DFE-система с 72 отводами прямой и 24 отводами обратной связи. Кроме этого, сложность математического обеспечения для каждого отвода может привести к дальнейшему увеличению их количества. Поэтому сложность всей системы экспоненциально зависит от полосы пропускания несущего сигнала. На рис. 20.12 показана сравнительная сложность систем квадратурно-амплитудной модуляции с обратной связью и ортогонального мультиплексирования с разделением частот.

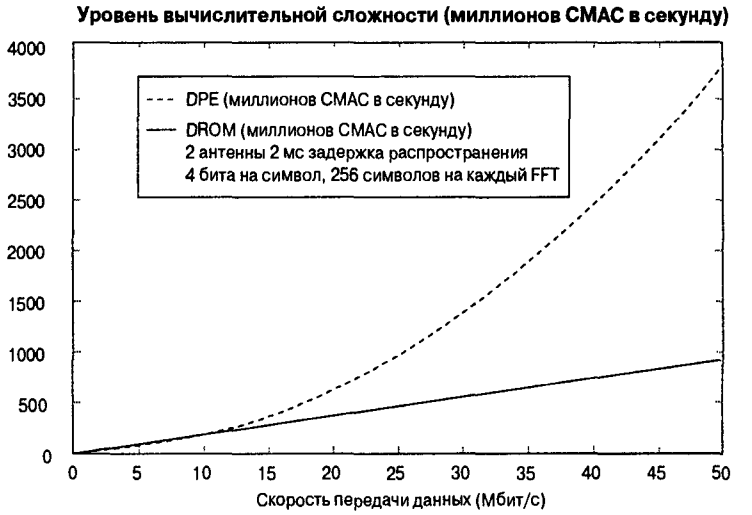


Рис. 20.12. Сравнительная вычислительная сложность систем квадратурно-амплитудной модуляции и ортогонального мультиплексирования с разделением частот

Широкополосная модуляция

Широкополосная модуляция представляет собой широко применяемый метод разбиения информации перед беспроводной передачей на управляемые фрагменты. Расширение спектра частот было изобретено киноактрисой Хедди Ламар (Heddy Lamar), которая до сих пор владеет патентом на данное изобретение и сравнительно недавно получила за это правительственную награду.

По существу, широкополосная модуляция сводится к разделению передаваемой информации по нескольким радиоканалам с разными частотами. Обычно таких частот около 70, и информация передается по всем или большинству из них, а затем на принимающем конце радиосистемы демодулируется или объединяется.

Используются два типа широкополосной модуляции:

- метод прямой последовательности (direct sequence spread spectrum — DSSS);
- метод частотных скачков (frequency hopping spread spectrum — FHSS).

Модуляция DSSS обеспечивает более высокие скорости передачи, вплоть до 11 Мбит/с. В системах FHSS достигаются скорости до 3 Мбит/с. Поскольку FHSS использует метод частотных скачков, в этом случае большее количество индивидуальных систем могут сосуществовать в одной области не создавая помех друг для друга. Однако системы, использующие метод прямой последовательности, более устойчивы по отношению к местным помехам. При одном и том же уровне мощности передатчика системы DSSS имеют меньший уровень мощности по спектральной плоскости. Это означает, что одна и та же мощность излучается в более широком диапазоне частот, что в целом ослабляет влияние помех от других локальных систем, использующих тот же диапазон частот.

Для пояснения сути широкополосной модуляции ее часто сравнивают с грузом, который на станции равномерно распределяется по нескольким поездам, отправляющимся в одно и то же время, а по прибытии поездов на место снова объединяется. При этом фрагменты часто дублируются, так что в случае искажения или потери при передаче избыточность, свойственная данной архитектуре, делает такой канал передачи данных более надежным.

Широкополосная модуляция методом прямой последовательности (DSSS) отличается невысокой сложностью и не требует выравнивания. Обычно используется узкополосный QPSK-сигнал, который умножается (или распространяется) на гораздо более широкий спектр частот. Требуемая ширина спектра рассчитывается по формуле 10 (SNR / 10) × скорость передачи узкополосного сигнала.

Например, если SNR составляет 20 дБ, то для получения приемлемого уровня BER общая ширина спектра, необходимая для передачи цифрового сигнала со скоростью 6 Мбит/с, составляет 600 МГц.

Таким образом, эта технология не очень эффективно использует полосу пропускания. Кроме того, скорость дискретизации на приемнике должна быть примерно в 100 раз больше скорости передачи данных. Следовательно, для рассматриваемой гипотетической системы скорость дискретизации должна составлять 600 миллионов квантов в секунду.

При использовании DSSS все "поезда" отправляются по очереди, начиная с "поезда" №1 и заканчивая "поездом" № N (количество "поездов" соответствует числу каналов в широкополосной системе). В архитектуре DSSS все " поезда" всегда отправляются в одном и том же порядке, хотя количество " железнодорожных путей" может составлять сотен и даже тысяч.

Множественный доступ с кодовым разделением каналов (Code Division Multiple Access — CDMA) обеспечивает возможность нескольких передач одновременно. Каждый поток данных умножается на псевдослучайный шумоподобный код (pseudorandom noise code — PN code). Все абоненты системы CDMA используют одну и ту же полосу частот. Каждый сигнал распространяется по нему поверх предыдущего и накладывается на него посредством распространения кода в одном и том же временном промежутке. Переданный сигнал восстанавливается с помощью PN-кода.

Данные, переданные другими абонентами, воспринимаются как "белый шум" и отбрасываются при приеме. Любой узкополосный шум в процессе восстановления сигнала размывается. Преимуществом технологии CMDA является возможность использования одной полосы частот для всех абонентов. Однако в системах с несколькими передатчиками

и приемниками необходим точный контроль мощности, чтобы ни один из абонентов не заглушал других на этой частоте. Такой контроль мощности является основным ограничением CMDA-архитектур.

Системы FHSS

В архитектуре широкополосной модуляции методом частотных скачков (Frequency Hopping Spread Spectrum — FHSS) " поезда" отправляются беспорядочно, а не один за другим, т.е. начиная с "поезда" №1 и заканачивая "поездом" N. В лучших системах FHSS "поезда", у которых по пути встретились помехи, не отправляются повторно до тех пор, пока помехи не ослабнут. Другими словами, некоторые каналы (частоты) не используются до уменьшения интенсивности помех.

Обычно помехи захватывают сразу несколько каналов. Поэтому системы DSSS имеют тенденцию терять больше данных от помех при передаче по последовательным каналам. Системы FHSS "перепрыгивают" между каналами в произвольном порядке. Лучшие из них позволяют определить наиболее зашумленные каналы и избегают их использования при передаче данных, что обеспечивает очень низкую частоту битовых ошибок. Выбор конкретного подхода определяется требованиями заказчика. В основном это ограничения по наложению сигналов и радиочастотное окружение.

Системы FDM

В системах с частотным уплотнением (Frequency-Division Multiplexing — FDM) существующая полоса частот делится на несколько подканалов, среди которых распределяются передаваемые данные. Поскольку каждый подканал обрабатывается независимо от других, вокруг него создается защитная частотная полоса. Наличие такой защитной полосы снижает эффективность использования частотного диапазона. В некоторых FDM-системах до 50% полосы пропускания тратится впустую. В большинстве FDM-систем каждый абонент "привязывается " к своему подканалу, из-за чего скорость передачи данных не может превышать емкости этого подканала. Даже если некоторые подканалы свободны, их полоса частот не может использоваться другими подканалами.

Системы OFDM

В системах ортогонального мультиплексирования с делением частоты (Orthogonal Frequency-Division Multiplexing — OFDM), как и в системах FDM, диапазон частот делится на несколько подканалов или тонов, по которым передаются данные (рис. 20.13). Однако в системах OFDM каждый тон рассматривается как ортогональный (независимый, несвязанный) по отношению к соседним, и, таким образом, не требующий защитной полосы частот. Поскольку системы OFDM требуют создания защитной полосы частот только вокруг всего диапазона, эффективность использования ими полосы частот значительно выше, чем в системах FDM. Так как системы OFDM состоят из большого количества узкополосных тонов, то узкополосная интерференция будет влиять только на небольшие фрагменты сигнала и почти не повлияет на остальные частотные составляющие.

В системах OFDM для уменьшения межсимвольных помех, вызванных задержкой распространения, используется пакетная передача данных. Данные передаются

пакетами, каждый из которых состоит из циклического префикса и следующих за ним символов данных. Например, сигнал OFDM на частоте 6 МГц состоит из 512 отдельных несущих частот (или тонов), каждая из которых переносит один символ QAM в одном пакете. Циклический префикс используется для поглощения переходных процессов, вызванных наложением сигнала от предыдущих пакетов, и состоит из дополнительных 64 символов.

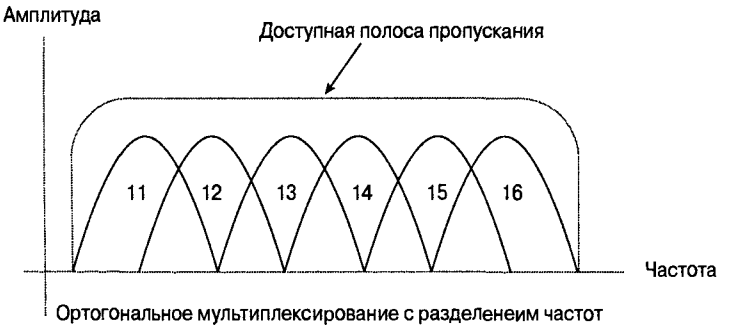


Рис. 20.13. Пример тонов OFDM

В каждом символьном периоде передается 576 символов, и только 512 из них являются символами QAM. Обычно к тому времени, когда закончится передача циклического префикса, полученная волна, представляющая собой комбинацию полезных сигналов, не является функцией каких-либо частей предыдущего пакета. Таким образом обеспечивается отсутствие межсимвольных помех. Длительность циклического префикса должна быть больше задержки многоканальных сигналов. Для системы с частотой 6 МГц период одного цикла составляет 0,16 мс. Следовательно, общая продолжительность циклического префикса равна 10,24 мс, что превышает ожидаемую задержку распространения, составляющую 4 мс.

Системы VOFDM

Кроме стандартных принципов OFDM, применяется пространственное разнесение, позволяющее повысить устойчивость системы к шумам, наложению сигналов и каналов. Такой принцип называется направленным ортогональным мультиплексированием с разделением частот (Vectored OFDM — VOFDM). Пространственное разнесение — распространенная технология повышения производительности в средах с наложением сигналов. Поскольку наложение сигналов является результатом нескольких отраженных сигналов, то оно зависит от места расположения принимающей антенны. Если в системе существует две и более антенны, то у каждой из них будет свое наложение сигналов. Каждый канал будет по-разному влиять на каждую антенну, так что несущие частоты, непригодные для одной антенны, могут оказаться подходящими для другой. Для этого антенны должны располагаться на расстоянии, которое превышает длину волны по меньшей мере в 10 раз.

Использование нескольких антенн позволяет значительно улучшить соотношение сигнал/шум. Обычно вторая антенна позволяет улучшить такой показатель приблизительно на 3 дБ в системах LOS и до 10 дБ в остальных средах.

Элементы единой сети

В единую сеть входят следующие общие элементы:

- абонентские сети;
- сети доступа;
- центральные сети;
- системы управления сетями;
- системы развертывания.

Абонентские сети

Под *абонентской сетью* понимается сеть для передачи речи, данных или видео, которая принадлежит или будет принадлежать абоненту. В рассматриваемом случае границей между сетью абонента и сетью доступа обычно можно считать канальные банки, мини-АТС, маршрутизаторы или устройства мультисервисного доступа.

Оборудование абонентских сетей получает сигналы от концентратора, преобразует их в данные, пригодные для обработки абонентами, а также передает данные обратно концентратору. Передатчик, приемник и антенна обычно помещаются в компактном внешнем модуле, который монтируется на крыше здания (rooftop unit — RTU) и размер которого не превышает спутниковой телеантенны. Такой модуль располагается на крыше здания, где помещается абонент, в пределах прямой видимости ближайшего концентратора LMDS. Для обеспечения максимальной производительности RF-канала при установке производится настройка модуля.

Внутренний модуль, модуль сетевого интерфейса (network interface unit — NIU), выполняет модуляцию, демодуляцию, служит внутренним проводным интерфейсом и обеспечивает промежуточную частоту для RTU. Поскольку оборудование абонента нуждается в разных интерфейсах, NIU должен обладать широким спектром как физических, так и логических интерфейсов.

Модули NIU разработаны для удовлетворения потребностей разных абонентов, нуждающихся в T1/E1, POTS, Ethernet и других стандартных сетевых интерфейсах. Эти интерфейсы обеспечиваются NIU при помощи плат межсетевого взаимодействия (interworking function cards — IWF cards). Благодаря различным типам IWF-плат модули NIU обеспечивают преобразование входных данных в ячейки ATM и снабжают их соответствующей сигнализацией. Широко распространены IWF-платы для 10BaseT, для эмуляции каналов T1/E1 и другие. В состав функций модуля NIU также входит передача промежуточной частоты на обрабатывающий элемент в модуле RTU.

Сети доступа

Под *сетью доступа* понимается сеть передачи и распространения, служащая мостом между абонентскими сетями и центральной сетью. В рамках данного обсуждения основным транспортным средством передачи от точки присутствия (POP) в сети доступа к абонентам является радио, а распространение данных между точками присутствия сети доступа осуществляется по беспроводному каналу или по волоконно-оптическому кабелю.

Базовые сети

Под базовыми или центральными сетями понимаются открытые или частные магистральные сети, которые используются операторами сетей доступа для соединения множества географически разнесенных точек присутствия и элементов сетей провайдеров открытых служб. В рамках данного обсуждения границей между сетью доступа и центральной сетью можно считать центральный коммутатор, который является расположенным в восходящем направлении получателем (upstream destination point) для множества ветвей и элементов сети доступа.

Управление сетью

Система управления сетью (Network Management System — NMS) и входящая в ее состав система операционной поддержки (Operational Support System — OSS) связывают в единое целое все элементы сети и обеспечивают выполнение основных задач по обработке информации. Полноценная система управления сетью представляет собой исключительно сложный комплекс программных платформ средней и высокой степени интеграции. В рамках настоящей главы можно считать, что данная система состоит из средств управления элементами на каждом уровне сети доступа; полное описание системы NMS выходит за рамки этой главы.

В идеальном случае NMS должна обеспечивать сквозное функционирование беспроводных и проводных элементов сети, включая магистраль и абонентские сети.

Система управления сетью обеспечивает управление службами, сетью и ее элементами независимо от производителя и технологии, в том числе:

- управление топологией;
- управление соединениями;
- управление событиями.

Более подробно функции системы управления сетью можно описать следующим образом.

- Создание интегрированной карты топологии с отображением узлов и каналов сети с системой предупреждений.
- Хранение описания физических (узлы и каналы) и логических (каналы и PVC) элементов топологии сети.
- Обслуживание абонентского интерфейса для сообщения о состоянии сети и абонентов.
- Сбор статистики о производительности PCR, SCR, MBS, CDVT, а также о состоянии сетей и каналов.
- Сбор SLA-информации о деятельности абонентов и предупреждение о нарушениях ими своих полномочий.
- Анализ предупреждений и вызвавших их причин.
- Имитация работы сети для выяснения, полностью ли устранена проблема.
- Документирование проблем, управление обслуживающим персоналом.
- Формирование отчетов о производительности на основании собранных статистических данных с точки зрения абонента и сети.

- Ведение счетов за пользование ATM-соединениями.
- Ведение защищенного от записи журнала учета соединений.

Развертывание

Как уже отмечалось, абоненты яруса 1 (tier 1) используют партнерскую экосистему развертывания Cisco. Развертывание систем с BTA, MTA и общенациональных систем требует следующих знаний и ресурсов:

- конструкции (башни, мачты);
- лицензирование (FCC и местные согласования частот, конструкции, доступа);
- инспекция местности (оценка радиочастотной обстановки);
- интеграция (выбор и приобретение различных RF-компонентов);
- развитие сети (заключение контрактов с заказчиками);
- финансирование (обеспечение финансирования проекта);
- установка (сборка компонентов);
- обеспечение (запасными частями)
- системы расчетов.

Беспроводные локальные сети WLAN

Данный раздел представляет собой введение в, вероятно, наиболее быстро развивающуюся технологию наших дней. Использование беспроводных локальных сетей (Wireless Local-Area Networks — WLAN) широко распространено на многих предприятиях.

Обзор WLAN

WLAN-сеть представляет собой систему передачи данных, предназначенную для того, чтобы предоставить традиционные LAN-службы с использованием беспроводного физического уровня. В сентябре 1999 года институт IEEE утвердил стандарт 802.11b, который является доминирующим WLAN-стандартом. Рабочая группа IEEE 802.11 продолжает работу над развитием данных стандартов.

Целью сетей стандарта 802.11b является предоставление мобильным пользователям производительности, сравнимой с проводными Ethernet-сетями, доступности и пропускной способности, а также обеспечение независимости от проводной инфраструктуры.

В табл. 20.4 приведено краткое сравнение WLAN-стандартов.

К табл. 20.4 необходимо сделать следующие замечания.

- 40- и 128-разрядный RC4 — алгоритмы шифрования данных.
- Для стандарта 802.11 дальность в 1000 футов приведена для наружных условий. Использование подобных радиосистем внутри помещений затруднено.
- Для стандарта 802.11 выходная мощность 1 Вт, разрешенная FCC, является базовой, хотя большинство устройств 802.11 имеют выходную мощность 100 МВт или меньше.

- Максимальное количество поддерживаемых устройств зависит от скорости передачи данных для каждого устройства.
- В сетях, использующих средства Cisco Aironet, применяется спецификация 802.11.

Таблица 20.4. Краткое описание стандартов Bluetooth и 802.11

	Bluetooth	802.11
Физический уровень	FHSS	FHSS, DSSS, IR (инфракрасное излучение)
Частота переходов (количество узлов в секунду, Hop frequency)	1600 узлов в секунду	2,5 узлов в секунду
Передаваемая мощность, мВт	100	1000
Скорость передачи данных, Мбит/с	1	11
Максимальное количество устройств	до 26	до 250
Безопасность	0-, 40- и 64-разрядное шифрование	от 40- до 128-разрядного RC4
Дальность (футов)	30-300	400 — в помещении, 1000 — при прямой видимости
Последняя версия	1.0	1.0

Несмотря на использование трех стандартов в США и еще двух в Европе (HyperLAN и HyperLAN2), Федеральная комиссия по связи (FCC) благосклонно относится к стандарту 802.11b, и существует тесная связь между FCC и институтом IEEE, который поддерживает данный стандарт.

В табл. 20.5 перечислены различные рабочие группы 802.11.

Таблица 20.5. Рабочие группы стандартов 802.11

Рабочая группа	Технологический стандарт
802.11a	54 Мбит/с, 5 ГГц, утвержден в 1999 году
802.11b	11 Мбит/с, 2,4 ГГц, утвержден в 1999 году
802.11d	Международный режим и регуляторные области
802.11e	Качество обслуживания
802.11f	Протокол Interaccess Point Protocol (IAPP)
802.11g	2,4 ГГц, высокие скорости передачи данных (более 20 Мбит/с)
802.11h	Динамическое выделение частоты и механизмы управления мощностью передачи
802.11i	Аутентификация и безопасность

Стандарт 802.11 состоит из нескольких компонентов и служб, которые взаимодействуют друг с другом для того, чтобы обеспечить прозрачную мобильность станций для вышестоящих уровней сетевого стека.

802.11 WLAN определяет два блока оборудования.

- **Беспроводная LAN-станция или клиент** — беспроводная станция представляет собой основной компонент беспроводной сети. Беспроводной LAN-станцией является любой блок оборудования, реализующий функции протокола 802.11 как на MAC-уровне, так и на физическом уровне и имеющий соединение с беспроводной средой передачи. Как правило, функции протокола 802.11 реализуются в программном и аппаратном обеспечении платы сетевого интерфейса (Network Interface Card — NIC). Беспроводной станцией может быть PC, мобильный или портативный компьютер.
- **Точка доступа (access point — AP)** — точка доступа функционирует как мост между беспроводной и проводной сетями. Точка доступа содержит беспроводной интерфейс (radio), интерфейс проводной сети (такой как Ethernet или ATM) и мостовое программное обеспечение. Точка доступа функционирует как базовая станция для беспроводной сети, обеспечивающая доступ к проводной сети для множества беспроводных станций. Если точка доступа присутствует, то через нее осуществляется весь обмен данными между беспроводными станциями или между беспроводной станцией и клиентом проводной сети.

WLAN-архитектура

Архитектура 802.11 включает в себя пять главных компонентов:

- набор базовых служб (Basic Service Set — BSS);
- независимый BSS;
- инфраструктурный BSS;
- систему распределения;
- расширенный набор служб.

Основным компонентом при построении беспроводной сети 802.11 является набор BSS. Он состоит из беспроводных станций, которые взаимодействуют друг с другом непосредственно или опосредованно.

Независимый BSS — базовая WLAN-топология, которая представляет собой множество станций, которые опознают друг друга и устанавливают равноправные соединения. Узлы взаимодействуют друг с другом непосредственно и, следовательно, должны быть в одном диапазоне.

Инфраструктурный BSS имеет дополнительную функцию точки доступа. Точка доступа позволяет клиентам, которые подключены к WLAN, получить возможность связи за пределами сети WLAN, если точка доступа подключена к проводной сети. При этом также удваивается радиус беспроводной сети, поскольку два устройства, подключенные на максимальном расстоянии, могут взаимодействовать через данную точку доступа.

Система распределения представляет собой проводную сеть. Она предоставляет точкам доступа возможность магистральной связи.

Расширенный набор служб представляет собой продукт совмещения нескольких BSS, в котором точки доступа могут передавать данные через распределенный BSS. Таким образом клиенты, связанные с соответствующими точками доступа, могут устанавливать сквозные соединения.

WLAN-технология уникальна на первом и втором уровнях модели OSI, т. е. на физическом и канальном уровнях. Физический уровень 802.11 — уровень между MAC-уровнем и беспроводной средой передачи данных, где передаются и принимаются фреймы. Физический уровень обеспечивает три функции.

Физический уровень обеспечивает интерфейс для обмена фреймами с MAC-уровнем при передаче и приеме данных. На физическом уровне используется сигнальная несущая (signal carrier) и модуляция разброса спектра (spread spectrum modulation) для передачи фреймов данных через беспроводную среду. Физический уровень предоставляет MAC-уровню контроль несущей для проверки активности.

В стандарте 802.11 предусмотрены следующие физические уровни:

- **инфракрасный** — используется инфракрасное излучение для передачи двоичных данных либо со скоростью 1 Мбит/с (базовая скорость доступа), либо 2 Мбит/с (повышенная скорость доступа).
- **FHSS** — для передачи данных на скоростях 1 и 2 Мбит/с используются RF-сигналы 2,4 ГГц.
- **DSSS** — для передачи данных на скоростях 1, 2, 5,5 и 11 Мбит/с используются RF-сигналы 2,4 ГГц.

MAC-уровень 802.11 обеспечивает надежную доставку данных для вышестоящих уровней через среду беспроводного физического уровня. Доставка данных основывается на негарантированной асинхронной доставке (best-effort) без установки соединения. Ниже перечислены основные характеристики такой доставки.

- Успешная доставка не гарантируется.
- MAC-уровень 802.11 также предоставляет метод контролируемого доступа к совместно используемой беспроводной середе передачи посредством CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance). Методика CSMA/CA подобна методике обнаружения коллизий, которая используется в локальных сетях Ethernet 802.3.
- MAC-уровень также обеспечивает защиту передаваемых данных с помощью служб обеспечения безопасности и секретности. Безопасность обеспечивается с помощью аутентификации и шифрования.

В качестве протокола безопасности стандарта 802.11 определен протокол WEP (Wired Equivalent Privacy). Его целью является достижение уровня безопасности и секретности существующего в проводных сетях. RF-соединения открыты, поэтому существует возможность вмешательства в передачу данных. WEP — функция, применяемая для шифрования данных между клиентом и точкой доступа. Минимальной реализацией является использование статического 40- или 128-разрядного ключа RC4. В недавнем прошлом была выявлена уязвимость данного метод шифрования. Данная атака описана в официальных документах, опубликованных в Internet. Эта уязвимость уменьшена в реализациях Cisco с помощью более надежных критериев безопасности. Крайне важно, чтобы при любом проектировании сети учитывалась оценка сетевой безопасности во WLAN-среде.

Службы распределения

Система распределения должна иметь возможность предоставлять определенные службы клиентам WLAN. Данные службы распределения, как правило, предоставляются точками доступа. Службы распределения включают в себя:

- службу установки связи;
- службу разъединения;
- службу переустановки связи;
- службу распределения;
- службу интеграции.

Служба установки связи (association service) ответственна за логические соединения между точкой доступа и клиентом. Каждый клиент должен связаться с точкой доступа, чтобы получить возможность отправлять данные через данную точку доступа в систему распределения. Соединение необходимо для того, чтобы система распределения получила информацию о том, куда отправлять данные для определенного клиента. Клиент обычно формирует службу связи только один раз, когда станция входит в BSS. Каждый клиент может быть связан с одной точкой доступа, но точка доступа может быть связана с несколькими станциями.

Служба разъединения (disassociation service) разрывает связь между точкой доступа и клиентом, когда последний более не нуждается в службах, предоставляемых системой распределения. Если станция отсоединилась, то для обмена данными с точкой доступа она должна инициировать новую связь. Точка доступа может заставить клиента разорвать связь из-за ресурсных ограничений, из-за отключения точки доступа или из-за того, что точка доступа более не доступна. Клиенты разрывают связь при отключении от сети. Разъединение представляет собой уведомление и может быть инициировано любой из связанных сторон. Ни одна из сторон не может отклонить разрыв связи.

Переустановка связи (reassociation) позволяет клиенту изменить его текущую связь с точкой доступа, например, когда клиенту требуется вновь установить связь с той точкой доступа, с которой он был связан ранее. Служба переустановки связи подобна службе установки связи, но включает в себя информацию о точке доступа, с которой мобильная станция была связана ранее.

Необходимо отметить, что клиенту требуется служба переустановки связи, когда он перемещается через ESS, теряет контакт со связанной точкой доступа и пытается связаться с новой точкой доступа. При переустановке связи клиент предоставляет той точке доступа, с которой он соединяется, информацию о точке доступа, с которой он разрывает связь. Новая точка доступа контактирует с предыдущей точкой доступа, чтобы получить данные, которые, возможно, понадобится передавать клиенту, а также другую информацию относительно новой связи. Переустановку связи всегда инициирует клиент.

Основной службой, которую использует клиент 802.11, является служба распределения. Клиент использует данную службу каждый раз, когда отправляет MAC-фреймы канального уровня через систему распределения. Система распределения предоставляет клиенту необходимую информацию для того, чтобы он мог отправлять свои MAC-фреймы соответствующему BSS-получателю. Три данные службы связи — установки, переустановки и разъединения — предоставляют необходимую информацию для работы службы распределения. В системе распределения не обязательно задействованы какие-либо дополнительные функции за рамками служб связи, однако клиент должен быть связан с точкой доступа, прежде чем служба распределения сможет успешно передавать фреймы.

Служба интеграции соединяет сети WLAN 802.11 с другими локальными сетями, беспроводными или проводными. Службу интеграции осуществляет главный общедоступный узел сети (network portal). Эта служба предоставляет возможность связи между данными локальными сетями, имеющими уникальные функции.

Cisco Systems предоставляет широкий диапазон аппаратного обеспечения, которое обеспечивает функциональные и масштабируемые беспроводные LAN-решения. В настоящее время доступны решения на базе спецификаций 802.11a и 802.11b. Корпорация предлагает точки доступа, мосты, антенны, клиентские адаптеры, а также OSS- и BSS-решения.

Ниже приводится перечень WLAN-устройств, входящих в семейство Cisco Aironet.

- **Cisco Aironet 1200** — группа устройств данной серии является флагманом серии Aironet и стандартом для высокопроизводительных, безопасных, управляемых, надежных WLAN-сетей следующего поколения. Устройства данной серии тесно интегрируются с существующей сетью как беспроводное перекрытие или создают автономные полностью беспроводные сети, обеспечивая быстрое и эффективное использование мобильных станций. Модульная и расширяемая платформа позволяет сохранить текущие и будущие инвестиции в инфраструктуру. Согласующиеся со стандартами IEEE 802.11a и 802.11b устройства серии Cisco Aironet 1200 допускают как одно- так и двух-полосную конфигурацию, а также масштабируемость для изменения конфигурации по мере развития требований и технологии. Устройства данной серии создают беспроводную инфраструктуру, которая обеспечивает для пользователей максимальную мобильность и гибкость, предоставляя возможность постоянной связи со всеми сетевыми ресурсами из практически любой точки, где реализован беспроводной доступ.
- **Cisco Aironet 1100** — точки доступа данной серии предоставляют безопасное, доступное по цене и простое в использовании WLAN-решение, которое комбинирует мобильность и гибкость с функциями масштаба предприятия, которые необходимы профессионалам, поддерживающим сеть. Используя преимущества безопасности беспроводных устройств Cisco для достижения более строгой безопасности предприятия, а также простое в использовании и знакомое многим программное обеспечение Cisco IOS, точки доступа серии Cisco Aironet 1100 обеспечивают управляемость, высокую производительность, защиту инвестиций и масштабируемость в эффективном пакете с экономной полной стоимостью владения. В данной серии представлен единый, расширяемый беспроводной интерфейс 802.11, интегрированные вибраторные антенны с симметричным разнесением, а также передовую систему монтирования, обеспечивающую простую установку в различных местностях и с разной ориентацией.

Внимание!

Приведенное выше описание продуктов Aironet взято с web-сайта корпорации Cisco Systems. Более подробная информация представлена на странице www.cisco.com/en/US/products/hw/wireless/index.html.

Резюме

Базовое понимание концепций беспроводной связи является необходимым для принятия верных решений при разработке беспроводных сетей. Хорошее понимание основ полезно при попытке разобраться в конструкции существующей сети, в которой понадобится устранять неисправности. При определении режима работы сети более

высокого уровня очень важным является влияние низкоуровневой сети и ее отличительных особенностей.

При проектировании новой сети важно определить соответствующий спектр, а также определить возможность данной сети сосуществовать с другими беспроводными коммуникациями. Для нахождения причин низкой производительности в беспроводной сети важным является понимание используемого спектра.

Другим критически важным проектным решением является выбор аппаратного обеспечения. Антенна, кабель и аппаратное обеспечение являются частями конструкции, и разработчику необходимо тщательно выбирать корректные компоненты в соответствии с целями проектируемой сети.

Ограничения NLOS-соединений и доступные методы их преодоления являются критически важными при выборе беспроводной технологии. Методы модуляции, схемы более эффективного использования ограниченного спектра и предотвращения помех являются теми элементами, которые необходимо учесть в конструкции.

При разработке единой сети необходимо идентифицировать множество компонентов. Ниже перечислены основные преимущества внедрения беспроводных систем независимо от выбора оборудования или технологии.

- **Они дополняют набор технологий доступа.** Потребители обычно используют несколько технологий доступа и для обслуживания различных частей своей сети, и во время плановой перестройки сетей. Беспроводные технологии обеспечивают комплексный доступ для работы с существующими технологиями — коммутируемыми, кабельными и DSL-соединениями.
- **Они применимы там, где нельзя проложить ни провода, ни оптическое волокно.** По своей природе беспроводные соединения не требуют прокладки кабелей для передачи данных, речи или видео. Поэтому беспроводная система способна передавать информацию через географические области, недоступные с точки зрения расстояний, стоимости или времени. Это также позволяет избежать многих проблем, связанных с расположением ILEC.

Хотя за доступ к возвышающимся точкам, таким как мачты, башни и крыши высотных зданий, обычно приходится платить, эти расходы вместе со связанной с ними логистикой зачастую едва сравнимы с затратами на рытье траншей и прокладку кабеля.

- **Сокращается срок окупаемости.** Компании, использующие беспроводные решения, могут начать получать прибыль быстрее, чем в случае использования других технологий, потому что сборка и подключение беспроводной системы занимает не более 2–3 часов.
- Эта технология позволяет провайдерам предоставлять доступ, не ожидая завершения закладки кабеля или получения доступа от вышестоящего провайдера.
- **Обеспечивается возможность расширения полосы пропускания.** Обычно беспроводные системы составляют конкуренцию и дополняют существующие системы широкополосного доступа. Беспроводные технологии играют главную роль при расширении области доступа, обеспечиваемой проводным кабелем, оптоволоконым кабелем и DSL, причем быстро и надежно. Кроме того, они являются конкурентоспособной альтернативой широкополосным проводным линиям связи, а также обеспечивают доступ в районах, где прокладка кабеля невозможна.

Независимо от провайдера фундаментальные элементы беспроводной системы практически остаются неизменными:

- данные (локальная сеть);
- граница (маршрутизатор доступа);
- среда передачи DSP;
- среда передачи RF (коаксиальный кабель, модулятор/демодулятор, антенна);
- программное обеспечение для управления RF.

Подобно любым средам и технологиям доступа, беспроводные системы имеют свои преимущества и недостатки. Их достоинства заключаются в следующем:

- Их внедрение обходится гораздо дешевле, чем прокладка наружного кабеля.
- Их внедрение требует гораздо меньше времени — канал можно подготовить в течение нескольких часов.
- Беспроводную связь можно обеспечить там, куда нельзя проложить кабель, например, в горные и недоступные районы.
- Распространение этих систем связано с меньшей бюрократической волокитой — достаточно иметь право на установку оборудования на крыше или на мачте.
- Беспроводным системам присуща высокая внутренняя безопасность, которую можно усилить дополнительно.
- Беспроводные системы обеспечивают мобильность полосы пропускания и портативность, недоступную для кабельных систем.

Контрольные вопросы

1. Каковы главные компоненты беспроводной системы?
2. Чему равна длина волны для сигнала с частотой 850 МГц?
3. Какие факторы следует учесть при выборе канала передачи?
4. Каковы два базовых типа антенны?
5. Что означает аббревиатура EIRP?
6. Что называется зоной Френеля?
7. Что называется наложением сигналов?
8. Каковы пять основных модулей архитектуры сети 802.11?
9. Какие пять служб предлагает служба распределения?
10. Каковы четыре основных преимущества использования беспроводных технологий?

Дополнительные источники

- http://home.earthlink.net/~aareiter/introto.htm (Руководство по беспроводному Internet)
- http://http.cs.berkeley.edu/~gribble/cs294-7_wireless/summaries/index.html (Курс UC Berkeley по беспроводной связи)

- http://winwww.rutgers.edu/pub/Links.html (беспроводные каналы)
- www.airlinx.com/products.htm (Список RF-продуктов)
- www.allnetdevices.com/news/index.html (Новости allNetDevices)
- www.americasnetwork.com/issues/97issues/971001/100197_futurebb.html (История развития широкополосных сетей)
- www.broadbandforum.com (Форум, посвященный кабельным широкополосным сетям)
- www.businesswire.com/cnn/wcii.htm (Пресс-релизы WinStar)
- www.comet.columbia.edu/~angin/e6950/coolsites.html (Web-узел, посвященный беспроводным технологиям)
- www.ctimag.com/ (Новости CTI)
- www.data.com/tutorials/web_connection.html (Руководство по беспроводным Web-технологиям)
- www.dectweb.com/sitemap.htm (DECTweb)
- www.dnspublishing.com/rc/rcindex.cfm (Web-узел Reciprocal Compensation)
- www.ericsson.com/BN/dect2.html (Ericsson DECT)
- www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/recent.html (Носители FCC)
- www.beropticsonline.com (Fiberoptics Online)
- www.gbmarks.com/wireless.htm (Ссылки Goodman's Wireless Telecomm)
- www.globalwirelessnews.com/ (Новости RCR Global Wireless)
- www.herring.com/mag/issue48/comm.html (Планы широкополосных сетей Ericsson)
- www.hometoys.com/htinews/oct99/articles/allied/allied.htm
- www.internettelephony.com (Internet-телефония)
- www.internettelephony.com/archive/featurearchive/7.06.98.html (Обзор FSAN)
- www.it.kth.se/edu/gru/Fingerinfo/telesys..nger/Mobile.VT96/DECT.html (DECT)
- www.itu.int/imt/2-radio-dev/proposals/index.html (Мировые радиостандарты ITU)
- www.mobilecomputing.com/ (Mobile Computing & Communications)
- www.phonezone.com/tutorial/nextgen.htm (Телефонные системы следующего поколения)
- http://www-star.stanford.edu/~osama/links.html (Однокристальное радио с частотой 2,4 ГГц)
- www.tek.com/Measurement/App_Notes/ap-Wireless/welcome.html (Цифровая модуляция в беспроводных системах)
- www.telecomweb.com/ct/ (Communications Today)
- www.ti.com/sc/data/wireless/panos1.pdf (Обзор беспроводных систем и технологий)
- www.ti.com/sc/docs/wireless/cellterm.htm (Толковый словарь беспроводных технологий)
- www.tiap.org (Руководство по развивающимся беспроводным службам)

- www.tr.com/ (Telecommunications Reports)
- www.trio.ca/annual/thrusts/mobsat.htm (Исследования в области беспроводных систем и мобильной связи в Онтарио, Канада)
- www.wapforum.org/what/technical.htm (Форум специалистов по WAP)
- www.webproforum.com/wpf_wireless.html (Учебные пособия по беспроводным технологиям)
- www.wirelessdata.org (Форум по беспроводным технологиям)
- www.wirelessdata.org/news/currenttxt.asp (Последние новости)
- www.wirelessdesignonline.com (Wireless Design Online)
- www.wirelessweek.com/industry/indtoc.htm (Wireless Week, информация и статистика отрасли)
- www.wow-com.com/index.cfm (Web-страница о беспроводной связи CTIA: World Of Wireless)
- www.wow-com.com/wirelesssurvey/1298datasurvey.pdf (Обзор беспроводных технологий в США, 1998г.)
- www.zdnet.com/anchordesk/story/story_1384.html (Обзор технологий доступа от ZD Anchordesk)
- www.zdnet.com/intweek/print/971013/158897.html (Обзор технологий доступа, октябрь 1997)

Акты и постановления

- www.broadband-guide.com/lw/reg/index.html (Публикации Pennwell)
- www.commnow.com/3rd_Generation.html (Статьи семинара по TR-45 на IMT-2000)
- www.fcc.gov/bandwidth/ (Web-страница FCC)
- www.itu.ch/imt/ (International Mobile Telecommunications-2000 [ITU R/T Initiative])
- www.ntia.doc.gov/osmhome/allochrt.html (U.S. spectrum chart)

WLL

- www.analysys.co.uk/publish/registered/locloop/default.htm#contents (LL)
- www.globaltelephony.com/archives/GT598/GT598cover.html (Функции WLL)
- www.internettelephony.com/content/html/focus/feature1.html (WLL следующего поколения, февраль 1998)
- www.isir.com/wireless/ (Мир WLL)
- www.ntia.doc.gov/forums/wireless/index.html (Форум WLL)
- www.verticom.com/cieee_1/index.htm (Steve Goldberg's IEEE talk on wireless LL)
- www.wavespan.com/solutions/ultraman.shtml (Wavespan Stratum 100)

LMDS/MMDS

- http://businesstech.com/telecom/btfreetelecom9902.html (История MMDS)
- http://grouper.ieee.org/groups/802/16/ (IEEE 802.16 BroadBand Fixed Wireless)
- http://nwest.nist.gov/ (деятельность Click News в сфере текущих стандартов)
- http://nwest.nist.gov/tutorial_ets.pdf (Брифинг, посвященный LMDS)
- www.americasnetwork.com/issues/98issues/980801/980801_lmds.html
- www.americasnetwork.com/issues/99supplements/990601lmds/990601_toc.htm
- www.cabledatacomnews.com/wireless/cmic12.html (North American MMDS)
- www.fcc.gov/Bureaus/Wireless/Factsheets/lmds.html (Отчеты FCC о результатах аукционов LMDS)
- www.nmcfast.com (Партнерство IBM и NewMedia в области MMDS)
- www.teledotcom.com/1097/features/tdc1097telcos.html (BellSouth MMDS)
- www.WCAI.com/index.htm (Web-страница WCA)
- www.webproforum.com/nortel4/ (Учебное пособие Nortel по LMDS)
- www.zdnet.com/intweek/print/970630/inwk0009.html (Широкополосные беспроводные системы)

Беспроводные системы

- www.broadband-guide.com/wi/techupdate/techupjf98.html (Беспроводные внутренние телефонные системы)

Спутниковая связь

- http://sat-nd.com/news/ (Новости спутниковой связи)
- http://tcpsat.grc.nasa.gov/tcpsat/ (TCP через спутник)
- www.data.com/issue/990707/satellite.html (Спутниковые каналы Internet)
- www.ee.surrey.ac.uk/Personal/L.Wood/constellations/ (Орбиты)
- www.herring.com/mag/issue48/space.html (Loral portrait)
- www.iridium.com/index.html (Web-страница Iridium)
- www.msua.org/mobile.htm (Ассоциация пользователей мобильной спутниковой связи)
- www.project77.com Project77 (Прайс-лист Iridium)
- www.satphone.com/ (Обзор программ)
- www.satphone.net (Iridium service provider satellite warehouse)
- www.skybridgesatellite.com/ (SkyBridge)
- www.skyreport.com/ (Отчеты об исследованиях в области спутниковой связи)
- www.spotbeam.com/links.htm (Спутниковые каналы Internet)

- www.spotbeam.com/mansum.htm (Обзор GEO)
- www.spotbeam.com/mansum99.htm (Обзор Internet и ISP)
- www.techweb.com/se/directlink.cgi?NWC19980315S0011 (безопасность спутниковой связи)
- www.techweb.com/se/directlink.cgi?NWC19980315S0017 (broadband Ka satellites)
- www.wizard.net/~vvaughn/sat.htm (Сравнение спутниковых систем передачи речи)

Модуляция

- http://diva.eecs.berkeley.edu/~linnartz/MCCDMA.html (Термины OFDM)
- http://propagation.jpl.nasa.gov/propdb/HELP/CLOUD.HTM (Влияние облачности и осадков)
- http://sss-mag.com/favlinks/index.html (Много ссылок на тему модуляции)
- http://wireless.stanford.edu/research.html (Исследования Станфордского университета в области беспроводной связи)
- www.catv.org/modem/technical/ofdm.html (OFDM, the next upstream modulation)
- www.ee.mtu.edu/courses/ee465/groupe/index.html (класс CDMA)
- www.gr.ssr.upm.es/~ana/ofdm_links.htm (OFDM sites)
- www.sm.luth.se/csee/sp/projects/ofdm/ofdm.html (Описание OFDM)

Интерфейсы

- http://cx667314-a.chnd1.az.home.com/1394Informer/990800.htm 1394 (Новости)
- http://skipstone.com/compcon.html (Обзор IEEE 1394)
- http://www-europe.cisco.com/warp/public/459/8.html (HSSI)
- www.mfsdatanet.com/mfs-international/hssi.html (HSSI)
- www.sdlcomm.com/ (HSSI PCI)

Глоссарий

- **Смежный канал.** Канал, который по частоте примыкает к данному каналу сверху или снизу.
- **Амплитуда.** Высота, или сила волны, которая обычно представляется в виде графика вдоль оси x.
- **Аналоговый сигнал.** Представление информации в виде постоянно изменяющейся физической величины, например напряжения. Поскольку аналоговый сигнал постоянно изменяется во времени и пространстве, он может принимать неопределенное количество значений, в отличие от цифрового сигнала, который передается с помощью волн прямоугольной формы и принимает ограниченное количество дискретных значений.

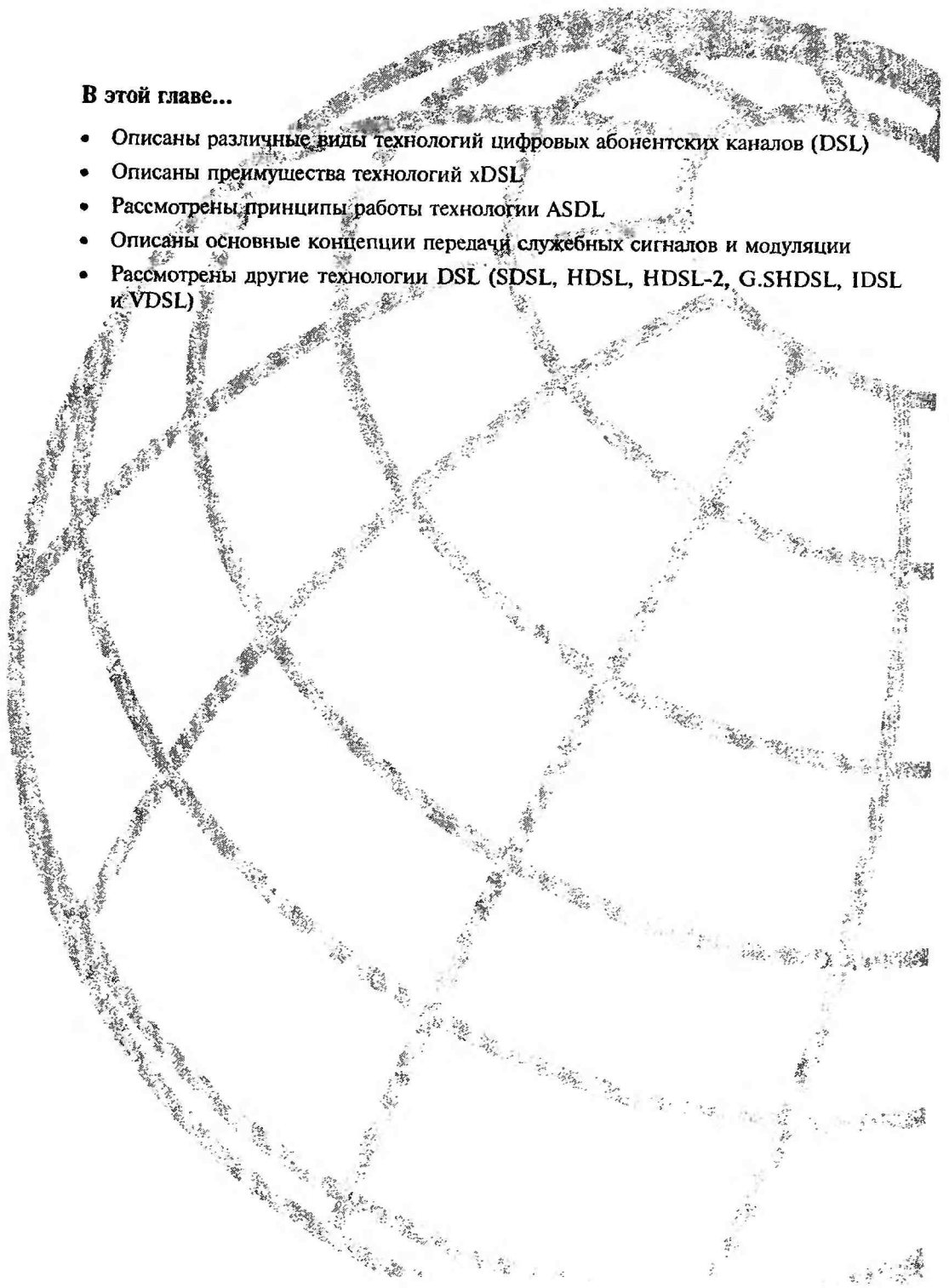
- **Антенна.** Устройство для передачи и приема радиоволн (Radio Frequency — RF). Антенны разрабатываются для определенных тесно связанных между собой частот и имеют различную конструкцию. Антенна для частоты 2,5 ГГц (диапазон MMDS) не будет работать на частоте 28 ГГц (диапазон LMDS).
- **Коэффициент усиления антенны.** Эффективность данной антенны по отношению к гипотетической антенне, называемой изотропным излучателем (термин *излучатель* рассматривается как синоним слова *антенна*). Антенна наиболее эффективна на определенной частоте и в определенном направлении.
- **Полоса частот.** Диапазон частот для передачи сигнала. Единицей измерения частоты является герц (Гц). Например, для передачи человеческого голоса достаточно полосы частот приблизительно в 7 кГц, а передача данных требует полосы частот около 50 кГц. Второе значение данного термина — фактическая ширина или величина спектра, используемого беспроводной системой.
- **Широкополосная передача.** Обычно радиосистемы называются широкополосными, если их скорость передачи данных выше 1,5 Мбит/с. Остальные системы называют узкополосными.
- **Широковещательная передача.** В отличие от направленной передачи, сигнал посылается одновременно нескольким получателям, т.е. в нескольких направлениях.
- **BTA** (Basic Trading Area). Базовая территория обслуживания — территория, в пределах которой действует лицензия на использование радиочастоты; термин BTA введен в обиход компанией Rand McNally и определяется как перечень округов. В описании Rand McNally он использовался для точного описания географической области, подлежащей лицензированию в FCC.
- **CDMA** (Code Division Multiple Access). Множественный доступ с кодовым разделением. Технология передачи, позволяющая нескольким абонентам использовать один и тот же частотный диапазон. В результате система может передавать большой объем данных в узком диапазоне частот. Передатчики используют предварительно заданный набор не прилегающих друг к другу частотных диапазонов. Приемник собирает различные блоки данных из разных частот в согласованный поток данных. Являясь частью радиосистемы, приемник обладает информацией о последовательности используемых для передачи частот. Важным аспектом этой схемы является фильтрация приемником всех сигналов, кроме предназначенных для данной передачи.
- **Канал.** Коммуникационный тракт, достаточно широкий для обеспечения одной RF-передачи.
- **Коаксиальный кабель.** Тип кабеля с центральным проводником, который окружен экраном.
- **Конвертор.** Радиосистемы используют две основные частоты: одна (несущая) — для радиоэфира, а вторая (промежуточная) — для передачи данных между устройствами Cisco и антенной. Преобразование этих частот осуществляется конвертором, который также называют повышающим конвертером, или трансвертером. Промежуточные частоты подразделяются на относительно высокие и относительно низкие частоты, которые используются для приема и получения данных при радиообмене между антенной и устройствами Cisco.

- **дБ.** Децибел — единица измерения относительной мощности. Используется при измерении шумов или потерь. Эта единица измерения представляет собой десятичный логарифм отношения измеряемых величин, которые обычно измеряются в ваттах. дБ является не абсолютной единицей, а, скорее, показателем потери или приращения между двумя устройствами. Например, потери в -3 дБ соответствуют 50% потерь мощности; усиление в +3 дБ говорит об удвоении мощности. Полезно знать, что 10 дБ соответствует усилению (или ослаблению) в 10 раз. Аналогично, потери в 20 дБ говорят об усилении (или ослаблении) в 100 раз, а 30 дБ — в 1000 раз. Поскольку антенны и прочие радиосистемы, как правило, ослабляют или усиливают сигнал не меньше чем в 4 раза, для них удобнее использовать децибелы.
- **dBi.** Децибел по отношению к гипотетической изотропной антенне (индекс i), которая теоретически идеальна в понятиях симметричной направленности. Реальная антенна никогда не создает даже номинальной симметричной направленности, однако понятие изотропной антенны удобно использовать для конструировании систем.
- **дБм.** Децибел на милливатт; 0 дБм —мощность в 1 мВт на частоте 1 КГц при сопротивлении в 600 Ом.
- **дБВт.** Децибел на ватт.
- **Демодулятор.** Устройство для сборки сигналов после их получения антенной. Обычно демодулятор является первым крупным устройством в принимающей системе после антенны и на блочной диаграмме располагается перед различными устройствами Cisco. Соответствующее устройство на передающей стороне называют модулятором.
- **EIRP** (Effective Isotropic Radiated Power). Эффективная мощность изотропного излучателя. Показывает эффективность антенны в данном направлении по отношению к гипотетической (изотропной) антенне; единица измерения — Вт или дБВт. EIRP представляет собой сумму мощности, посылаемой на антенну, и усиления антенны.
- **Электромагнитный спектр.** Полный спектр электромагнитных (а также магнитных) частот, подмножество которых используется в коммерческих радиосистемах. Коммерческие системы обычно классифицируются по используемому диапазону частот (MF, HF, VHF, SHF и EHF). В оборонных системах обычно применяются частоты, лежащие за пределами этих диапазонов.
- **Фиксированные беспроводные сети.** Один из типов беспроводных сетей Cisco, в которых ни приемник, ни передатчик не являются мобильными. Фиксированные сети Cisco представляют собой широкополосные системы со скоростью передачи свыше 1,5 Мбит/с.
- **Площадь покрытия** (footprint). Географическая территория, в пределах которой действует разрешение на передачу радиосигнала.
- **Повторное использование частоты.** Одна из фундаментальных идей, лежащих в основе коммерческих беспроводных систем. Заключается в разбиении зоны радиоизлучения (ячейки) на сегменты (например, в сетях Cisco ячейка делится на три равноценных сегмента). Каждый из сегментов использует частоту, значительно отличающуюся от частот соседних сегментов (во избежание взаимных

помех). Одинаковые частоты используются только в удаленных друг от друга ячейках. Такая практика позволяет провайдеру мобильной связи, используя одну и ту же лицензию, обслуживать в несколько раз больше абонентов.

- **Коэффициент усиления.** Отношение амплитуды выходного сигнала к амплитуде входного. Обычно выражается в децибелах. Чем больше коэффициент усиления, тем лучше антенна принимает и передает сигнал, однако шумы при этом тоже усиливаются.
- **Лицензия.** Приобретаемое право, разрешающее передачу радиоволн в пределах BTA (базовой территории обслуживания). Как правило, выдается на десять лет. В лицензии четко определены параметры радиосистемы и правила ее использования. Обычно лицензии выдаются FCC на тендерной основе. FCC выдает лицензии для обеспечения максимальной конкуренции в условиях свободного рынка (хотя при рассмотрении условий тендеров, проводимых FCC, это не совсем очевидно) и повышения эффективности использования радиоресурса.
- **LMDS** (Local Multipoint Distribution Service). Местная многоабонентская служба распределения. Относительно ограниченная лицензия на широковещательную передачу речи, видео и цифровых данных. Чаще всего предоставляются две лицензии, каждая на три частоты, с различными зонами BTA. Эти лицензии также называют лицензиями блока A и блока B. Лицензии блока A действуют на частотах от 27,5 до 28,35 ГГц, от 29,10 до 29,25 ГГц и от 31,075 до 31,225 ГГц, что образует полосу частот 1,159 МГц. Лицензии блока B действуют на частотах от 31,00 до 31,075 ГГц и от 31,225 до 31,300 ГГц всего на полосу частот 150 МГц. Максимальная дальность передачи систем LMDS обычно достигает примерно 3 миль, в то время как для систем MMDS она составляет около 25 миль. Это различие в дальности обусловлено, прежде всего, физическими законами и ограничением выходной мощности нормами FCC.
- **LOS** (Line Of Sight). Прямая видимость. Подразумевает отсутствие препятствий на прямой линии передатчик-приемник. Данное обстоятельство существенно для развертывания продуктов семейства LMDS. Антонимом термина LOS является отсутствие прямой видимости или непрямая видимость (non-line-of-sight — NLOS).
- **MMDS** (Multichannel Multipoint Distribution Service). Многоканальная многоабонентская служба распределения. Заключается в организации до 33 дискретных каналов, передача по которым осуществляется в псевдослучайной последовательности. Комиссия FCC выделяет два диапазона частот для каждой BTA — от 2,15 до 2,161 ГГц и от 2,5 до 2,686 ГГц.
- **Мобильные беспроводные системы.** Cisco не разрабатывает мобильных беспроводных компонентов, однако предлагает магистральные устройства (например, GGSN) для мобильных беспроводных систем.
- **NLOS** (Non-Line-Of-Sight). Непрямая видимость. Также называется трактом или магистралью с помехами.
- **Параболическая антенна.** Антенна в форме тарелки, которая хорошо фокусирует посылаемые радиоволны. Такие антенны обеспечивают большой коэффициент усиления и высокую эффективность. Преимущественно используются в системах Cisco LMDS, U-NII и MMDS, но предназначены не только для этих систем.

- **Потери при передаче.** Энергия, которая теряется при передаче радиоволн в пространстве. Потери при передаче обусловлены эффектом ослабления сигнала атмосферой. Некоторые частоты (сверхвысокие, не используемые в коммерческих системах) полностью блокируются атмосферой.
- **Многоточечная система** (Point-To-MultiPoint — P2MP). Обычно подразумевает связь между несколькими приемопередатчиками и центральной точкой. В системах P2MP Cisco ячейка делится на три сегмента для обеспечения повторного использования частот. Cisco предлагает следующие типы многоточечных систем: MMDS, U-NII и LMDS.
- **Система "точка-точка"** (Point-To-Point — P2P). Обеспечивает большую полосу пропускания, чем технология P2MP, поскольку отсутствует необходимость распределения канала передачи данных и каждому передатчику соответствует только один приемник. Cisco предлагает следующие типы систем "точка-точка": MMDS, U-NII и LMDS.
- **Радиочастота** (Radio Frequency — RF). Обычно этот термин применяют к системам с частотами ниже 300 ГГц.
- **TDMA** (Time-Division Multiple Access). Множественный доступ с разделением времени. Технология, позволяющая разбивать передаваемые данные на временные слоты и, таким образом, обслуживать на заданной частоте большее число абонентов. В отличие от CDMA, технология TDMA широко распространена.
- **U-NII** (Unlicensed National Information Infrastructure). Нелицензируемая национальная информационная инфраструктура. В рамках этого стандарта Cisco предлагает беспроводную систему, работающую на частоте 5,7 ГГц. Использование такой частоты не требует лицензирования, но, как и все электронные устройства, распространяемые на коммерческой основе, требует регистрации в FCC. Часто термином *NII* обозначают доступ к информации гражданских лиц и коммерческих структур. Подобно термину "информационная супермагистраль", он не описывает архитектуру системы или топологию.
- **Протокол беспроводного доступа** (Wireless Access Protocol — WAP). Язык написания Web-станиц, в котором сокращаются издержки передачи. Наиболее полезен для беспроводного доступа к Internet. Соответствущая WAP операционная система была разработана корпорацией 3Com для устройств Palm Pilot. Кроме того, компания Nokia недавно адаптировала ОС Palm для своих мобильных телефонов с возможностью просмотра Web-страниц.



В этой главе...

- Описаны различные виды технологий цифровых абонентских каналов (DSL)
- Описаны преимущества технологий xDSL
- Рассмотрены принципы работы технологии ASDL
- Описаны основные концепции передачи служебных сигналов и модуляции
- Рассмотрены другие технологии DSL (SDSL, HDSL, HDSL-2, G.SHDSL, IDSL и VDSL)

Глава 21

Цифровые абонентские каналы

Введение

Технология цифрового абонентского канала DSL (Digital Subscriber Line — DSL) представляет собой модемную технологию, которая использует имеющиеся телефонные линии на базе витой пары для передачи абонентам данных, требующих широкой полосы пропускания, таких как мультимедиа и видео. Термином xDSL обозначают несколько схожих, но, тем не менее, конкурирующих видов DSL-технологий, в том числе ADSL, SDSL, HDSL, HDSL-2, G.SHDL, IDSL и VDSL. Технология xDSL привлекает большое внимание со стороны разработчиков и провайдеров, поскольку позволяет доставлять данные, требующие широкой полосы пропускания, абонентам, расположенным в разных местах, при относительно небольших изменениях в имеющейся инфраструктуре телефонных компаний.

Службы xDSL предоставляют доступ по выделенной линии к общедоступной сети типа "точка-точка", осуществляемый по электрическому кабелю на базе витой пары по местной линии связи ("последняя миля") между центральным офисом провайдера сетевых служб (Network Service Provider — NSP) и узлом клиента или по местным линиям связи внутри здания либо комплекса. В настоящее время большинство систем DSL относятся к типу ADSL и обслуживают преимущественно индивидуальных пользователей. По этой причине основное внимание в настоящей главе будет уделено технологии ADSL.

Технология ADSL

Благодаря своей асимметрии технология цифрового абонентского канала (Asymmetric Digital Subscriber Line — ADSL) обеспечивает более широкую нисходящую полосу пропускания — от центрального офиса провайдера сетевых служб к абоненту, — чем восходящую, от абонента к центральному офису. Эта асимметрия, а также постоянный доступ (что устраняет необходимость в установке соединения) делает ADSL идеальным вариантом для работы в сети Internet или в intranet-сети, получения видео по заказу и для удаленного доступа к локальной сети. Пользователи этих приложений обычно получают гораздо больше информации, чем посылают.

Технология ADSL обеспечивает передачу данных со скоростью более 6 Мбит/с в направлении абонента и более 640 Кбит/с в обоих направлениях (рис. 21.1). Такие скорости передачи расширяют существующие возможности доступа более чем в 50 раз без прокладки дополнительных кабелей. Применение технологии ADSL позволяет преобразовать существующую общедоступную информационную сеть с ограниченными возможностями передачи голоса, текста и графики низкого разрешения в мощную, разветвленную систему, которая дает возможность доставлять мультимедийную информацию, включая полноценное видео, в каждый дом.

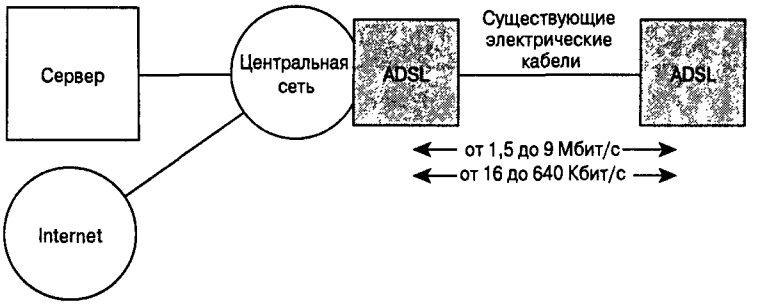


Рис. 21.1. В состав сети ADSL входят телефонные линии и CPE

Можно ожидать, что технология ADSL будет играть решающую роль еще не менее десяти лет, так как в этот период телефонные компании станут осваивать новые рынки доставки видео- и мультимедийной информации. Потребуются десятилетия, чтобы новые широкополосные кабельные сети достигли всех потенциальных абонентов. Успех этих новых служб зависит от того, сколько абонентов удастся получить в течение первых нескольких лет. Доставляя кинофильмы, телевидение, информацию видеокаталогов и удаленных CD-ROM, предоставляя доступ к корпоративным локальным сетям и к сети Internet из дома или из малого офиса, технология ADSL сделает эти рынки жизнеспособными и выгодными как для телефонных компаний, так и для разработчиков приложений.

Возможности технологии ADSL

Каналы ADSL соединяют ADSL-модемы телефонной витой парой и создают три информационных канала: высокоскоростной канал нисходящих потоков данных, среднескоростной дуплексный канал и основной телефонный канал. Основной телефонный канал отделяется от цифрового модема фильтрами, гарантируя таким образом непрерывность телефонной связи даже при сбое в канале ADSL. Скорость передачи высокоскоростного канала может изменяться в пределах от 1,5 до 9 Мбит/с, дуплексного — от 16 до 640 Кбит/с. Все каналы можно субмультиплексировать (подразделить) на несколько каналов с меньшей скоростью передачи.

В сетях ADSL фильтры называются *делителями сигналов в общедоступной телефонной сети (Plain Old Telephone System Splitters — POTS Splitters)*. Они функционируют как два полосных фильтра для отдельных частотных диапазонов с частотами выше 15 КГц и ниже 15 КГц. Их назначение состоит в том, чтобы обеспечить сосуществование как низкочастотного сигнала для голоса, так и высокочастотного модулированного сигнала цифровых данных в одном и том же канале передачи. Для этого требуются

делители POTS или фильтры как на узле пользователя ADSL, так и в центральном офисе провайдера службы.

ADSL-модемы обеспечивают скорости передачи данных, соответствующие североамериканской T1 (1,544 Мбит/с) и европейской E1 (2,048 Кбит/с) цифровым иерархиям (рис. 21.2). В продаже имеются модели с различными скоростями и техническими характеристиками. Минимальная конфигурация обеспечивает скорость передачи 1,5 или 2 Мбит/с по нисходящему каналу и 16 Кбит/с по дуплексному; другие модели обеспечивают 6,1 Мбит/с по нисходящему каналу и 64 Кбит/с по дуплексному. Уже сейчас можно приобрести модели со скоростью передачи данных до 8 Мбит/с по нисходящему каналу и до 64 Кбит/с по дуплексному. ADSL-модемы поддерживают как передачу в асинхронном режиме (Asynchronous Transfer Mode — ATM) с переменными скоростями передачи и компенсацией служебных ATM-сигналов, так и IP-протоколы.

Нисходящие каналы	
n x 1.536 Mbps	1.536 Мбит/с
	3.072 Мбит/с
	4.608 Мбит/с
	6.144 Мбит/с
n x 2.048 Mbps	2.048 Мбит/с
	4.096 Мбит/с
Дуплексные каналы	
C-канал	16 Кбит/с
	64 Кбит/с
Дополнительные каналы	160 Кбит/с
	384 Кбит/с
	544 Кбит/с
	576 Кбит/с

Рис. 21.2. Скорости передачи данных по нисходящему и дуплексному каналам

Скорость передачи данных по нисходящим каналам зависит от ряда факторов, включая длину электрического кабеля, его диаметр, наличие мостовых ответвлений и уровень перекрестных помех. Поглощение сигнала в линии увеличивается с возрастанием ее длины и частоты и уменьшается с увеличением диаметра провода. Рабочие характеристики ADSL без учета мостовых ответвлений показаны в табл. 21.1.

Таблица 21.1. Номинальная физическая производительность каналов ADSL

Скорость передачи, Мбит/с	Диаметр провода (стандарт AWG)	Расстояние, футы	Толщина провода, мм	Расстояние, км
1,5 или 2	24	18 000	0,5	5,5
1,5 или 2	26	15 000	0,4	4,6
6,1	24	12 000	0,5	3,7
6,1	26	9 000	0,4	2,7

Двумя факторами, оказывающими негативное влияние на качество связи в локальном ответвлении являются наличие мостовых ответвлений и витки нагрузки (load coil).

Мостовое ответвление (bridged tap) представляет собой любую часть локального ответвления, которая не находится непосредственно на маршруте передачи данных между центральным офисом CO и конечным оборудованием пользователя службы и не имеет терминирующей точки. Мостовое ответвление может представлять собой неиспользуемую кабельную пару, подсоединенную к промежуточной точке или расширение канала за пределы помещения пользователя. Дефекты канала, такие как полуответвления, замыкания или разомкнутость уменьшают максимальную дальность передачи сигнала, его качество и скорость передачи данных.

Витки нагрузки используются для изменения электрических характеристик локального ответвления и позволяют повысить качество передачи сигналов голосовых частот на большие расстояния (обычно более 18 000 футов). В таких случаях витки нагрузки располагаются через каждые 6000 футов. Обычно они представляют собой индукторы с индуктивностью 88 МГн (mH), устанавливаемые в корпусе, где сращиваются кабели или в распределительных шкафах. Витки нагрузки значительно повышают качество сигнала с частотой 3 КГц (частота ответной передачи) в длинных телефонных кабелях, однако уменьшают способность кабеля передавать частоты DSL. Это вызвано тем, что они изменяют индуктивное реактивное сопротивление канала передачи.

Хотя приведенные в табл. 21.1 параметры несколько меняются в зависимости от конкретной телефонной линии, эти характеристики применимы к 95% абонентского шлейфа, в зависимости от желаемой скорости передачи. Остальным абонентам служба может быть обеспечена при помощи систем оптоволоконных каналов. Когда такие системы станут коммерчески доступными, телефонные компании смогут предложить фактически повсеместный доступ за сравнительно короткое время.

Многие потенциальные области применения ADSL связаны с передачей сжатых цифровых видеоданных. Поскольку эти данные передаются в реальном времени, обычные процедуры контроля ошибок на канальном или сетевом уровне здесь неприменимы. Поэтому в ADSL-модемах используется метод прямой коррекции ошибок, радикально уменьшающий количество ошибок, порождаемых импульсными помехами. Посимвольная коррекция также снижает количество ошибок, вызванных постоянными канальными помехами. Двумя компонентами опережающей коррекции ошибок являются кодировка Reed-Solomon и чередование байтов (Byte Interleaving). Кодировка Reed Solomon вставляет биты служебной информации в данные, передаваемые в прямом направлении, что дает возможность обнаруживать и исправлять ошибки на принимающем конце канала без повторной передачи. Чередование битов переупорядочивает данные потока во временном домене для ослабления влияния кратковременных импульсных шумов.

Технология ADSL

Для того чтобы передать такой большой объем сжатой информации по телефонной витой паре, ADSL использует самые передовые технологии обработки цифровых сигналов и сложные алгоритмы. Кроме того, потребовалось значительно усовершенствовать преобразователи, аналоговые фильтры и аналогово-цифровые (analog/digital — A/D) конвертеры. Ослабление сигнала в 1 МГц (внешняя граница полосы частот ADSL) на длинных телефонных линиях может достигать на 90 дБ, что вызывает большую нагрузку на аналоговые секции ADSL-модемов, которые должны обеспечить широкие динамические диапазоны, разделение каналов и низкий уровень помех.

Внешне технология ADSL выглядит просто — как прозрачные синхронные каналы с различными скоростями передачи данных по обычным телефонным линиям. Но внутри, где работают транзисторы, она представляет собой чудо современной технологии. Приемо-передающая сеть ADSL показана на рис. 21.3.

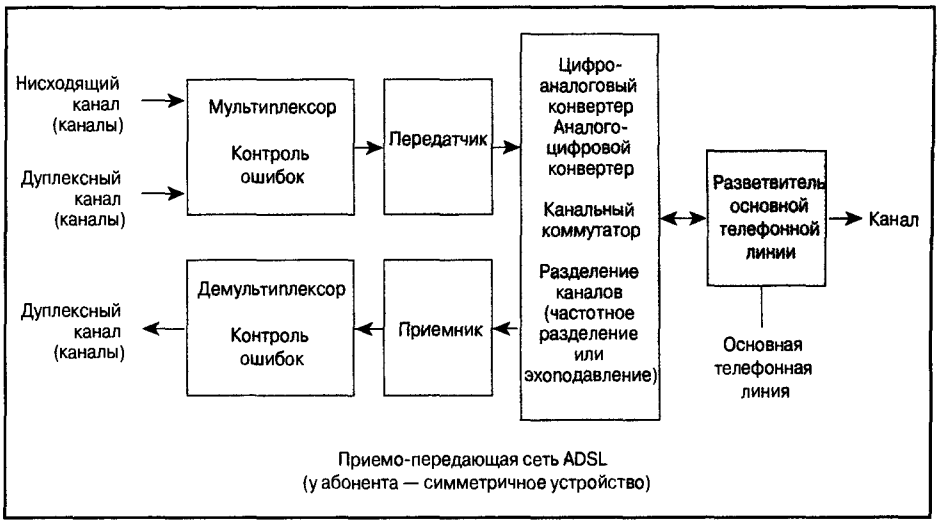


Рис. 21.3. Общая схема топологии приемо-передающей сети ADSL

Для создания нескольких каналов ADSL-модемы делят всю доступную полосу пропускания телефонной линии одним из двух способов: частотным уплотнением (Frequency-Division Multiplexing — FDM) или эхоподавлением (рис. 21.4). При частотном уплотнении выделяется отдельная полоса частот для восходящего и отдельная полоса — для нисходящего потока данных. Восходящая полоса частот, в свою очередь, делится методом временного мультиплексирования на один или несколько высокоскоростных и один либо несколько низкоскоростных каналов. Методом эхоподавления восходящая полоса частот частично накладывается на нисходящую полосу. Разделение полос осуществляется хорошо известным в модемах V.32 и V.34 методом эхоподавления. Независимо от того, какой метод используется, ADSL выделяет участок в 4 КГц на низкочастотном конце общего диапазона для основной телефонной линии.

На рис. 21.4 показана схема эхоподавления. Передача и прием информации с использованием одного и того же частотного спектра порождает интерференцию внутри самой отдельной шлейф-системы. Эта интерференция отличается от перекрестных помех тем, что форма искажающей сигнал волны известна приемнику и может быть изъята из ослабленного принимаемого сигнала. Устранение влияния передатчика называется эхоподавлением.

ADSL-модем группирует совокупный поток данных, созданный мультиплексированием нисходящих, восходящих и служебных каналов, в блоки и добавляет к каждому блоку код исправления ошибок. Затем получатель исправляет ошибки, возникшие при передаче, до пределов, допустимых кодом и размером блока. По усмотрению пользователя модуль может также создавать суперблоки, чередуя данные внутри субблоков. Это позволяет приемнику исправить любую комбинацию ошибок в пределах конкретного битового промежутка. и обеспечивает более эффективную передачу как сигналов цифровых данных, так и видеосигналов.

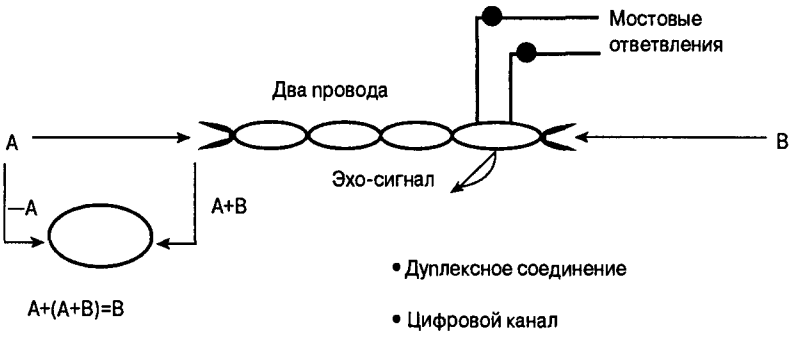


Рис. 21.4. Эхоподавление

Управляющие сигналы и модуляция

В этом разделе будут рассмотрены следующие вопросы:

- CAP- и DMT-модулированный ADSL;
- стандарты и объединения ADSL.

CAP- и DMT-модулирование ADSL

DMT и *CAP* представляют собой методы линейного кодирования для модуляции электрических сигналов, передаваемых по электрическим проводам в локальном шлейфе. Метод амплитуды и фазы без несущей (Carrierless Amplitude and Phase — CAP) является широко распространенным методом линейного кодирования. Эту технологию легко освоить благодаря ее сходству с QAM. Однако несмотря на эту легкость и малую стоимость некоторые специалисты утверждают, что технологию CAP трудно масштабировать, так как в ней используется модуляция только одной несущей и она чувствительна к узкополосной интерференции. В методе DMT применяется несколько несущих частот. В настоящее время этот метод обеспечивает более высокие скорости, чем CAP, что является одной из причин, по которой комитет ANSI T1E1.4 в документе T1.413 присвоил данной технологии статус стандарта.

Этот стандарт предусматривает 256 поддиапазонов по 4 КГц, которые занимают, соответственно, полосу в 1,024 ГГц. Каждый поддиапазон можно модулировать методом QAM-64 для получения свободных от помех поддиапазонов, вплоть до QPSK. Если все поддиапазоны способны поддерживать модуляцию QAM-64, то прямой канал обеспечивает скорость передачи 6,1 Мбит/с. Обратный канал имеет 32 поддиапазона с потенциальной скоростью передачи 1,5 Мбит/с.

Сравнение CAP и DMT

CAP представляет собой метод одной несущей, использующий широкую полосу пропускания, DMT — метод нескольких несущих, который использует много узкополосных каналов. Между названными двумя методами существует несколько технических

различий, хотя, в конечном итоге, они предоставляют аналогичные службы описанным выше сетевым уровням.

Адаптивная компенсация

Адаптивные компенсаторы представляют собой усилители, формирующие частотные характеристики для того, чтобы компенсировать затухания и фазовые погрешности. Адаптивная компенсация требует от модемов распознавания линейных характеристик путем анализа возвращающихся пробных сигналов. По ним компенсатор определяет, насколько треубется усилить сигнал для получения правильной и ровной частотной характеристики. Чем шире динамический диапазон, тем сложнее компенсация. При использовании ADSL требуется динамический диапазон в 50 дБ, что усложняет адаптивную компенсацию. Только последние достижения в области обработки цифровых сигналов (цифровое уплотнение) сделали возможной такую компенсацию в относительно небольшом конструктивном исполнении.

CAP нуждается в адаптивной компенсации потому, что параметры помех значительно изменяются в пределах полосы пропускания. Для DMT адаптивная компенсация не требуется, поскольку параметры помех не изменяются по ширине любой полосы пропускания шириной в 4 КГц. При сравнении методов DMT и CAP необходимо обратить внимание на определение точки, в которой сложность адаптивной компенсации превышает сложность многократных вычислений преобразования Фурье для DMT. Чтобы определить этот момент, необходим некоторый опыт реализации подобных систем.

Потребляемая мощность

Хотя DMT легко и просто масштабируется и не требует адаптивной компенсации, следует учесть и другие факторы. Прежде всего, DMT со своими 256 каналами потребляет больше мощности (и, следовательно, дороже обходится), чем CAP. DMT имеет высокое отношение пикового значения мощности к среднему, поскольку несколько несущих могут накладываться, порождая мощный сигнал. DMT отличается более высокими вычислительными требованиями и, значит, большим количеством транзисторов в микросхемах. Точные данные пока не опубликованы, но, по приблизительным оценкам, даже с дальнейшими усовершенствованиями один трансивер будет потреблять 5 Вт. Вопрос потребляемой мощности является важным из-за того, что в центральном офисе могут находиться сотни или даже тысячи (как очень надеются телефонные компании) трансиверов. Потребности теплоотвода в этом случае для DMT намного больше, чем для CAP.

Латентность

Еще одной проблемой для DMT является то, что латентность здесь несколько выше, чем у CAP (15). Поскольку все поддиапазоны используют только 4 КГц, ни один бит не может перемещаться быстрее, чем позволяет QAM-64. Компромисс между пропускной способностью канала и латентностью остается камнем преткновения в индустрии передачи данных и конкретное решение обычно определяется рынком.

Скорость

По скорости передачи данных DMT, по-видимому, превосходит CAP. Из-за того что у узкополосных несущих частот сравнительно немного проблем с компенсаций, во всех каналах могут применяться более агрессивные модуляционные технологии. Для достижения сопоставимых скоростей методом CAP может потребоваться более

широкий диапазон, значительно превышающий 1 Мгц. Это порождает новые проблемы, связанные с высокими частотами, при передаче по проводам и уменьшает преимущество в потребляемой мощности, которое имеет CAP сегодня.

Стандарты и объединения ADSL

Рабочая группа T1E1.4 Американского национального института стандартов (ANSI) недавно утвердила стандарт ADSL для скоростей до 6,1 Мбит/с (стандарт DMT/ANSI T1.413). Европейский институт стандартов по телекоммуникациям (ETSI) добавил к T1.413 приложение, отражающее европейские требования. В настоящее время T1.413 описывает единый терминальный интерфейс абонента. Выпуск II расширяет этот стандарт, включая в него мультиплексированный интерфейс абонента, протоколы настройки и управления сетью, а также другие усовершенствования.

Форум ATM и Цифровой аудиовизуальный совет (Digital Audio-Visual Council — DAVIC) признали ADSL протоколом передачи физического уровня для неэкранированной витой пары.

Другие технологии DSL

В этом разделе описываются следующие технологии DSL:

- SDSL;
- HDSL;
- HDSL-2;
- G.SHDSL;
- цифровая абонентская линия ISDN (Digital Subscriber Line — DSL);
- VDSL.

SDSL

Симметричный цифровой абонентский канал (Symmetric Digital Subscriber Line — SDSL,) представляет собой версию HDSL с настраиваемой скоростью передачи и, подобно HDSL, является симметричным. В этой технологии создаются одинаковые полосы пропускания как для нисходящего канала — от центрального офиса NSP к абоненту, так и для восходящего канала — от абонента к центральному офису NSP. Технология SDSL поддерживает передачу данных только по одной линии и не поддерживает аналоговых соединений. В SDSL используется линейное кодирование 2B1Q и обеспечивается скорость передачи до 1,54 Мбит/с в обоих направлениях. SDSL можно также настроить на предоставление переменной полосы пропускания со скоростью до 1,45 Мбит/с.

Внимание!

Two Binary, One Quarternary (два бинарных — одно четверичное) представляет собой метод линейного кодирования, в котором два бита данных сжимаются в одно временное состояние, представляющее собой код четырех уровней.

Симметричность SDSL-метода в сочетании с постоянным доступом (что устраняет необходимость установки соединения) делает этот метод привлекательной технологией распределенной сети для мелких и средних предприятий, а также филиалов крупных предприятий. Он может быть недорогой альтернативой выделенным линиям и службам Frame Relay. Благодаря симметричности потоков данных SDSL позволяет эффективно организовать передачу файлов, Web-хостинг и дистанционное обучение.

HDSL

Высокоскоростные технологии DSL (HDSL)/T1/E1 начали разрабатываться компанией Bellcore, а затем были стандартизированы институтом ANSI в Соединенных Штатах и институтом ETSI в Европе. Стандарт ANSI описывает передачу по двум парам T1 со скоростью 784 Кбит/с по каждой витой паре, стандарт ETS1 —систему E1 из двух пар со скоростью 1168 Кбит/с и систему E1 из трех пар со скоростью 784 Кбит/с по каждой витой паре.

Технология HDSL получила широкое распространение, поскольку она является лучшим способом предоставления каналов T1 или E1 по витой паре, чем давно применяемый метод кодирования с чередованием полярности элементов (Alternate Mark Inversion —AMI). Технологии HDSL требуется меньшая полоса пропускания и вплоть до диапазона CSA не требуются повторители. Используя адаптивную линейную компенсацию и модуляцию 2B1Q, передает данные со скоростью 1,544 Мбит/с или 2,048 Мбит/с.

Кодировка AMI представляет собой метод синхронной временной кодировки, который использует биполярные импульсы для представления значений логической единицы и, следовательно, является трехуровневой системой. Логический ноль представляется отсутствием символа, а логическая единица представляется импульсами переменной полярности. Кодировка AMI широко использовалась в первых поколениях сетей PCM, однако она имеет недостаток, состоящий в том, что длинная последовательность нулей не вызывает перехода в потоке данных и, следовательно, не содержит достатоного количества переходов для того, чтобы гарантировать запирание DPLL.

Службу T1 можно создать за один день менее чем за $1000 путем установки HDSL-модемов на каждом конце линии. Установка с AMI стоит дороже и занимает больше времени из-за необходимости установки повторителей между абонентом и центральным офисом. В зависимости от длины линии затраты на установку повторителей для AMI могут составить сумму до $5000 и занять больше недели. HDSL широко применяется в сотовой телефонии. Ретрансляция данных с базовой станции в центральный офис в более чем 50% систем осуществляется с использованием HDSL. Технология HDSL в настоящее время используется в подавляющем большинстве новых линий T1.

Однако у метода HDSL есть свои недостатки. Прежде всего, поскольку он использует речевой диапазон, он не предусматривает передачу аналоговой речи. Во-вторых, ADSL обеспечивает более высокие скорости, чем HDSL, так как асимметричность ADSL намеренно сохраняет перекрестные помехи только на одном конце линии. В симметричных линиях, таких как HDSL, перекрестные помехи имеются на обоих концах.

HDSL-2

Технология HDSL-2 представляет собой новый стандарт и многообещающую альтернативу HDSL. Целью данного метода является симметричное обслуживание со

скоростями T1, используя только одну витую пару, вместо двух. Это позволит предоставлять услуги более широкому кругу потенциальных потребителей. Для этого будут необходимы более агрессивная модуляция, меньшие расстояния (около 10000 футов) и телефонные линии лучшего качества.

Значительное количество оборудования SDSL, имеющегося сегодня на рынке, использует линейный код 2B1Q, разработанный для сетей ISDN. Американские региональные телефонные компании утверждают, что применение SDSL со скоростями, превышающими 768 Кбит/с, может создавать помехи в речевых и других службах, предоставляемых по тому же электрическому кабелю.

Наибольшим преимуществом метода HDSL-2, претендующего на стандарт, по которому могло бы взаимодействовать оборудование различных производителей, является то обстоятельство, что он был разработан таким образом, чтобы не создавать помех другим службам. Однако HSDL-2 может работать только на полной скорости передачи, передавая данные со скоростью 1,5 Мбит/с.

G.SHDSL

G.SHDSL представляет собой стандартизированную многоскоростную версию HDSL-2 предоставляющую симметричную службу передачи данных.

Преимуществом метода HDSL-2, призванного стать стандартом для взаимодействия оборудования различных производителей, является то, что он не должен создавать помех для других служб. Однако стандарт HSDL-2 обеспечивает службу только со скоростью передачи 1,5 Мбит/с. Многоскоростной метод HDSL-2 вошел во второе издание стандарта, известного как G.SHDSL, и был одобрен ITU. G.SHDSL использует преимущества метода HDSL-2, обеспечивая симметричные скорости передачи 2,3 Мбит/с.

Цифровой абонентский канал ISDN

Цифровой абонентский канал ISDN (ISDN Digital Subscriber Line — ISDL) представляет собой сочетание методов ISDN и xDSL. Эта технология подобна ISDN в том, что использует одну витую пару для дуплексной передачи данных со скоростью 128 Кбит/с на расстояния вплоть до диапазона RRD. Подобно ISDN, IDSL использует линейное кодирование 2B1Q для прозрачной работы через U-интерфейс ISDN. Кроме того, для соединения с центральным офисом пользователь продолжает эксплуатировать имеющееся у него оборудование (терминальные адаптеры BRI ISDN, мосты и маршрутизаторы).

Существенное отличие состоит в том, как данный метод выглядит с точки зрения провайдера. ISDL не осуществляет, как ISDN, соединений через речевой коммутатор. Для этого применяется оборудование другого типа, которое разрывает ISDL-соединение и замыкает его на маршрутизатор или коммутатор данных. В указанном и заключается главная особенность, поскольку перегрузка речевых коммутаторов центрального офиса клиентами, передающими данные, становится все более серьезной проблемой для телефонных компаний.

Ограничением ISDL является то обстоятельство, что абонент лишается доступа к ISDN-соединению или к речевым службам. Но для провайдеров Internet, которые не выполняют функций общедоступной телефонной сети, ISDL представляет собой привлекательный метод использования обычной коммутируемой телефонной сети для доступа к Internet. Таким образом к нему в качестве начального рынка переходят свыше пяти миллионов уже имеющихся пользователей ISDN.

VDSL

Сверхскоростной цифровой абонентский канал (Very-High-Hate Digital Subscriber Line —VDSL,) передает данные с высокой скоростью на короткие расстояния по телефонной витой паре. Диапазон скоростей передачи зависит от фактической длины канала. Максимальная скорость передачи нисходящего потока данных колеблется в пределах от 51 до 55 Мбит/с по каналам длиной до 300 метров (1000 футов). Низкие скорости передачи нисходящего потока, такие как 13 Мбит/с на дистанции свыше 1500 метров (4000 футов), тоже распространены довольно широко. Скорости восходящего потока данных в первых моделях будут асимметричными, подобно ADSL, при скоростях от 1,6 Мбит/с до 2,3 Мбит/с. Оба канала данных будут частотно отделены от каналов, используемых для обычных телефонных переговоров, и от сети ISDN, позволяя провайдерам предоставлять VDSL параллельно с уже существующими службами. В настоящее время эти два высокоскоростных канала также частотно разделены. По мере возрастания потребностей в высокоскоростных восходящих каналах или в симметричных скоростях в системах VDSL может понадобиться эхоподавление.

Резюме

ASDL является асимметричной технологией, предоставляющей для нисходящего потока данных более широкую полосу пропускания, чем для восходящего. Эта асимметричность в сочетании с постоянным доступом делает ADSL идеальным вариантом для пользователей, которые обычно принимают гораздо больше данных, чем отправляют.

ASDL-модемы подключаются к обоим концам витой пары телефонной линии, образуя три информационных канала: высокоскоростной — для нисходящих данных, среднескоростной дуплексный канал и основной телефонный канал. ASDL-модемы создают мультиканалы, разделяя доступный диапазон частот телефонной линии одним из двух методов: путем частотного уплотнения (Frequency Division Multiplexing — FDM) или эхоподавления. Оба метода отделяют полосу в 4 КГц на низкочастотном конце диапазона для основной телефонной линии.

Синхронная цифровая абонентская линия (Synchronous Digital Subscriber Line — SDSL) обеспечивает переменную, симметричную, высокоскоростную передачу данных со скоростью до 1,54 Мбит/с. Но SDSL, в отличие от ADSL, не позволяет передавать по той же линии аналоговый сигнал. В SDSL применяется линейное кодирование 2B1Q, подобно ISDN и T1. Метод SDSL целесообразно использовать для предприятий, потому что он позволяет передавать данные с высокой скоростью на большие расстояния от центрального офиса и отличается простотой установки, которая обеспечивается его спектральной совместимостью.

Высокоскоростная линия DSL (High Bit-Rate DSL — HDSL) представляет собой одну из версий DSL, в которой, как и в SDSL, используется кодирование 2B1Q, но применяются две витые пары. Метод HDSL ориентирован на коммерческое применение, так как он обеспечивает полноскоростную симметричную передачу данных со скоростью 1,5 Мбит/с. HDSL-2 представляет собой основанную на стандартах версию метода HDSL, которая, подобно HDSL, дает возможность передавать данные со скоростью 1,5 Мбит/с, но использует только одну витую пару. Метод HDSL работает лишь на постоянной скорости.

Метод G.SHDSL обеспечивает многоскоростное обслуживание и симметричные скорости до 2,3 Мбит/с. Цифровая абонентская линия ISDN (ISDN Digital Subscriber

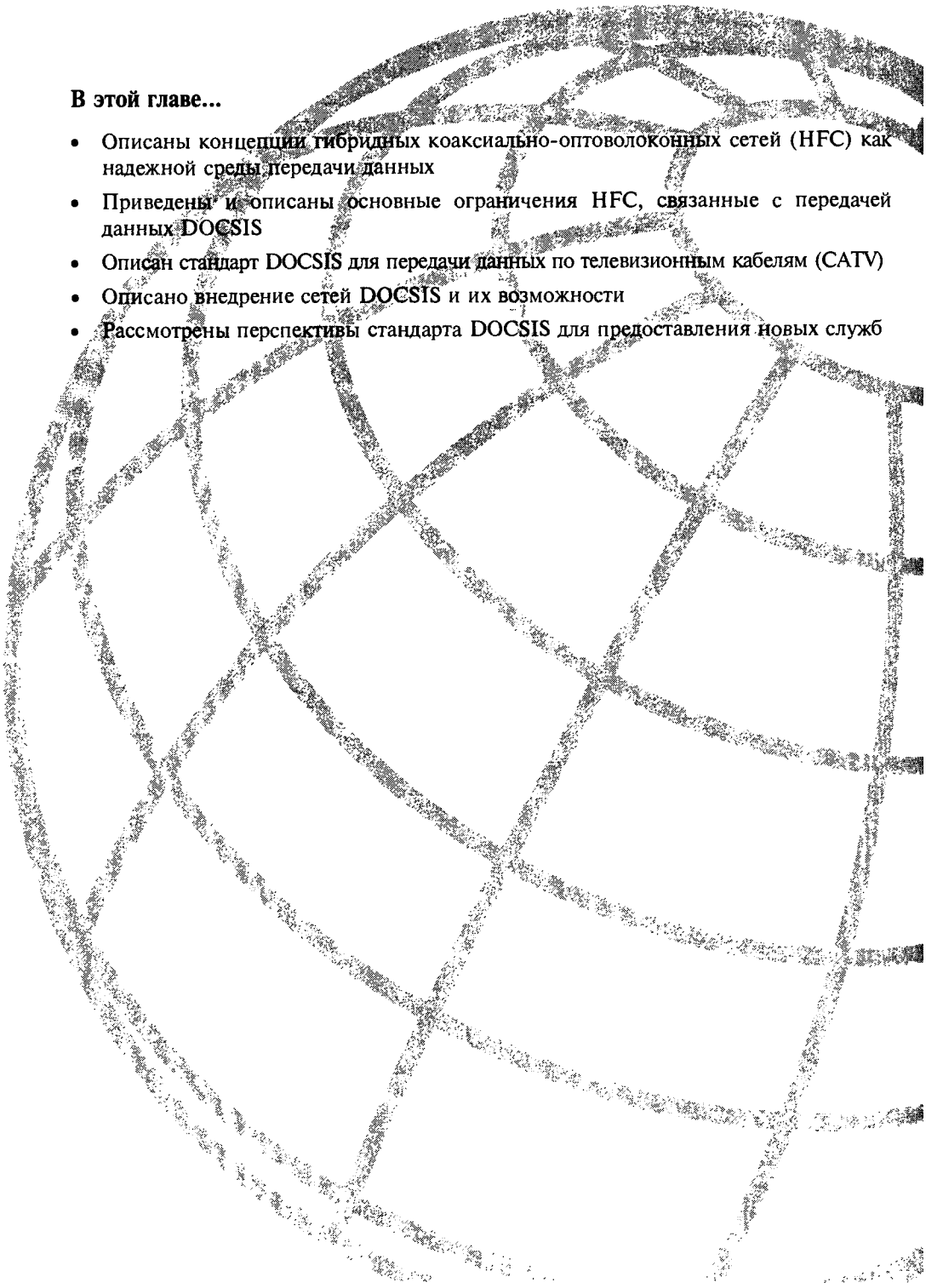
Line — IDSL) во многом похожа на ISDN. Основное отличие состоит в том, что IDSL всегда находится во включенном состоянии и с применением сжатия возможны скорости, доходящие до 512 Кбит/с. Метод IDSL использует линейное кодирование 2B1Q и не поддерживает передачу аналогового сигнала. С другой стороны, метод IDSL обеспечивает передачу данных на более длинные дистанции, чем прочие методы DSL (вплоть до 26000 футов), и в большинстве случаев стоит значительно дешевле ISDN. Поскольку IDSL позволяет использовать уже установленное абонентское оборудование, переход от ISDN на IDSL осуществляется весьма легко. Сверхскоростная цифровая абонентская линия (Very-High-Data-Rate Digital Subscriber Line — VDSL) передает данные с высокой скоростью на короткие дистанции по телефонной витой паре. Технология VDSL пока что находится в состоянии разработки, и, прежде чем ее можно будет стандартизировать, необходимы дополнительные исследования. VSDL и ADSL очень похожи. Однако, хотя VDSL передает данные почти в 10 раз быстрее, чем ADSL, технология ADSL сложнее.

Контрольные вопросы

1. Назовите существующие виды технологии DSL.
2. Какие два метода линейного кодирования применяются в ADSL?
3. Какие версии DSL предоставляют симметричные службы?
4. Какая симметричная версия DSL предоставляет многоскоростную службу по одной витой паре?
5. На какое расстояние от центрального офиса можно передавать данные с при использовании технологии IDSL?
6. Какие скорости для нисходящего и восходящего потоков данных предлагаются для VDSL?

Дополнительные источники

- Форум ADSL (http://www.adsl.com/)
- Cisco DSL Depot (http://www.cisco.com/warp/public/779/servpro/promotions/dsldepot/)



В этой главе...

- Описаны концепции гибридных коаксиально-оптоволоконных сетей (HFC) как надежной среды передачи данных
- Приведены и описаны основные ограничения HFC, связанные с передачей данных DOCSIS
- Описан стандарт DOCSIS для передачи данных по телевизионным кабелям (CATV)
- Описано внедрение сетей DOCSIS и их возможности
- Рассмотрены перспективы стандарта DOCSIS для предоставления новых служб

Глава 22

Технологии кабельного доступа

Введение

Исторически телевизионные кабельные системы (Cable Television System — CATV) были однонаправленной средой передачи, предназначенной для трансляции аналоговых видеоканалов максимальному количеству клиентов по минимальной цене. Со времени появления CATV прошло более 50 лет, но с тех пор мало что изменилось, кроме увеличения количества каналов. Технологии двусторонних разнообразных служб оставались недоступными.

В 90-х годах XX в. с возникновением прямого спутникового вещания (Direct Broadcast Satellite — DBS) и цифровых абонентских линий (Digital Subscriber Line — DSL) конкурирующие технологии поставили под вопрос существование операторов кабельных сетей. Им угрожало вытеснение с рынка их единственной продукции.

Благодаря цифровым технологиям DBS-операторы предоставляли более широкий выбор и лучшее качество развлекательной продукции, а местные телефонные компании (Local Exchange Carriers — LEC) обещали обеспечить средствами DSL параллельную передачу речи, видео и цифровых данных.

Из-за боязни потерять свой рынок, а также чтобы остаться "на плаву", операторы мультисистем (Multiple System Operators — MSO) решили объединиться в компанию Multimedia Cable Network System Partners, Ltd. (MCNS). Их целью было разработать стандарт продукции и системы для передачи данных и услуг, предоставляемых по сетям CATV. В противоположность предлагаемой в стандарте IEEE 802.14 системе на базе ячеек (ATM) MCNS предложила пакетный вариант (IP). В число партнеров MCNS вошли Comcast Cable Communications, Cox Communications, Tele-Communications Inc., Time Warner Cable, MediaOne, Rogers CableSystems и Cable Television Laboratories (CableLabs).

В качестве стандарта для Северной Америки была единодушно принята созданная усилиями MCNS спецификация интерфейса службы передачи данных по кабельным сетям DOCSIS 1.0 (Data Over Cable Service Interface Specification — DOCSIS 1.0), и производители стали активно предлагать соответствующую этому стандарту продукцию. Для увеличения полосы пропускания своих сетей и обеспечения возможности двусторонней передачи MSO определили программы усовершенствования и реконструкции.

Стандарт DOCSIS 1.0 предполагает функциональную совместимость между продукцией различных производителей и розничную продажу кабельных модемов (Cable Modem — CM) непосредственно потребителям. Чтобы обеспечить функциональную

совместимость между продукцией различных производителей, CableLabs подвергает всю производимую продукцию тщательному тестированию. Центральные системы CMTS (Cable Modem Terminating System) и кабельные модемы, успешно прошедшие все тесты, получают сертификаты CableLabs.

На сегодняшний день DOCSIS 1.0 является наиболее универсальным стандартом. Созданные на его базе системы применяются по всему миру.

Сейчас CableLabs совместно с производителями и пользователями разрабатывает стандарт DOCSIS 1.1 с передачей речи по протоколу IP (VoIP) и усовершенствованной системой защиты, а также подготавливает почву для будущих мультимедийных служб.

Эволюция от однонаправленного вещания к двусторонним гибридным коаксиально-волоконным сетям

Сеть CATV состоит из центрального пункта, куда поступают все входящие сигналы и, независимо от их источника, к ним применяется частотное уплотнение (Frequency-Division Multiplexing — FDM). Затем сигналы усиливаются и передаются по *нисходящему потоку* (downstream) для распространения по всей кабельной сети.

Первоначально сети CATV были исключительно односторонними и содержали каскады разнообразных усилителей, компенсирующих внутреннюю потерю сигналов в коаксиальных кабелях, а также метки для распределения видеосигнала главных магистралей по ответвительным кабелям, идущим в дома абонентов (рис. 22.1).

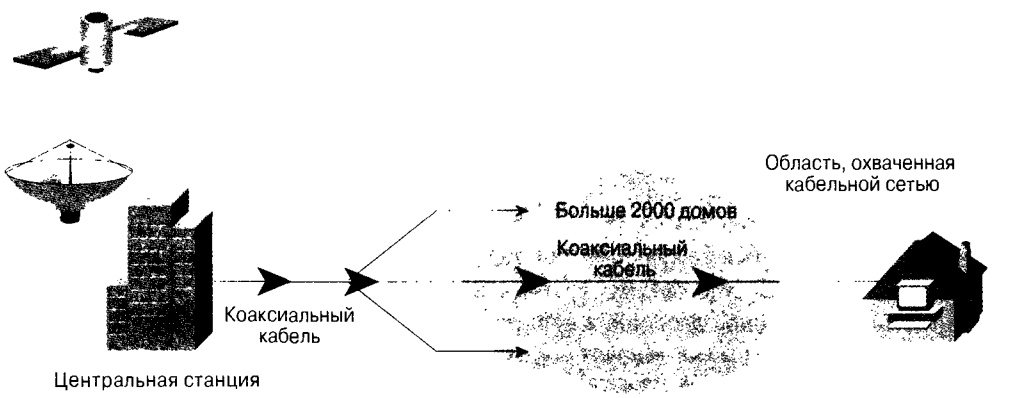


Рис. 22.1. Топология простого одностороннего вещания, построенная исключительно на коаксиальных кабелях

Кроме однонаправленности, длинные каскады усилителей вызывают высокий уровень шумов в системе, отчего она становится внутренне ненадежной и склонной к сбоям. К этому следует добавить восприимчивость к атмосферным разрядам и внешним помехам от радиосигналов.

Первым существенным улучшением в структуре CATV стало введение оптоволоконной технологии и появление оборудования HFC (рис. 22.2).

Коаксиальный кабель, подключенный к центральной станции, или концентратору, и сопутствующие ему усилительные элементы были заменены многоволоконным

оптическим кабелем. Собранный видеосигнал использовался для модуляции исходящего лазера, передающего оптический сигнал в оптический узел. Последний, в свою очередь, преобразовывал сигнал из оптического в электрический, и этот сигнал затем распространялся по обслуживаемой зоне.

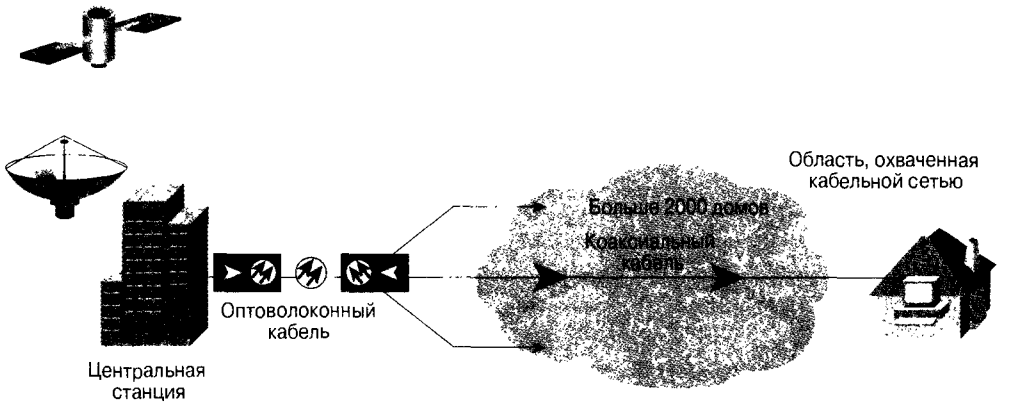


Рис. 22.2. Простая распределительная сеть HFC

Нетрудно заметить, что благодаря оптоволоконным кабелям значительно уменьшилось количество каскадных усилителей и, следовательно, повысилась надежность системы, отношение "сигнал/шум" (Signal-to-Noise Ratio — SNR) нисходящего сигнала и потенциальная полоса пропускания системы. Кроме того, это подготовило систему к следующему шагу в направлении двусторонней передачи данных. Дополнительным преимуществом применения HFC стало сокращение эксплуатационных расходов и затрат на обслуживание и, к тому же, повышение устойчивости системы к внешним помехам.

Для двусторонней передачи нужно установить в системе усилители восходящего сигнала и, кроме узкополосного восходящего лазера в оптическом узле, специальный восходящий оптоволоконный кабель на центральной станции, а также совместимый оптический приемник для преобразования любой восходящей информации в электрический сигнал. После установки всех указанных компонентов остается только настроить соответствующий обратный маршрут.

Благодаря введению оптической кольцевой топологии обеспечивается более высокая надежность кабельной сети, большая пропускная способность и возможность передачи большего количества информации. Сеть готова к двусторонней передаче данных, остается только установить необходимые для этого компоненты (рис. 22.3).

При установке промежуточного концентратора повышается надежность, масштабируемость и гибкость сети, а также, в конечном счете, появляется возможность предоставления дополнительных услуг.

Описанные HFC-сеть и топология являются основными составляющими для развития возможностей доступа к среде передачи, необходимого MSO для конкурирования в динамической коммуникационной среде.

Характеристики и ограничения HFC-сетей

Потенциал HFC-сети позволяет обеспечить огромную пропускную способность нисходящего канала или прямой передачи от центральной станции или концентратора

к потребителю. В зависимости от сложности системы пропускная способность может составлять от 54 до 860 МГц. Пропускная способность нисходящих каналов определяется государственными стандартами телевещания.

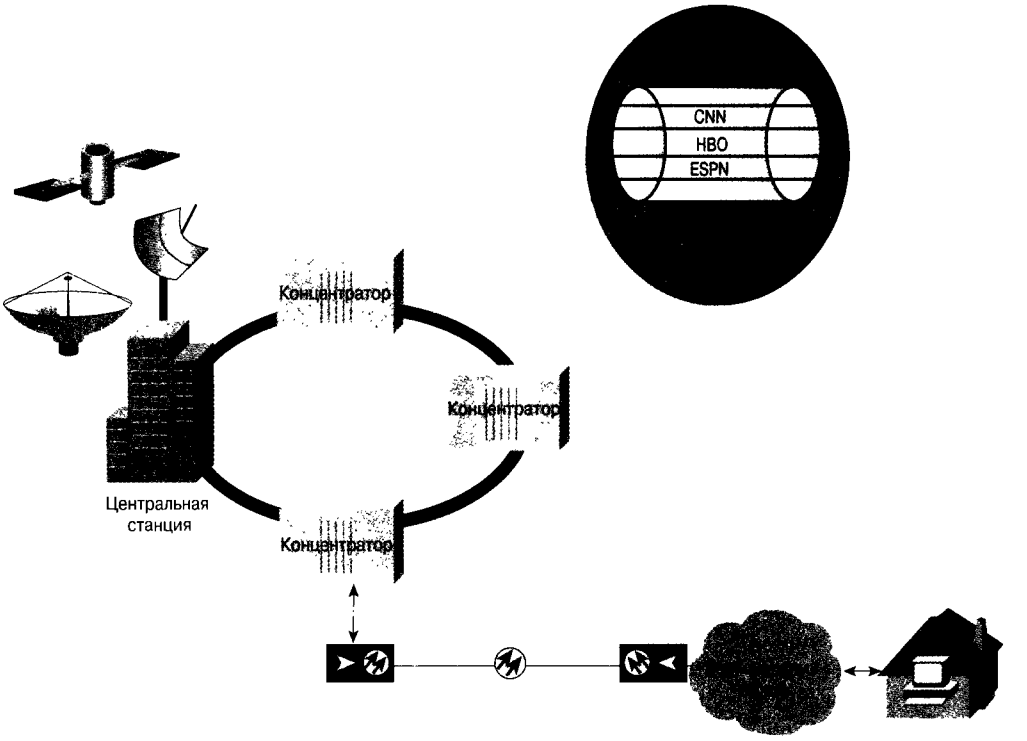


Рис. 22.3. Усовершенствованная сеть HFC с кольцевой топологией

Исторически сложившееся назначение широковещательных видеоканалов ограничивает восходящий поток, или обратную передачу данных от потребителя, диапазоном 5–42 МГц. Для поддержания обратной связи этого часто оказывается недостаточно из-за внешних помех, таких как любительские радиосигналы и другие законные источники радиоволн.

Характеристики нисходящего потока приведены в табл. 22.1, а восходящего — в табл. 22.2.

Система DOCSIS должна обеспечивать больше чем 99-процентную надежность при передаче 1500-байтовых пакетов со скоростью не менее 100 пакетов в секунду. Для этого необходимо обеспечить некоторые параметры производительности CATV как для восходящего, так и нисходящего потоков.

Хорошая конструкция, структура и техническое обслуживание сетей CATV позволяют без труда соблюсти эти традиционные видеопараметры в операционных системах. Однако параметры первостепенной важности связаны с уровнем сигнала и шумом.

Таблица 22.1 Характеристики нисходящего кабеля

Параметры нисходящего потока	Предполагается номинальный уровень аналогового видеоканала (групповая пиковая мощность) в канале на уровне 6 МГц при всех условиях, выполняемых одновременно на частоте свыше 88 МГц
Разбивка RF-канала (BW)	6 МГц
Задержка передачи от CMTS к наиболее удаленному клиенту	Не более 0,800 мс
CNR в полосе 6 МГц	Не менее 35 дБ (уровень аналогового видео)
Отношение C/I для общей мощности (дискретные и широкополосные посторонние сигналы)	Не менее 35 дБ в структуре BW
Общее трехтактовое искажение для аналоговых модулированных каналов	Не более –50 дБ по шкале C в структуре BW
Общее искажение второго порядке для аналоговых модулированных каналов	Не более –50 дБ по шкеле C в структуре BW
Кроссмодуляционный уровень	Не болеее –40 дБ по шкеле C в структуре BW
Колебание амплитуды	0,5 дБ в структуре BW
Колебание групповой задержки в спектре CMTS	75 нс в структуре BW
Микроотражения основного эхосигнала	–10 дБ по шкале C не более чем за 0,5 мс –15 дБ по шкале C не более чем за 1,0 мс –20 дБ по шкале C не более чем за 1,5 мс –30 дБ по шкале C не более чем за 1,5 мс
Фоновая модуляция канала	Не более –26 дБ по шкале C (5%)
Шум всплесков	Менее 25 мс со средней частотой 10 Гц
Сезонные и суточные колебания уровня сигнала	8 дБ
Спад уровня сигнала (50–750 МГц)	16 дБ
Максимальный уровень аналогового видеокенала на входе CM, включая колебания верхнего уровня сигнала	17 дБ/мВ
Минимальный уровень аналогового видеоканала на входе CM, включая колебания верхнего уровня сигнала	–5 дБ/мВ

Таблица 22.2 Характеристики восходящего кабеля

Параметры восходящего потока	Предполагается выполнение всех условий
Диапазон частот	5-42 МГц по всей длине канала
Задержка передачи между неиболее удаленным CM и ближайшим CM или CMTS	Не более 0,800 мс
Отношение канал/шум	Не менее 25 дБ

Окончание табл. 22.2

Параметры восходящего потока	Предполагается выполнение всех условий
Отношение мощности канал/помеха (сумма дискретной и широкополосной помехи)	Не менее 25 дБ
Отношение канал/интерференция (сумма шума, искажений, искажений общего пути и перекрестной модуляции)	Не менее 25 дБ
Фоновая модуляция в канале	Не более –23 дБ по шкале С (7%)
Шум всплесков	Обычно не дольше 10 мс при средней скорости 1 КГц
Колебания амплитуды	0,5 дБ/МГц (5–42 МГц)
Колебания групповой задержки	200 нс/МГц (5–42 МГц)
Микроотражения: единичный эхосигнал	–10 дБ по шкале С не более чем за 0,5 мс –20 дБ по шкале С не более чем за 1,0 мс –20 дБ по шкале С не более чем за 1,0 мс
Сезонные и суточные колебания уровня сигнала	Не более 8 дБ между минимальным и максимальным уровнями

Серьезной проблемой для операторов стало обеспечение полезной полосы пропускания, соответствующей требованиям передачи данных и других служб. Ограниченную восходящую полосу пропускания часто приходится делить с другими службами, такими как абонементное телевидение (Impulse Pay-Per-View — IPPV), телеметрия и предупреждения от активных элементов кабельной сети. Кроме того, приходится бороться с наложением сигналов низкочастотного диапазона.

Из-за ограниченной и часто недружелюбной восходящей полосы частот при конструировании оборудования необходимо принять контрмеры для уменьшения влияния постоянных и временных шумов. К тому же, сетевому разработчику при внедрении DOCSIS нужно выбирать из оставшегося доступного спектра и часто идти на компромиссы.

Конфигурация физического уровня обратного пути в конце концов будет определяться качеством восходящего сигнала, которое измеряется отношением "канал/шум" (Carrier-to-Noise Ratio — CNR), ожидаемым проникновением на рынок, спектром предлагаемых услуг и доступной полосой частот.

Стандарты, сигнальные протоколы и приложения DOCSIS

Спецификации интерфейса DOCSIS сделали возможным развитие и внедрение общедоступных кабельных систем передачи данных на базе оборудования разных производителей с обеспечением функциональной совместимости для прозрачной двусторонней передачи данных по IP-протоколу между центральной станцией кабельной системы и пользователями по полностью коаксиальным или гибридным коаксиально-оптоволоконным (Hybrid-Fiber/Coax — HFC) кабельным сетям.

Система состоит из CMTS, расположенной на центральной станции, коаксиальной или коаксиально-волоконной среды передачи и кабельных модемов, находящихся у потребителя, а также уровнями DOCSIS, обеспечивающими функциональную

совместимость и возможности дальнейшего развития и предоставления в будущем более широкого спектра услуг.

На уровне DOCSIS определены следующие понятия.

- Сетевой уровень протокола IP.
- Канальный уровень, состоящий из следующих подуровней:
  - — подуровень управления логическим соединением (Logical Link Control — LLC), соответствующий стандартам Ethernet;
  - — подуровень безопасности канала, обеспечивающий общую безопасность, авторизацию и аутентификацию;
  - — подуровень управления доступом к среде передачи (Media Access Control — MAC) для поддержки модулей данных протокола (Protocol Data Units — PDU) переменной длины, имеет следующие функции:
    - — CMTS-управление конфликтами и возможностями передачи;
    - — восходящий поток мини-слотов;
    - — эффективность полосы пропускания за счет пакетов переменной длины;
    - — расширения для поддержки в будущем асинхронной передачи (Asynchronous Transfer Mode — ATM) и других типов PDU;
    - — поддержка многоуровневых служб и различных скоростей передачи.
- Физический (PHY) уровень, состоящий из следующих подуровней:
  - — подуровня нисходящей конвергенции, согласованного с MPEG-2 (Rec. H.222.0);
  - — физического подуровня, зависящего от среды передачи (Physical Media Dependent — PMD), который, в свою очередь, состоит из следующих элементов:
    - — нисходящего потока, соответствующего ITU-T Rec. J.83 Annex B с 64- или 256-кратной квадратурно-амплитудной модуляцией (QAM), сочетание упреждающей коррекции ошибок (Forward Error Correction — FEC) Reed-Solomon и Trellis и чередования переменной глубины;
    - — восходящего потока, где применяются:
      - — квадратурно-фазовая модуляция (Quadrature Phase-Shift Keying — QPSK) или 16-QAM;
      - — поддержка нескольких символьных скоростей;
      - — CM, управляемый и программируемый из CMTS;
      - — быстрая перестройка частоты;
      - — поддержка форматов PDU для фреймов фиксированной и переменной длины;
      - — множественный доступ с разделением времени (Time-Division Multiple Access — TDMA)
      - — программируемые FEC Reed-Solomon и префиксы;
      - — поддержка возможных будущих технологий физического уровня.

Кроме того, эта спецификация определяет способ, которым CM может самостоятельно определять частоты, битовые скорости, формат модуляции, коррекцию ошибок и уровни напряжения для восходящих и нисходящих потоков. Для обеспечения одинакового качества обслуживания кабельным модемам разрешается передавать данные только в определенных и управляемых условиях.

На рис. 22.4 представлено сравнение уровней DOCSIS и классических уровней OSI.

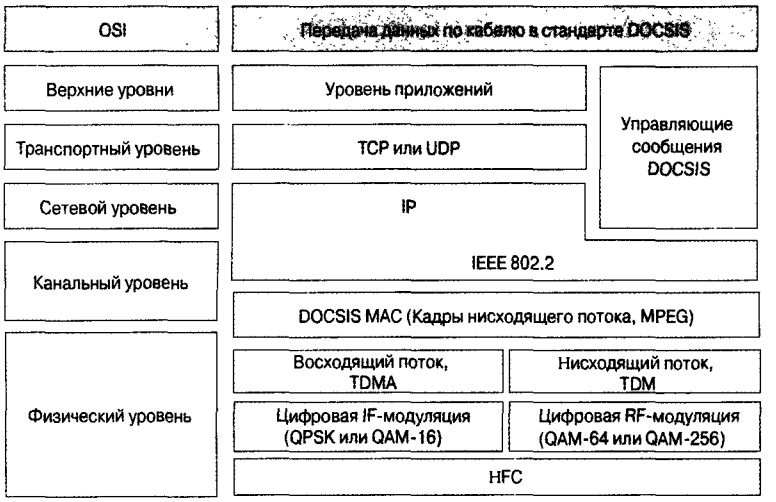


Рис. 22.4. Уровни протоколов DOCSIS и OSI

Физический уровень DOCSIS обеспечивает значительную гибкость, гарантирующую качественную передачу, которой можно достичь на кабельном оборудовании разного качества. Особое значение имеют пропускные способности дополнительных восходящих каналов и варианты модуляции — как восходящих, так и нисходящих потоков.

Суммарные и эффективные скорости передачи данных в системах DOCSIS, основанные на пропускной способности и вариантах модуляции, а также определяемых DOCSIS символьных скоростях, приведены в табл. 22.3–22.5. Разница между соответствующими скоростями обусловлена большим объемом передачи служебных данных, который возникает вследствие неэффективности FEC.

Таблица 22.3. Номинальные скорости передачи нисходящих данных DOCSIS по каналу с полосой пропускания 6 МГц

Тип модуляции	64 QAM	256 QAM
Символьная скорость	5,057 МС/с	5,360 МС/с
Общая скорость передачи данных	30,34 Мбит/с	42,9 Мбит/с
Эффективная скорость передачи данных	27 Мбит/с	38 Мбит/с

Таблица 22.4. Номинальные скорости передачи восходящих данных DOCSIS для QPSK

Полоса пропускания	200 КГц	400 КГц	800 КГц	1600 КГц	3200 КГц
Символьная скорость	0,16 МС/с	0,32 МС/с	0,64 МС/с	1,28 МС/с	2,56 МС/с
Общая скорость передачи данных	0,32 Мбит/с	0,64 Мбит/с	1,28 Мбит/с	2,56 Мбит/с	5,12 Мбит/с
Эффективная скорость передачи данных	0,3 Мбит/с	0,6 Мбит/с	1,2 Мбит/с	2,3 Мбит/с	4,6 Мбит/с

Таблица 22.5. Номинальные скорости передачи восходящих данных DOCSIS для 16-QAM

Полоса пропускания	200 КГц	400 КГц	800 КГц	1600 КГц	3200 КГц
Символьная скорость	0,16 МС/с	0,32 МС/с	0,64 МС/с	1,28 МС/с	2,56 МС/с
Общая скорость передачи данных	0,64 Мбит/с	1,28 Мбит/с	2,56 Мбит/с	5,12 Мбит/с	10,24 Мбит/с
Эффективная скорость передачи данных	0,6 Мбит/с	1,2 Мбит/с	2,3 Мбит/с	4,5 Мбит/с	9 Мбит/с

Согласно DOCSIS, для того чтобы система стала функциональной и находилась в рабочем состоянии, в ее состав обязательно должны входить следующие серверы, играющие роль интерфейса между CMTS и CM.

- **Сервер протокола динамической конфигурации хоста** (Dynamic Host Configuration Protocol — DHCP), описанный в RFC 2181. Предоставляет IP-адреса для CM и связанных с ним PC-устройств.
- **Сервер регистрации времени суток (Time of Day TOD)**, описанный в RFC 868. Записывает время совершения событий операционной системы.
- **Сервер простейшего протокола передачи файлов (Trivial File Transfer Protocol — TFTP)**, описанный в RFC 1350. Предназначен для регистрации и загрузки конфигурационных файлов CM для отдельных абонентских служб. Эти конфигурации могут содержать параметры качества обслуживания (QoS), версию основной системы обеспечения конфиденциальности (Baseline Privacy — BPI), значение рабочей частоты, количество устройств-узлов и т.п.

В крупных системах рекомендуется выделить для этих серверов отдельные компьютеры, что обеспечило бы быстрое реагирование системы и масштабируемость.

Как видно из рис. 22.5, спецификации DOCSIS диктуют условия регистрации CM. В среде с CMTS и необходимыми серверами CM при первом включении проверяет нисходящий спектр частот на наличие совместимого RF-канала, передающего данные, полностью соответствующие физическому уровню DOCSIS. CMTS периодически делает по DS-каналу широковещательную рассылку дескрипторов восходящих каналов (Upstream Channel Descriptors — UCD), из которой кабельные модемы узнают назначенную им рабочую частоту восходящего потока. После этого CM устанавливают частоты US и DS.

Периодически CMTS передает в общих временных слотах нисходящего потока схемы распределения восходящей полосы частот (здесь и далее называемые MAP).

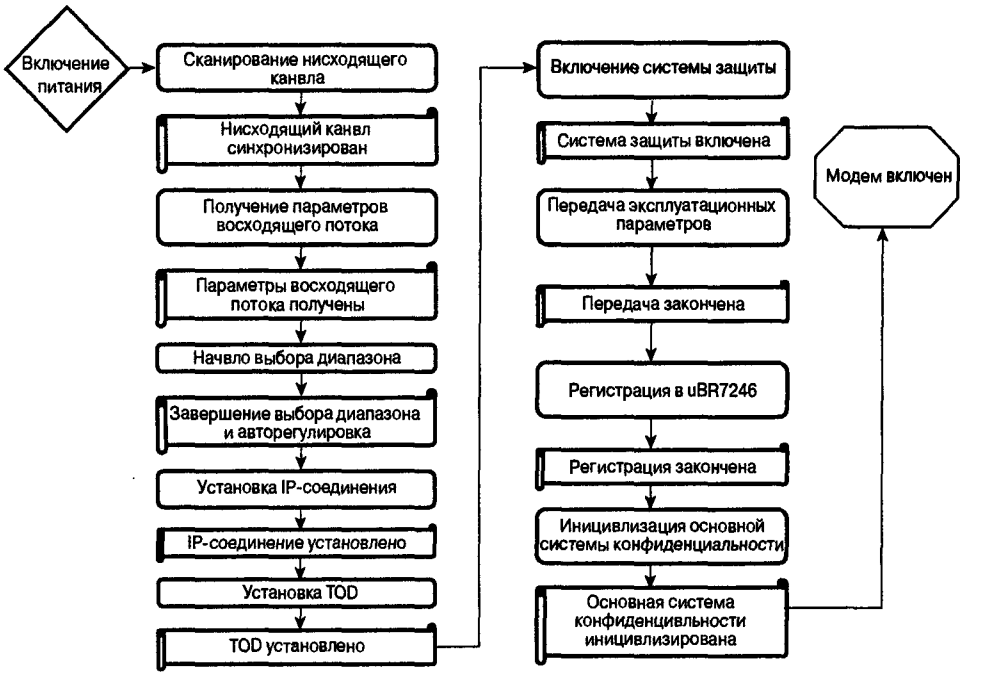


Рис. 22.5. Последовательность действий при регистрации кабельного модема

CMTS назначает кабельному модему, который начинает грубый выбор диапазона мощности (R1 с шагом 3 дБ), временные идентификаторы служб (Service IDentifier — SID, обычно SID=0) и процесс конкурентной синхронизации между собой и CMTS, используя общие временные слоты.

Периодически CMTS посылает "пустые" сообщения, чтобы убедиться в непрерывности связи со всеми кабельными модемами своего домена. Когда CM получает первое "пустое" сообщение, он переходит на точный выбор диапазона мощности (R2 с шагом 0,25 дБ).

После процесса R2 считается, что CM установил *соединение* с CMTS. Но если 16 последовательных "пустых" сообщений будут потеряны, то это соединение разорвется.

CM на конкурентной основе в общих временных слотах направляет CMTS запрос на полосу пропускания, используя временный SID. CMTS направляет CM ответ, дающий ему право передавать восходящую информацию в соответствующих временных слотах. Затем CM ищет в сети сервер DHCP и направляет туда запрос. CMTS передает DHCP-подтверждение от сервера DHCP, где указаны IP-адрес, стандартный шлюз, адреса серверов TFTP и TOD и имя файла конфигурации TFTP.

CM последовательно запускает процессы TOD и TFTP. От сервера TFTP CM получает файл конфигурации, содержащий параметры QoS, защиты, назначенные частоты и все образы нового программного обеспечения.

CM передает этот файл конфигурации CMTS и делает запрос на регистрацию. Если конфигурационный файл действителен, то CMTS присваивает CM постоянный SID, а CM — интерактивный статус.

После регистрации CM может активировать алгоритм 56-разрядного шифрования DES, чтобы обеспечить безопасность передачи данных на протяжении всего маршрута между собой и CMTS.

Как только CM зарегистрирован, его индивидуальное состояние может отслеживаться удаленно при помощи команд доступа к CMTS. В табл. 22.6 приведены определения сообщений о состоянии, поступающие от универсального широкополосного маршрутизатора Cisco.

Таблица 22.6. Определения команд состояния кабельного модема для Cisco CMTS

Сообщение	Его содержание
Offline	Модем отключен от сети
init(r1)	Модему послан первичный выбор диапазона
Init(r2)	Модем выбирает диапазон
Init(rc)	Выбор диапазона завершен
Init(d)	Получен запрос DHCP
Init(i)	Получен ответ на запрос DHCP; назначен IP-адрес
Init(t)	Получен запрос TOD
Init(o)	Получен запрос TFTP
online	Модем зарегистрирован и готов к получению данных
Online(d)	Модем зарегистрирован, но не имеет доступа к сети
Online(pk)	Модем зарегистрирован, BPI открыт, KEK назначен
Online(pt)	Модем зарегистрирован, BPI открыт, TEK назначен
Reject(m)	Модем сделал попытку зарегистрироваться; в регистрации отказано из-за плохого MIC
Reject(c)	Модем сделал попытку зарегистрироваться; в регистрации отказано из-за плохого COS
Reject(pk)	Отказано в назначении модему ключа KEK
Reject(pt)	Отказано в назначении модему ключа TEK

Согласно спецификации DOCSIS, передача данных через CMTS может осуществляться прозрачно, через мост, использовать маршрутизацию сетевого уровня или IP-коммутацию. Кроме того, в ней говорится что передача данных через CM должна быть прозрачной, через мост, на канальном уровне, с модификациями, обеспечивающими поддержку нескольких сетевых уровней.

Кроме того, DOCSIS определяет общие спецификации CMTS и CM, обеспечивающие функциональную совместимость оборудования различных производителей в одной системе. Эти параметры приведены в табл. 22.7.

Таблица 22.7. Общие аппаратные спецификации CMTS

Параметр	Характеристика	
Диапазон частот	Восходящий поток	5-42МГц (5–65 МГц вне США)
	Нисходящий поток	88-860 МГц
Полоса пропускания	Восходящий поток	200, 400, 800, 1600, 3200 КГц
	Нисходящий поток	6 МГц (8 МГц вне США)

Окончание табл. 22.7

Параметр	Характеристика	
Режимы модуляции	Восходящий поток	QPSK или 16 QAM
	Нисходящий поток	64 или 256 QAM
Символьная скорость	Восходящий поток	160, 320, 640, 1280, 2560 КС/с
	Нисходящий поток	5.056941 или 5.360537 КС/с
Диапазон уровня питания CMTS	Восходящий поток	от 8 до 58 dBmV (QPSK) от 8 до 55 dBmV (16 QAM)
	Нисходящий поток	от -15 до +15 dBmV

Для того чтобы достичь или превысить критерий доступности DOCSIS, в оборудовании должны быть предусмотрены средства шумопонижения или оно должно обладать свойствами, позволяющими работать в недружелюбном восходящем потоке. Для восходящего потока оператор может выбрать либо QPSK, либо 16-QAM с пониженным CNR, но с уменьшенной спектральной эффективностью.

Кроме того, можно настроить систему упреждающей коррекции ошибок (Forward Error Correction — FEC), позволяющую уменьшить количество данных, испорченных шумом. Более того, оператор может выбрать оптимальную восходящую BW для каналов данных в шумном спектре или в спектре, предназначенном для других служб.

Последней из возможных контрмер, на случай непостоянных шумов, является управление спектром, то есть изменение выбранной восходящей частоты, модуляции и полосы пропускания канала, чтобы обеспечить надежную передачу данных между CMTS и CM.

В табл. 22.8 приведены основные физические характеристики для оборудования DOCSIS 1.0, шумопонижающие контрмеры и соответствующие параметры кабельной сети. На основании этой информации, зная реальные характеристики кабельной сети, оператор может сделать вывод о возможности построения сети с использованием данного оборудования.

Таблица 22.8. Характеристики CM

Параметр	Характеристика
Диапазон уровня напряжения CM:	
Выходной	QPSK: 8–58 дБ/мВ 16 QAM: 8–55 дБ/мВ
Входной	–15 — 15 дБ/мВ
Уровень передачи	–6 — –10 дБ по шкале С

Внедрение систем DOCSIS и их возможности

При использовании топологии HFC CATV (рис. 22.6) на базе оборудования CMTS можно построить как концентратор, так и центральные станции. Для этого можно использовать универсальный широкополосный маршрутизатор Cisco. uBR7246 представляет собой интегрированный маршрутизатор, поддерживающий до четырех модулей CMTS, каждый из которых имеет один нисходящий и от одного до шести восходящих портов. Кроме

того, для подключения к опорной сети универсальный широкополосный маршрутизатор может быть оборудован портовым адаптером, выбор которых весьма широк — от последовательного T1/E1 до Packet Over SONET (POS) и Dynamic Packet Transport (DPT) и от 10BaseT Ethernet до High-Speed Serial Interface (HSSI).

Система Cisco mBR10012 является последней разработанной корпорацией Cisco CMTS. Она имеет значительно большую производительность и обеспечивает большую избыточность, что дает возможность MSO обслуживать большее количество пользователей с меньшими затратами. Также разработана новая карта модема MC520, которая поддерживает пять нисходящих доменов RF и двадцать восходящих.

При подключении к опорной сети нужно учитывать размеры общих магистральных потоков данных и доступную среду передачи. По всей вероятности, в рассматриваемом примере опорная сеть будет соединять концентратор и центральную станцию и проходить по оптоволоконному кабелю, где все потоки данных сначала группируются маршрутизатором или IP-коммутатором, и только потом направится в Internet, либо в общедоступную коммутируемую телефонную сеть. Часто на центральной станции MSO имеются кэш-процессоры, позволяющие уменьшить полосу пропускания для Internet и, соответственно, затраты на аренду оборудования.

Нередко для коммутируемого доступа к Internet, речевых служб или обратной связи по телефону требуется подключение к общедоступной телефонной сети.

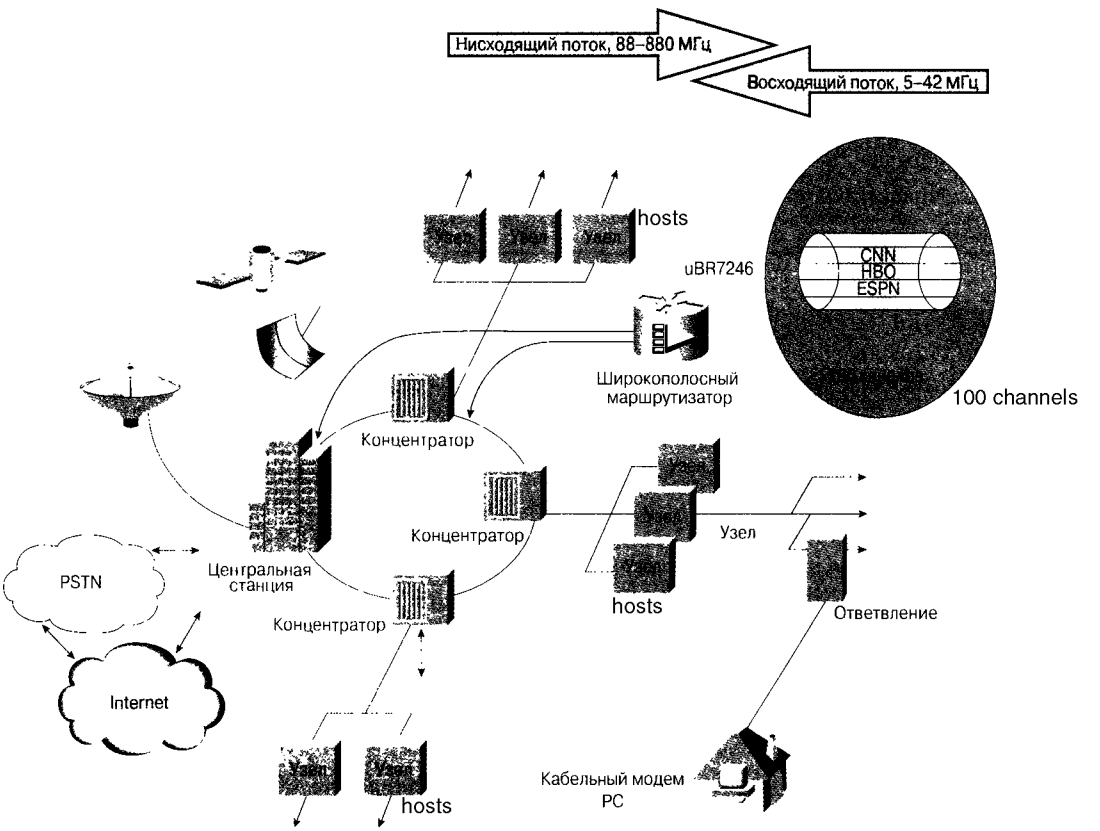


Рис. 22.6. Возможности использования систем CMTS в типичной сети HFC CATV

Обратная связь по телефону, иногда предоставляемая MSO, является временной мерой, к которой прибегают из-за того, что топология сети еще не обеспечивает двусторонней работы. В таких приложениях высокоскоростное нисходящее соединение обеспечивается сетью HFC, а восходящее соединение устанавливается по протоколу "точка-точка" (PPP), по телефонной сети с коммутируемым модемом у пользователя и сервером доступа, к которому он осуществляет электрическое подключение до соединения с Internet.

Рассмотрим инженерные особенности сети DOCSIS на простой коммерческой модели. Соответствующие бизнес-параметры приведены в табл. 22.9. Мы будем анализировать только частных клиентов и мелкие предприятия, обслуживаемые центральной станцией.

Таблица 22.9. Сводные данные пятилетнего бизнес-плана

Тип структуры	0,75% в год
Предоставляемые услуги по высокоскоростной передаче данных:	
Для частных лиц	256 Кбит/с DS и 128 Кбит/с US
Для мелких предприятий	1,5 Мбит/с DS и 512 Кбит/с US
Скорость развития:	
Для частных лиц	3% в первый год и 30% среднегодового роста в сложных процентах
Для мелких предприятий	2% во второй год и по 1% в год
Предположения:	
Коэффициент активности частных пользователей	25%
Коэффициент активности предприятий	25%
Коэффициент пика данных	8%

Согласно бизнес-плану, услуги DOCSIS предполагается предоставлять на территории, уже охваченной другими службами, с умеренным ростом, возможно, с ограниченными перспективами расширения круга частных пользователей в течение действия плана. Оператор намерен предлагать частным пользователям и малым предприятиям, находящимся в обслуживаемой зоне, одну и ту же услугу.

Скорость развития представляет собой процент зданий, находящихся в зоне обслуживания. Определяет количество клиентов, покупающих услугу.

Коэффициент активности представляет собой процент пользователей, активно использующих услугу, посылая или получая информацию.

Коэффициент пика представляет собой соотношение между видимой загрузкой полосы пропускания системы и реальной шириной полосы пропускания, физически предоставляемой CMTS. Достижение пика отражает, что передача данных пользователю обычно происходит практически мгновенно.

Характеристики, выделенный спектр и выбранная модуляция для кабельной инфраструктуры (центральная и обслуживаемая зоны) рассматриваемой сети приведены в табл. 22.10.

Центральная станция обслуживает зону из 25000 домов, распределенных между 25 оптическими узлами с восходящим CNR в пределах от 30 до 36 дБ. CNR — существенный параметр, так как он определяет количество узлов, которое можно объединить

в один приемный порт. Согласно требованиям DOCSIS, CNR должен составлять 25 дБ независимо от выбранной модуляции восходящего потока.

Таблица 22.10. Характеристика и доступный спектр частот зоны, обслуживаемой центральной станцией

Характеристики HFC	Нисходящий поток: 88–750 МГц Восходящий поток: 5–42 МГц
Зона, обслуживаемая центральной станцией	25000 домов 25 узлов (примерно по 1000 домов каждый) CNR колеблется между 30 и 36 дБ; в среднем — 32 дБ
Доступный спектр частот	Нисходящий поток: EIA-канал 60 дБ при 439,25 МГц Восходящий поток: 32 МГц, ширина полосы 800 КГц
Модуляция	Нисходящий поток: 64 QAM Восходящий поток: QPSK

Выбор QPSK и полосы пропускания в 800 КГц влияет на скорость обратной передачи данных.

По данным бизнес-плана составлен пятилетний план клиентуры и объема передачи данных, приведенный в табл. 22.11.

Как видно из таблицы, при условии, что видимая полоса пропускания обрабатывается на центральной станции оборудованием CMTS, количество домов и скорость развития заметно возросли.

Количество модулей CMTS, обслуживающих видимую нагрузку, должно определяться исходя из того, что используется Cisco uBR-MC16C, состоящий из одного порта для нисходящего и шести портов для восходящего потока. Однако прежде всего нужно выбрать подходящий сценарий группировки восходящего потока.

Рассмотрим комбинацию из трех узлов, у каждого из которых CNR составляет 36 дБ, что дает итоговый CNR приблизительно в 27 дБ и удовлетворяет критерию DOCSIS.

Нужно определить необходимое количество устройств CMTS:
25 узлов/3 узла на каждый приемник = 9 приемников, т.е. два uBR-MC16C.

Учитывая ограничение на восходящий поток в 800 КГц, накладываемое QPSK, выбор оборудования должен соответствовать анализу объема передачи данных для бизнес-плана (табл. 22.11).

Таблица 22.11. Клиентура и профиль передачи данных на центральной станции

	Год 1	Год 2	Год 3	Год 4	Год 5
Количество домов	25000	25188	25376	25666	25758
Частные пользователи	750	982	1286	1685	2207
Првдприятия		2	3	4	5
Суммарный объем передачи данных	DS 48M US 24M	DS 64M US 32M	DS 84M US 42M	DS 100M US 55M	DS 144M US 72M

- **Нисходящий поток**

  Два uBR-MC16C обеспечивают 2*27 = 54 Мбит/с, что значительно превышает требования пятого года — 144/8 = 18,1 Мбит/с (где 144 Мбит/с — видимая полоса пропускания, 8 — коэффициент пика данных).

- **Восходящий поток**

  Два uBR-MC16C с 9 активными приемниками, настроенными для QPSK и BW 800 КГц, обеспечивают 9*1,2 = 10,8 Мбит/с, а требования пятого года составляют 72/8 = 9 Мбит/с (где 72 Мбит/с — видимая полоса пропускания, 8 — коэффициент пика данных).

- **Предельное количество абонентов**

  Общее количество абонентов на пятом году составляет 2207+5 = 2212, что вполне попадает в предполагаемый предел в 1200 абонентов на каждую CMTS.

Как видно из анализа этого простого примера, начальное внедрение оборудования CMTS будет отвечать требованиям всего пятилетнего плана и даже больше, без необходимости усовершенствовать конфигурацию.

Перспективные приложения DOCSIS

В этой главе описана спецификация продуктов DOCSIS 1.0 для поддержки высокоскоростной передачи данных по кабельным сетям. Этот стандарт развивается в версии DOCSIS 1.1, которая поддерживает дополнительные службы и соответствующие им перспективные приложения, отвечающие потребностям рынка по обеспечению надежности и высокой доступности сетей.

Среди планируемых в будущем услуг и приложений — телефония, основанная на передаче речи по протоколу IP (VoIP), передача видео по IP в формате MPEG, качество обслуживания (QoS) и улучшенная безопасность. В то же время вводятся CM и устройства STB (Set Top Box), способные поддерживать эти и другие службы.

При условии одновременной поддержки таких новых служб и приложений во время планирования потребуется исходить из более обширных концепций.

Спецификация DOCSIS 1.1 предоставляет следующие функциональные усовершенствования по сравнению с сетями DOCSIS 1.0 на основе коаксиального кабеля:

- Улучшенное обеспечение качества обслуживания QoS, обеспечивающее приоритет данным реального времени, таким как голос и видео:
  - — Модель QoS версии DOCSIS 1.0 на основе ID службы (service ID — SID), связанного с профилем QoS, заменена моделью на основе потока службы (service-flow model), которая обеспечивает большую гибкость при назначении параметров QoS различным типам данных и реагировании на изменяющуюся полосу пропускания;
  - — Поддержка нескольких потоков служб для отдельных кабельных модемов позволяет одному кабельному модему поддерживать комбинацию обычных данных, голоса и видео;
  - — Большая индивидуализация QoS для каждого кабельного модема в обоих направлениях с использованием однонаправленных потоков служб;
  - — Динамические MAC-сообщения создают, модифицируют и удаляют потоки служб для данных, что позволяет поддерживать запросы по требованию;
- Для восходящего направления поддерживаются следующие модели QoS:
  - — Негарантированная доставка: передача данных на негарантированной основе;

— Согласованная скорость передачи информации (Committed information rate — CIR): гарантированная минимальная полоса пропускания;

— Предоставляемая без запроса (Unsolicited grants — UGS): постоянная битовая скорость передачи данных (Constant bit rate — CBR), таких как голосовые данные, характеризуемая регулярной передачей пакетов одинакового размера с фиксированными интервалами времени;

— Опрос в реальном времени (Real-time polling — RTPS): службы передачи данных реального времени, таких как видео, создающих одноадресатные пакеты различной длины с регулярными интервалами;

— Предоставляемая без запроса с обнаружением активности (Unsolicited grants with activity detection — USG-AD): сочетание UGS и RTPS для обработки данных реального времени, у которых могут быть периоды неактивности (таких как голосовые данные при использовании подавления пауз). Поток службы использует фиксированные UGS в периоды активности, однако переключается на опросы RTPS для предотвращения бесполезной затраты полосы пропускания во время неактивности.

- Усовершенствованные механизмы выделения тайм-слотов для поддержки гарантированной задержки для чувствительных к задержке данных при передаче по общему восходящему каналу множественного доступа;
- Подавление заголовка полезной нагрузки (Payload Header Suppression — PHS) экономит полосу пропускания на канальном уровне за счет подавления ненужных заголовков полезной нагрузки как в восходящих, так и в нисходящих потоках данных;
- Фрагментация на 2-м уровне в восходящем направлении предотвращает воздействие крупных пакетов данных на данные реального времени, такие как голосовые или видеоданные. Крупные пакеты данных фрагментируются и затем передаются в вакантные тайм-слоты, когда отсутствует передача данных реального времени;
- Конкантенация позволяет кабельному модему отправлять несколько MAC-фреймов в одном и том же таймслоте вместо запроса индивидуального гранта для каждого фрейма; это позволяет избежать напрасной затраты полосы пропускания в восходящем направлении при отправке большого количества очень мелких пакетов, таких как пакеты приветствия протокола TCP.
- Усовершенствованная аутентификация и защита путем использования цифровых сертификатов X.509 и шифрования по ключу Triple Data Encryption Standard (3DES).
- Безопасная загрузка программного обеспечения позволяет провайдеру службы удаленным образом обновлять программное обеспечение кабельного модема без риска перехвата или изменения передаваемых данных.

Резюме

В данной главе описана традиционная технология кабельного вещания по коаксиальным кабелям и указаны свойственные ей недостатки по сравнению с более совершенными службами. Рассмотрены также сети HFC и кратко приведены их преимущества по обеспечению высокоскоростной передачи данных.

Кроме того, описаны ограничения распространенных систем HFC, критерии доступности DOCSIS и необходимые характеристики кабельного оборудования с терминологией.

В этой главе также кратко описаны стандарт DOCSIS, сигнальный протокол, требуемые серверы поддержки, типичные характеристики продукции и приложения. Для отображения параметров и инструментов, необходимых для работы систем DOCSIS, перечислены типичные сообщения о состоянии CM, получаемые CMTS.

Дополнительно описаны перспективные услуги и приложения, опирающиеся на стандарт DOCSIS 1.1.

Контрольные вопросы

1. Опишите преимущества сетей HFC.
2. Как происходит двусторонняя передача данных в сетях HFC?
3. Каким условиям должны соответствовать полосы пропускания для восходящего и нисходящего потоков по стандарту DOCSIS?
4. Опишите критерии доступности DOCSIS.
5. Перечислите сетевые уровни DOCSIS.
6. Перечислите серверы DOCSIS 1.0. Каково их назначение?
7. Где MSO может установить универсальный широкополосный маршрутизатор?
8. Что такое обратная связь по телефону и когда она нужна?
9. Перечислите несколько будущих функций и приложений DOCSIS 1.1.

Дополнительные источники

Книги

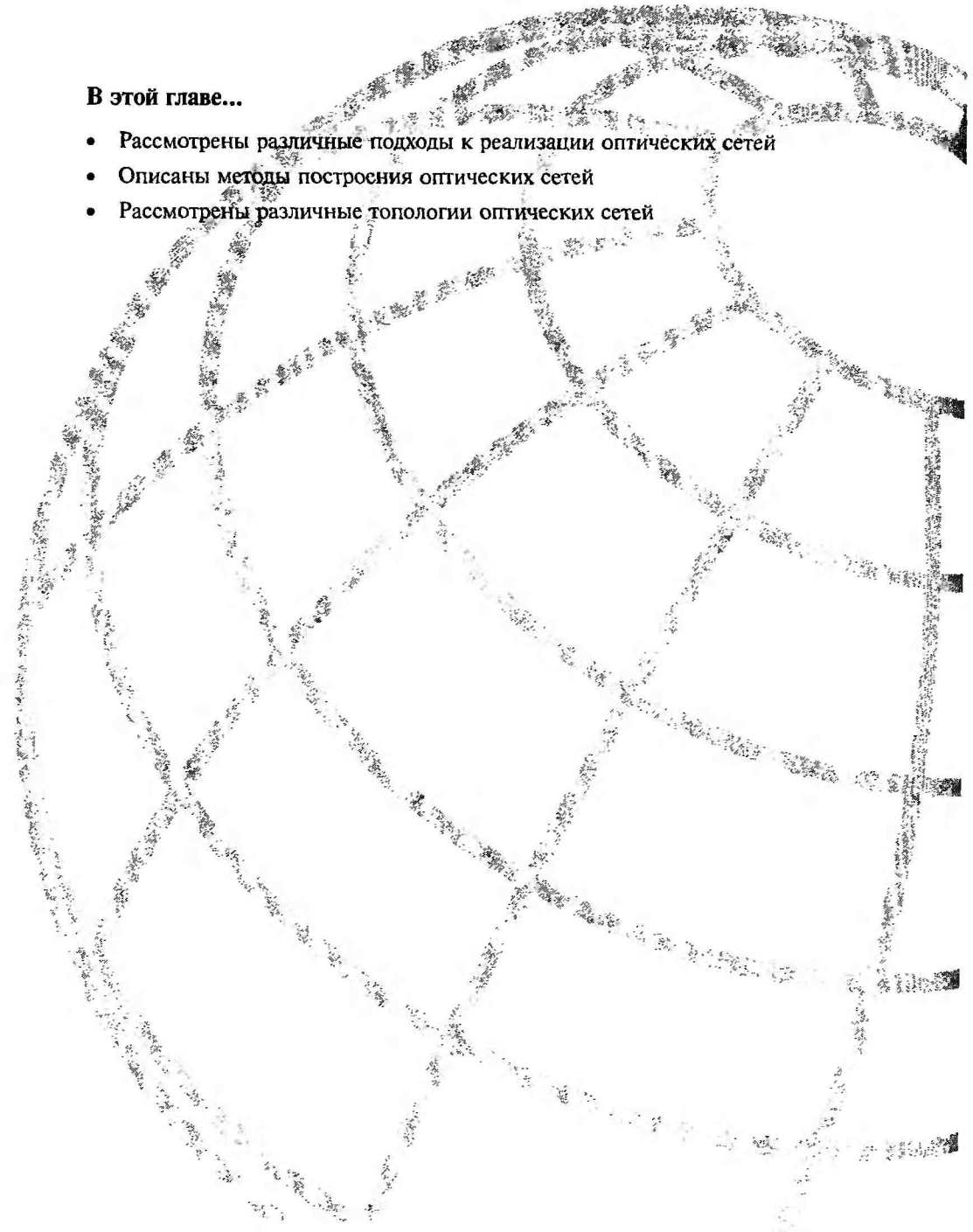
- Azzam, Albert, and Niel Ransom. *Broadband Access Technology.* New York: McGraw-Hill, 1999.
- Ciciora, Walter, James Farmer, and David Large. *Modern Cable Television Technology.* Boston: Morgan Kaufmann Publishers Inc., 1998.
- Grant W. *Cable Television,* Third Edition. New York: GWG Associates, 1997.
- Raskin, Donald, and Dean Stoneback. *Broadband Return Systems for Hybrid Fiber/Coax Cable TV Networks.* New York: Prentice Hall PTR, 1997.
- Thomas J. *Cable Television: Proof of Performance.* New York: Prentice Hall PTR, 1995.

Адреса URL

- www.cablelabs.com
- www.cablemodem.com
- www.cabletelephony.com
- www.catv.org/modem.com

Периодические издания

- *Cablevision.* 8773 South Ridgeline Blvd., Highland Ranch, Co 80126. http://www.cablevisionmag.com.
- *Cableworld.* Intertec Publishing, Primedia Company, 9800 Metcalf Ave., Overland Park, KS 66212-2215. http://cableworld.com.
- *CED (Communications Engineering & Design).* P.O. Box 266007, Highland Ranch, CO 80163-6007. http://www.cedmagazine.com.



В этой главе...

- Рассмотрены различные подходы к реализации оптических сетей
- Описаны методы построения оптических сетей
- Рассмотрены различные топологии оптических сетей

Глава 23

Введение в технологии оптических сетей

Оптические сети предоставляют возможность транспортировки аудио-, видео- и обычных данных с помощью оптической передачи и систем коммутации. В настоящей главе рассматриваются традиционные структуры, такие как SONET/SDN и новые подходы, такие как использование протокола IP с DWDM-мультиплексированием, технологий Gigabit Ethernet и ATM. В последнее время была начата разработка оборудования и создание органов стандартизации, которые определяют средства сигнализации и коммутации в оптических сетях. В настоящей главе обсуждаются последние разработки в области управлении и контроля оптических сетей таких организаций, как IETF, OIF и ITU.

Что такое оптическая сеть?

Под оптическими сетями понимаются сети, которые обеспечивают оптические маршруты между провайдерами служб и пользователями. С помощью оптических сетей осуществляются соединения между корпорациями и частными помещениями для передачи данных по оптоволоконному кабелю (Fiber To The Home — FTTH). Оптические сети предоставляют необходимую инфраструктуру для удовлетворения требований относительно пропускной способности в настоящее время и в будущем. Оптические передающие среды позволяют работать в сети узкополосным, широкополосным и широковещательным приложениям. По мере того как возрастает потребность в более широкой полосе пропускания, оптические сети становятся единственной средой, способной удовлетворить эти постоянно возрастающие требования.

Развитие оптических сетей требует углубленного обсуждения их функционирования. Существует и используется большое количество структур, устройств, кроссоединений и коммутаторов. В настоящем разделе рассматриваются только реальные реализации оптических сетей; при этом особое внимание уделяется крупным сетям. Оптическим сетям присущи и определенные электрические характеристики; по этой причине в настоящей главе рассматривается также унаследованное оборудование сетей предприятий и провайдеров служб.

В последующих разделах кратко описываются различные типы оптических сетей.

Мультиплексирование по частотам и мультиплексирование с уплотнением по частотам

Мультиплексирование по частотам и мультиплексирование с уплотнением по частотам обеспечивают оптические маршруты к провайдерам служб и от них, используя оптические устройства с высокой плотностью каналов. Союз ITU разработал спецификации для оптических передатчиков, использующих различные методы фильтрации (таких, в частности, как дифракционные волновые решетки (Arrayed Waveguide Grating — AWG) и оптические усилители (такие как EDFA), которые позволяют работать как с коммутируемыми каналами, так и с каналами данных.

Оптический кабель к домашнему офису пользователя (Fiber to the Home — FTTH)

Оптические сети могут предоставлять оптические маршруты непосредственно от провайдера службы к домашнему офису пользователя. Использование оптических инфраструктур позволяет провайдерам службы коммерчески эффективно предоставлять полосу пропускания непосредственно потребителям. Для телеработников использование FTTH предоставляет настоящее широкополосное соединение. FTTH позволяет объединять данные мультимедийных приложений и допускает расширение полосы пропускания по мере необходимости.

Полностью оптические сети

Под полностью оптическими сетями (All-Optical Network — AON) понимаются сети, обеспечивающие сквозные оптические маршруты между провайдерами служб и пользователями. Полностью оптические сети дают возможность передавать данные и коммутировать каналы и пакеты используя только оптическую форму сигналов. Передавая данные и осуществляя коммутацию в такой форме, промышленные потребители и провайдеры служб могут уменьшить количество оборудования, требуемого для регенерации электрических сигналов. Преимущество использования AON состоит в значительном уменьшении стоимости создания оптической сети и управления такой сетью.

Сети позволяют предоставлять службы непосредственно по оптоволоконному кабелю без промежуточных уровней, иными словами, оставаясь на физическом или световом уровне. Поскольку при передаче световых квантов по оптоволоконному каналу возникают различные проблемы, для их разрешения сетевыми провайдерами используются электрические усилители и регенераторы. В сетях AON используются методы передачи изолированных волн с помощью оптических усилителей (Raman) по оптоволоконному кабелю, что позволяет избежать операций электрической регенерации, восстановления формы и синхронизации. Аналогично фотонам, изолированные волны имеют дистанционные ограничения; однако их настройка и восстановление формы могут быть выполнены на физическом уровне. AON-сети, использующие коммутацию, также могут быть реализованы на световом уровне. Некоторые оптические методы (такие, как MEMS) позволяют коммутировать световые сигналы.

Все оптические сети делятся на оптические сети городского масштаба (metropolitan area network — MAN) и базовые оптические сети (также называемые междугородными — long-haul network).

Оптические сети городского масштаба

Взрывной рост Internet и промышленных приложений порождает потребность в распределенных сетях предприятий и провайдеров служб. Например, такие приложения, как электронная коммерция, консолидированное хранение и интеграция служб, изменяют весь характер работы промышленных пользователей и провайдеров служб. Службы оптических сетей городского масштаба включают в себя доступ к сети и использование базовой службы MAN. Оптические сети MAN соединяют между собой центральные офисы и/или точки присутствия службы (Point Of Presence — POP) и базовые точки подписчика (сети доступа). Для последующей передачи службы обычно группируются в крупные магистрали данных/каналов.

Базовые оптические сети

Базовые оптические сети расположены между центральными офисами и/или точками присутствия (POP) службы и соединены друг с другом с помощью оптоволоконного кабеля, способного передавать данные на большие расстояния (long-haul), дальние расстояния (extended long-haul) и сверхдальние расстояния(ultra long-haul). Объединенные данные служб оптических сетей городского масштаба передаются на большие расстояния к другим центральным офисам и/или точкам присутствия POP-служб. Более подробное описание такой передачи приведено в разделах "Сети для передачи данных на большие расстояния", "Сети для передачи данных на дальние расстояния", и "Сети для передачи данных на сверхдальние расстояния".

Пассивные оптические сети

Пассивные оптические сети (Passive Optical Network — PON) могут быть подразделены на две категории — домашние (residential) и коммерческие (business). Хотя сети PON могут рассматриваться как зрелая и установившаяся технология, они все же не достигают уровня крупномасштабной реализации. Сети PON состоят из модулей оптической сети (Optical Network Unit — ONU) и терминалов оптических сетей (Optical Network Terminal — ONT).

Обычно сети PON создаются в тех случаях, когда пользователи пытаются извлечь финансовые преимущества из асимметричных требований к полосе пропускания. Использование экономичных оптических разделителей позволяет передавать оптическую энергию (сигналы) в несколько различных мест. Обычно потоки данных в нисходящем направлении (потоки данных от провайдера службы) к пользователю требуют большей полосы пропускания, чем восходящие потоки данных (от пользователя). Используются также недорогие оптические трансиверы (приемопередатчики) с распределенной обратной связью (distributed feedback — DFB). В большинстве случаев сети PON используются компаниями, предоставляющими кабельные службы и соответствующее оборудование. Сеть PON может также быть частью гибридной сети. Гибридные сети используют небольшую стоимость сетей PON для предоставления пользователям объединенных широкополосных мультимедиа-служб, а также существующих унаследованных узкополосных служб.

Домашние и коммерческие PON-сети

У сетей PON имеется два вида пользователей —коммерческие и частные (домашние) пользователи. Коммерческим пользователям требуется более широкая

полоса пропускания, чем частным; в действительности, коммерческие пользователи могут даже продавать службы частным пользователям по той же самой инфраструктуре. Сети PON представляют собой решение задачи оптического доступа, которое не требует дополнительных затрат энергии и позволяет обслуживать несколько малых/домашних офисов (Small Office/Home Office—SOHO), коммерческих фирм и частных пользователей по одному оптоволоконному кабелю. Информация передается между пользователем и службами коммерческого приложения. По договоренности с провайдером пользователи могут получать либо свою собственную отдельную длину волны, либо поток данных. Обычно требования домашних пользователей к полосе пропускания ограничиваются некоторым максимальным объемом потока данных. Офисы SOHO и другие коммерческие пользователи обычно получают более широкую полосу пропускания и их потоки данных более симметричны, чем у домашних пользователей. При построении сети PON требования коммерческих пользователей и домашних пользователей рассматриваются и дифференцируются с помощью различных видов соглашений об уровне обслуживания (Service Level Agreement — SLA).

Модули оптических сетей и терминалы оптических сетей

Модули оптических сетей (Optical Network Unit — ONU) используются для агрегирования (объединения) терминалов оптических сетей (Optical Network Terminal — ONT). Терминалы ONT используются коммерческими и домашними пользователями в качестве терминирующего оборудования службы для доставки данных из сети и/или передачи данных в сеть. Обычно один модуль ONU может обслуживать до 32 терминалов ONT. Модули ONU, как правило, расположены в центральном офисе и/или в удаленном здании; в тех случаях, когда оборудование является устойчивым к значительным колебаниям температуры, они могут быть установлены на каком-либо возвышении.

Пассивные оптические сети Ethernet

Пассивные оптические сети Ethernet (Ethernet Passive Optical Network — EPON) предоставляют службы Ethernet или службы протокола IP непосредственно по оптоволоконному кабелю без участия уровней ATM или SONET. При использовании служб гигабитового Ethernet (Gigabit Ethernet — GE) и/или 10-гигабитного Ethernet (10-Gigabit Ethernet — 10GE), данные которых непосредственно используются DWDM-мультиплексированием, провайдеры служб могут коммерчески эффективно предоставлять пользователям широкополосные и узкополосные службы Ethernet/IP. Более подробно о сетях PON рассказывается в разделе "Пассивные оптические сети".

Сети доступа городского масштаба (сети MAN)

Современное состояние окружающей среды и условия работы предприятий и провайдеров служб изменили ландшафт традиционных сетей. Традиционные сети доступа обычно включали в себя все оборудование, находящееся в радиусе 40 км от центра коммутации службы (POP, TDM-коммутатор и т.д.). Сети MAN в на-

стоящее время могут включать в себя MAN-сети доступа и базовые MAN-сети благодаря интегрированным решениям DWDM. Это позволяет предприятию и провайдерам службы иметь metro-сети доступа в радиусе от 40 до 80 км и базовые MAN-сети в радиусе до 200 км.

Как MAN-сети доступа, так и базовые MAN-сети, позволяют провайдерам службы собирать потоки данных пользователя и, в некоторых случаях, обеспечивать коммутацию и маршрутизацию в сети, если в этом есть необходимость. Если требуется обработка данных и их передача, то эти функции осуществляются в точке присутствия POP и/или коммутирующем центре межофисного оборудования.

Прозрачные оптические сети

Пользователи, которым необходимо прозрачно передавать свои службы без постороннего вмешательства, используют прозрачные оптические сети. Обычно пользователям требуется передавать конфиденциальные данные, а также данные, которые они или их партнеры не хотят реформатировать в существующих унаследованных или новых системах следующего поколения. В сущности, прозрачные оптические сети предоставляют пользователям возможность передать свои оптические сигналы преобразователям (transponders), которые не принимают во внимание скорость передачи по оптической линии и не влияют на нее и на способ создания фреймов. Прозрачные оптические преобразователи встречаются в сетях доступа, MAN-сетях и в транспортных сетях.

Транспортные сети

Транспортные сети осуществляют оптическое соединение между городскими сетями доступа и базовыми городскими сетями. Транспортные сети используют оборудование передачи данных на большие (long-haul), дальние (extended long-haul) и сверхдальние (long-haul) расстояния для предоставления предприятиям и провайдерам служб транспортных каналов для всех служб на расстояниях от 80 до 200 км. Сети OTN используют спроектированные союзом ITU и/или компанией Telcordia (BellCore) системы для передачи данных, обработанных или коммутируемых с помощью TDM и/или иных потоков данных в другие коммутирующие центры и из них, IOF, а системы SONET, SDH и PDH используются в транспортных сетях.

Сети передачи данных на большие расстояния

Возможность передавать службы каналов и данных между большими MAN-сетями доступа является в высшей степени желательной. Сети передачи данных на большие расстояния (Long-Haul — LH) обеспечивают передачу обработанных данных, данных канальных и пакетно-агрегированных служб между центральными офисами, а также между центральными офисами и точками присутствия (POP) служб. Это осуществляется с использованием лазеров WDM- и DWDM-мультиплексирования, фильтров и оптических усилителей.

Пакетные и канальные потоки данных обрабатываются в центрах коммутации и центрах IOF, после чего плотно упаковываются для создания оптической полезной нагрузки, которая будет оптическим путем передаваться в восходящем на-

правлении на расстояние до 600 км другим центрам коммутации, IOF-центрам или пользователям.

Скорости передачи по оптической линии для междугородных сетей обычно соответствуют стандартам OC-48/STM-16 и OC-192/STM-64. Расстояние и мощность определяются типом лазера, оптоволоконного кабеля и типом мультиплексирования. Использование непосредственно подсоединенных электрических преобразователей позволяет электрически регенерировать оптические сигналы, выполнять повторную синхронизацию и заново создавать фреймы, что позволяет восстановить форму оптического сигнала и увеличить дальность его распространения.

Сети передачи на дальние расстояния

Такие сети представляют собой относительно новую сетевую топологию, которая позволяет провайдерам предоставлять службы на расстояниях междугородных и сверхдальних сетей. При использовании гибридной техники EDFA и усиления Raman могут быть достигнуты расстояния передачи от 600 до 2500 км. Сети дальней передачи (Extended Long-Haul — ELH) позволяют коммерчески эффективно передавать с помощью оптических сигналов пакетные потоки данных и канальные потоки данных без необходимости использовать оптическую регенерацию на расстояниях до 2500 километров.

Сети передачи на сверхдальние расстояния

Сети передачи на сверхдальние расстояния (Ultra-Long-Haul — ULH) используются для потоков данных, которые требуется передавать на расстояния свыше 600 км. Сети ULH могут быть также использованы в тех же областях, где используются сети LH и ELH. Однако в основном сети ULH используются на расстояниях в несколько тысяч километров, включая подземные оптические сети или океанские сети. Наземные оптические ULH-сети используются в тех случаях, когда использование электрических регенераторов деласт их развертывание экономически выгодным.

При этом обычно используется AON-технология, позволяющая передавать оптические сигналы без электрической регенерации, повторной синхронизации и восстановления формы сигнала. Системы световой передачи не требуют оптоэлектронной регенерации. Следует отметить, что для передачи данных в сетях ULH требуется большое количество электрических регенераторов и мультиплексоров обрыва и вставки (Add Drop Multiplexer — ADM). Отсутствие необходимости в электрических регенераторах и мультиплексорах ADM позволяет добиться значительной операционной и финансовой экономии. Сети ULH предоставляют тот же самый уровень восстановления данных, инициализации и производительности сети, как и у традиционных сетей SONET/SDH.

На рис. 23.1 проиллюстрирована сложность оптических сетей ULH. При использовании оптического Raman-усиления провайдеры могут уменьшить количество электрических регенераций и используемого оборудования. Это особенно важно в вопросах операционной поддержки, в частности, в подземных и в океанских оптических сетях.

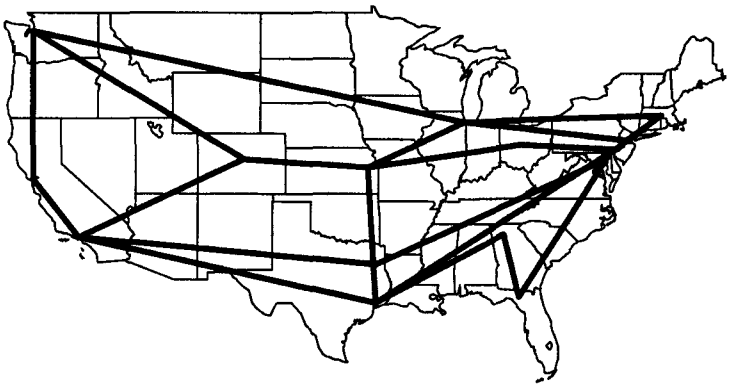


Рис. 23.1 Сеть передачи на сверхдальние расстояния

Оптические сети Gigabit Ethernet и 10 Gigabit Ethernet

Непосредственные преобразования Gigabit Ethernet (GE) и 10 Gigabit Ethernet (10GE) в оптическую сеть позволяет коммерчески эффективно удовлетворить требования пользователя к широкой полосе пропускания в настоящее время и в будущем. Непосредственная работа протокола IP по оптической линии не требует неблокирующих кросс-соединений, которые требуются для масштабируемости оптического порта. Устройства GE и 10GE могут использовать функции 1-го, 2-го и 3-го уровней, что увеличивает функциональность службы, ее производительность и расширяемость. Оптические сети GE и 10GE могут быть соединены между собой с помощью высокопроизводительных маршрутизаторов, что обеспечивает масштабируемость, восстановление и прозрачность побитовой передачи. Пакетные сети не имеют границ для службы и физического уровня.

Обобщенная многопротокольная коммутация по метке

Обобщенная многопротокольная коммутация по метке (Generalized Multiprotocol Label Switching — GMPLS), предложенная проблемной группой Internet Engineering Task Force (Internet Engineering Task Force — IETF), позволяет маршрутизаторам, коммутаторам (пакетным и канальным), сетям DWDM, ADM, световым кросс-соединениям (Photonic Cross-Connects — PXC) и оптическим кросс-соединениям (Optical Cross-Connects — OXC) динамически предоставлять ресурсы. Коммутация GMPLC также обеспечивает защиту и восстановление предоставляемых служб.

Коммутация GMPLS поддерживает наложение, одноранговые соединения и усовершенствованную модель, используемые для обеспечения управляющей плоскости для сетей TDM (таких как PDH, SDH/SONET и G.709), сетей DWDM и световой коммутации. Составляющими этих моделей являются синхронизация, сигнализация и маршрутизация.

В приведенных ниже разделах описываются только аспекты высокого уровня коммутации GMPLS. Дополнительная информация может быть получена из RFC 3031 и 2026, а также на форуме группы IETF.

Маршрутизаторы с коммутацией по метке

В RFC 3031 не определяются границы пакетов или ячеек, что делает невозможной пересылку данных, полученных из информации заголовка пакета или ячейки. Маршрутизаторы с коммутацией по метке (Label Switch Routers — LSR), которые передают такие пакеты и ячейки, могут осуществлять такую пересылку. Описанные ниже LSR-устройства, определенные группой IETF, поддерживают решения о пересылке, основанные на тайм-слотах, длине волны и оптических портах.

- **Интерфейсы, осуществляющие пакетную коммутацию (Packet Switch-Capable interfaces — PSC).** Интерфейсы, которые распознают границы пакетов и могут направлять данные исходя из содержания заголовка пакетов. В качестве примера можно привести интерфейсы маршрутизаторов, которые передают данные, основываясь на содержании заголовка и маршрутизаторов, пересылающих данные исходя из содержания промежуточного заголовка коммутации по метке (Multiprotocol Label Switching — MPLS).
- **Интерфейсы 2-го уровня, способные осуществлять коммутацию (Layer 2 Switch-Capable interfaces — L2SC).** Эти интерфейсы распознают границы фрейма/ячейки и могут пересылать данные исходя из содержания заголовка фрейма/ячейки. В качестве примера можно привести интерфейсы на мостах Ethernet, которые пересылают данные исходя из содержания MAC-заголовка, и интерфейсы на LSR-устройствах ATM, которые пересылают данные, согласно ATM-идентификаторам VPI/VCI.
- **Интерфейсы, осуществляющие мультиплексирование с разделением времени (Time-Division Multiplexing Capable interfaces).** Такие интерфейсы пересылают данные согласно тайм-слоту данных в повторяющемся цикле. В качестве примера можно привести кросс-соединение SDH/SONET (Cross-Connects — XC), терминальные мультиплексоры (Terminal Multiplexer — TM) и ADM. В качестве другого примера можно привести интерфейсы, предоставляющие возможности G.709 TDM ("Digital wrapper") и интерфейсы PDH.
- **Интерфейсы Lambda-коммутации.** Такие интерфейсы пересылают данные, основываясь на длине волны, на которой данные были получены. Примером такого интерфейса может служить фотонное кросс-соединение (Photonic Cross-Connect — PXC) или оптическое кросс-соединение (Optical Cross-Connect — OXC), которые функционируют на уровне индивидуальной длины волны. В качестве дополнительного примера можно привести интерфейсы PXC, которые функционируют на уровне группы длин волн — интерфейсы длины волны и G.709, предоставляющие оптические функции.
- **Интерфейсы с коммутацией оптоволоконных каналов.** Такие интерфейсы пересылают данные исходя из расположения данных в физическом (real-world) пространстве. Примерами таких интерфейсов могут служить PXC или OXC, которые функционируют на уровне отдельного оптоволоконного кабеля или нескольких таких кабелей.

Между двумя интерфейсами одного и того же типа или через них может быть установлен канал. В зависимости от конкретной технологии, используемой для каждого интерфейса, могут использоваться различные типы каналов, такие как канал SDH, оптический trail и световой маршрут. В контексте коммутации GMPLS все эти каналы называются общим именем: маршрут с коммутацией по метке (Label-Switched Path — LSP).

Концепция вложенных маршрутов LSP (LSP внутри других LSP), доступная уже в традиционной коммутации MPLS, облегчает построение иерархии пересылки — иерархии маршрутов LSP. Эта иерархия маршрутов LSP может происходить на одном и том же интерфейсе или между различными интерфейсами. Например, иерархия может быть построена в том случае, если интерфейс может мультиплексировать несколько маршрутов LSP от одной и той же технологии (уровня) — т.е. LSP SDH/SONET более низкого порядка, вложенная в LSP SDH/SONET более высокого порядка (VC-4). Некоторые уровни вложения сигналов (LSP) определены в иерархии мультиплексирования SDH/SONET.

Гнездовое вложение может происходить также между интерфейсами. В верхней части иерархии находятся интерфейсы FSC, за ними следуют интерфейсы LSC, интерфейсы TDM, интерфейсы L2SC и интерфейсы PSC. Таким образом, маршрут LSP, который начинается и заканчивается на интерфейсе PSC, может быть вложен (с другими маршрутами LSP) в маршрут LSP, который начинается и заканчивается на интерфейсе L2SC. Такой маршрут LSP в свою очередь может быть вложен (вместе с другими маршрутами LSP) в маршрут LSP, который начинается и заканчивается на интерфейсе TDM. В свою очередь, этот маршрут LSP может быть вложен (вместе с другими LSP) в маршрут LSP, который начинается и заканчивается на интерфейсе LSC, который в свою очередь может быть вложен (вместе с другими LSP) в маршрут LSP, который начинается и заканчивается на интерфейсе FSC.

Протокол управления каналом

Протокол GMPLS изначально основывается на протоколах расширенной маршрутизации и сигнализации с использованием протокола IPv4 (и IPv6 в будущем) для адресации. Однако использование маршрутов LSP предполагает рассмотрение вопросов по созданию фрейма, защитной коммутации и т.д. По этой причине для сигнализации требуется протокол управления каналом (Link Management Protocol — LMP). Протокол LMP в целом обычно рассматривается в тех случаях, когда протокол открытия кратчайшего пути (Shortest Path First — SPF) оказывается недостаточным.

От этих протоколов маршрутизации зависит анализ состояния ресурсов и топологии доменов. Плоскости управления и данных GMPLS разделены, поэтому требуется протокол LMP для поддержки обмена информацией между каналами TE и соседними узлами. Протокол LMP предоставляет механизм для поддержки соединения управляющих каналов (поддержка управляющих каналов протокола IP), для проверки физических соединений каналов, переносящих данные (тестирование каналов), для корреляции информации о свойствах канала (корреляция свойств канала) и для управления сбоями каналов (локализация сбоев и уведомление о них).

Большинство управляющих каналов для GMPLS требует, чтобы протокол IP передавал данные для протоколов сигнализации и маршрутизации (таких как протокол LMP). GMPLS не указывает, каким образом это должно делаться. Решение этих во-

просов предоставлено производителю. Управляющие каналы для GMPLS могут быть внутриполосными или внеполосными.

Протокол LMP обеспечивает менеджмент управляющих каналов (несколько длин волн, используемых между оптическими коммутаторами) и корреляцию свойств каналов. Тестирование соединений каналов и управления сбоями также могут быть рассмотрены в LMP, но группой IETF такое решение не считается обязательным.

Управляющий канал LMP и менеджмент управляющих каналов

Управляющий канал LMP (LMP Control Channel — CC) и менеджмент управляющего канала (Control Channel Management — CCM) используется для установки и поддержи узловых управляющих каналов. CC используется для обмена информацией управляющей плоскости MPLS. Маршрутизация, сигнализация и менеджмент каналов могут совместно использоваться между узлами. Эти каналы CC могут быть сконфигурированы динамически или статически. Каждому каналу CC предоставляется возможность обсуждать и поддерживать соединения с использованием протокола hello. Протокол hello может быть рассмотрен как упрощенный вариант сообщений об активности при сбоях в каналах, что позволяет осуществлять смежные соединения на канальном уровне. Протокол LMP требует, чтобы один управляющий канал всегда был доступен.

CCM осуществляет менеджмент и/или обсуждает обмен информацией управляющей плоскости. Управление сбоями, инициализация канала, управление маршрутом и распределение меток используется совместно между каналами в одном или более двухсторонних управляющих каналов. Инициализация управляющего канала осуществляется статически или автоматически, при этом CCM инициализирует IP-адрес на дальнем конце управляющего канала. CCM использует протоколы сигнализации, такие как RSVP-TE (RFC 3209), и расширение протоколов для перераспределения потоков, таких как OSPF-TE и IS-IS-TE для распределения каналов и управления маршрутами соответственно.

Свойства каналов

Протокол LMP также определяет корреляцию свойств каналов, которая используются для агрегирования нескольких каналов данных. Отдельные составляющие канала объединяются в пучок и коррелируются, обмениваются или модифицируются. Корреляция свойств канала (Link property — LP) может быть установлена, когда канал доступен, но не на стадии тестирования.

Интерфейсы PSC и иные интерфейсы наряду с узлами IP и маршрутизаторами могут быть легко идентифицированы по IP-адресам. При использовании протоколов маршрутизации IP маршруты для IP дейтаграмм могут маршрутизироваться с использованием алгоритма SPF. Каналы, отличные от каналов PSC, могут найти маршруты с использованием алгоритма CSPF.

Интерфейс "пользователь–сеть"

Для GMPLS важно, чтобы существующие протоколы IP-маршрутизации могли быть использованы для уровней, отличных от PSC. Последнее время наблюдается значительное развитие и обогащение функций этих протоколов, таких как внутридоменная маршрутизация (на канальном уровне) и междоменная маршрутизация (политика). Это особенно интересно для провайдеров, использующих модель наложения. Уровни, отличные

от PSC, могут быть автономными. Междоменная маршрутизация (такая как протокол BGP) может быть использована для информации о маршрутах в автономных сетях. Очевидно, это предоставляет огромные преимущества провайдерам, которые уже в настоящее время используют междоменную маршрутизацию. Сегментация внутридоменных областей может обеспечить домены маршрутизации с использованием протокола IS-IS или протокола OSPF (на канальном уровне) маршрутизации для TE. Интерфейс "пользователь–сеть" (User-to-Network Interface — UNI) представляет собой канал между узлом GMPLS и LSR-устройством GMPLS (со стороны сети). Интерфейс "сеть–сеть" (Network -to-Network Interface — NNI) представляет собой интерфейс между двумя сетевыми LSR-устройствами. Исторически GMPLS рассматривала UNI и NNI одновременно и создало различия для GMPLS. В настоящем разделе не рассматривается это различие; здесь только указывается о том, что оно существует. Спецификация UNI OIF представляет собой клиентскую спецификацию для SDH/SONET, которая предназначена для модели наложения. В настоящее время UNI OIF не поддерживает Digital Wrapper G.709 или другие фотонные сетевые модели. GMPLS предполагает, что UNI OIF представляет собой подмножество GMPLS.

Спецификация G.ASON

Спецификация ITU G.ASON (Automatic Switched Optical Networks — ASON) использует рекомендации по структуре транспортной сети (G.803, G.805, G.872 и I.326) и другие.

G.ASON использует управляющую плоскость для конфигурирования коммутируемых и постоянных программируемых соединений на транспортном уровне. При этом требуется повторное конфигурирование соединений или возможность модифицировать соединение при обеспечении восстановления. Более подробные технические подробности по G.ASON приведены в рекомендации ITU T-REC-G.8080.

G.ASON главным образом описывает структуру и требования к компонентам управляющей плоскости в SDH и PDH для того, чтобы позволить ресурсам транспортной сети установить, поддерживать и отключать соединения для G.ASON для выполнения сигнализации и предоставления служб соединений управляющей плоскости между тремя различными плоскостями — контроля, управления и транспортировки. Управление вызовом и управление соединением обеспечиваются с помощью сигнализации, при этом управляющая плоскость устанавливает и разрывает соединение (я). В этот процесс включено также восстановление соединения.

Взаимодействие (сбои, Qos и т.д.) между транспортной плоскостью и управляющей плоскостью позволяет транспортной плоскости обновлять статус соединения для управляющей плоскости, когда это требуется.

Управляющая плоскость

Управляющая плоскость поддерживает статус канала (мощность, сбои) для поддержки установки/разрыва соединений и их восстановления.

Домены используются для того, чтобы можно было осуществить подразделение управляющих плоскостей. При необходимости транспортные плоскости также могут быть подразделены на такие же плоскости. Подразделение доменов позволяет осуществлять их отдельное администрирование — это очень желательно для провайдеров служб, которые заинтересованы в географическом разнообразии и использовании различного оборудования. Интерфейс UNI представляет собой точку ссылки (сопряжения) между

точкой административного управления и конечным пользователем. Интерфейс E-NNI представляет собой точку сопряжения между доменами. Интерфейс I-NNI представляет собой точку сопряжения между областями маршрутизации и набором управляющих компонентов там, где они применимы.

Политики используются в различных точках сопряжения (UNI, I-NNI, и E-NNI) и для них являются уникальными. В табл. 23.1 приведены различные политики, применяемые для управления вызовом, управления соединением и для маршрутизации. Адресация различных элементов в управляющей плоскости G.ASON необходима для различных элементов, включая управление соединением, SNNP, область маршрутизации, управление вызовом вызывающей/вызываемой стороны, управление сетевым вызовом и транспорт UNI. Адресующие элементы могут быть уникальным образом назначены G.ASON и после этого использованы глобально и/или внутри области. Обнаружение ресурсов осуществляется статически или автоматически с помощью функций UNI, E-NNI и I-NNI.

Таблица 23.1 Функции политик

	UNI	I-NNI	E-NNI
Управление вызовом	Да	Да	Да
Обнаружение ресурсов	Да	Да	Да
Управление соединением	Да	Да	Да
Выбор соединения	Да	Да	Да
Маршрутизация соединения		Да	Да

Операционный опыт, приобретенный при использовании текущих технологий транспортных сетей, и новые технологии стремительно эволюционируют (использование пакетов переменного размера, высокоскоростные транспортные сети и ASON), поэтому должны быть усовершенствованы или разработаны новые стандарты систем транспортных сетей и оборудования.

Объединенная плоскость управления

Существует несколько подходов к управлению плоскостью оптического управления. Их объединяет необходимость в непосредственной сигнализации. Объединенная плоскость управления (Unified Control Plane — UCP) представляет собой метод, который позволяет сетям OTN осуществлять сигнализацию для отдельных узлов. Преимущество UCP состоит в том, что полоса пропускания (обычно большой ширины) может быть использована гораздо более эффективно. Большинство (если не все) разработанных UCP можно назвать фирменными. Однако это не означает, что они не могут и не будут взаимодействовать с другими реализациями UCP.

UCP представляет собой программное обеспечение, предоставляющие возможности адресации, маршрутизации и сигнализации. Оно работает на IP-маршрутизаторах (таких как GSR и 7600) и в элементах оптических сетей (таких как 15454, 15600, 15801 и 15200), где управляющие функции объединены через разрозненные технологические уровни, что делает управление независимым от транспортировки.

В промышленности определены различные модели. Наиболее популярными являются модель наложения и одноранговая модель. Одноранговая модель имеет только одну общую управляющую плоскость для 3-го уровня и оптических сетей.

Модель наложения

Модель наложения определяет два административных домена — один для IP-уровня и один для оптического уровня. Каждый уровень использует свою собственную управляющую плоскость и интерфейс пользователя оптической сети (Optical User Network Interface — O-UNI) для коммуникации с другими уровнями. (см. рис. 23.2).

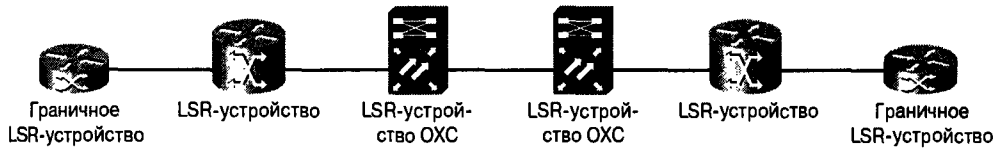


Рис. 23.2 Общая управляющая плоскость

Одноранговая модель

В телекоммуникационной индустрии в настоящее время разрабатывается несколько новых проектов плоскости оптического управления (Optical Control Plane — OCP). Конечной целью деятельности всех этих органов стандартизации является обеспечение автоматизированной сквозной инициализации оптической сети с добавлением восстановления полносеточной топологии. Ниже приведено краткое описание органов стандартизации и те аспекты, на которых фокусируются их инициативы по разработке OCP.

- Форум по объединенным оптическим сетям (Optical Internetworking Forum — OIF) работает над реализацией соглашения для интерфейса UNI между средой оптического интерфейса и клиентами.
- Группа IETF работает над стандартом, который расширяет возможности коммутации MPLS по управлению частотами и каналами в дополнение к управлению пакетами.
- Группа ITU работает над стандартом оптического управления.

Конфигурация сети наложения

Для сети с наложением, в которой не обязательно требуется маршрутизация, вместе с тем требуется возможность сигнализации запросов на соединение. Обычно модель наложения используется в тех случаях, когда строго не предполагается взаимное доверие между провайдером службы оптической сети и пользователем оборудования. Интерфейс O-UNI определяет требования оптического интерфейса для такого взаимодействия.

GMPLS маршрутизирует запросы клиентов внутри оптической сети, обеспечивая службу статически или динамически. Информация о маршрутизации остается в оптической магистрали и не предоставляется подсетям, поскольку в этом нет необходимости. Клиенты, использующие пакеты, используют данную оптическую сеть в качестве IP-каналов типа "точка–точка". Для клиентов TDM оптические маршруты LSP представляют собой маршруты с фиксированной полосой пропускания.

При использовании модели наложения по мере роста мощности сети масштабируемость может стать серьезной проблемой. В связи с недостатком информации о маршрутизации клиенты не могут выбрать наилучший маршрутизатор или наилучший маршрут. Однако в современных сетях эта проблема не столь остра и будет решаться по мере роста оптической сети.

Одноранговая модель

Модель наложения не может обеспечить оптимальные сквозные маршруты. Такова цена, которую приходится платить за административные ограничения. Одноранговая модель учитывает наличие этой проблемы и более подходит в ситуациях, в которых такие административные меры не требуются. В этих случаях рекомендуется использовать отдельную управляющую плоскость для всех устройств (такие как маршрутизаторы и оптические коммутаторы) и не использовать интерфейса UNI, как это подразумевает использование коммутации MPLS.

Полная одноранговая модель

Полная одноранговая модель имеет отдельный комплекс IGP, включая IP-маршрутизаторы и оптические коммутаторы. Возможны две реализации.

- **Реализация в отдельной области.** Общий протокол IGP. При этом используется плоская организация сети с общим протоколом IGP, работающим в IP-сети и в оптических сетях.
- **Использование нескольких областей**. Протокол IGP с использованием обобщенной информации; при этом используется иерархическая маршрутизация внутри IGP с несколькими областями и обобщение информации о доступности и ресурсах.

Модель фильтрованной пары и усовершенствованная модель

Модели фильтрованной пары и усовершенствованная модель не используют совместно информацию о топологии сети. Плоскость оптического управления и управляющие плоскости IP/маршрутизатора разделены и не знают о существовании друг друга. Использование этой модели позволяет протоколу IP/маршрутизатору получать информацию об одноранговых устройствах и ассоциированных оптических конечных точках путем совместного использования или обмена информацией друг с другом.

Интерфейс сети пользователя оптической управляющей плоскости

Интерфейс сети пользователя оптической управляющей плоскости (Optical Control Plane User Network Interface — OCP-UNI) представляет собой набор функций программного обеспечения, основанных на разрабатываемых протоколах стандартов, которые позволяют системам инициировать и закрывать канальные соединения и соединения световых маршрутов в оптических сетях. Эти элементы могут включать в себя ADM, кросс-соединения, оптические коммутаторы, маршрутизаторы и ATM-коммутаторы.

Например, реализация Cisco 15454 OCP-UNI позволяет потребителям расширить инициализацию "от A до Z" за пределы домена отдельной ONS 15454 SDCC-соединенной сети, не требуя использования системы высокоуровневого управления для "связывания" маршрута между подсетями. Эта функция аналогична функции инициализации ONS 15454 от "A до Z", но включает в себя ряд усовершенствований.

Сигнализация через интерфейс UNI используется для вызова служб, которые оптические сети предлагают клиентам. Использование UNI-интерфейса требует:

- определения служб, предлагаемых через интерфейс UNI;
- определения того, как эти службы будут вызываться;
- определения механизма сигнализации для вызова этих служб.

В реализации интерфейса UNI 1.0 эти службы используются для вызова таких функций, как создание соединения, удаление и запрос состояния (статуса). Для предоставления таких служб интерфейс UNI должен иметь возможность выполнить следующие процедуры.

- **Обнаружение соседнего устройства.** Эта процедура позволяет клиенту системы проинформировать элемент системы о его соединениях.
- **Обнаружение службы.** Позволяет сетевым элементам передавать информацию о доступных службах системам клиента. Обнаружение службы использует информацию об обнаружении соседнего устройства для передачи информации от службы системам клиента.
- **Поддержка сигнализации управляющего канала.** Управляющий канал, который соединяет клиента и сеть.
- **Определение адреса.** Эта процедура позволяет клиентам получить точки подсоединения оптической сети, поскольку между этими двумя элементами существует разделение. Этой службой осуществляются регистрация (запрос на связывание адресов клиентского уровня с точкой подсоединения оптической сети) и запрос (получение адреса точки подключения сети для удаленного клиента по его адресу).

Интерфейс OCP-UNI также включает в себя функции, которые автоматизируют работу оптических сетей через различные сетевые элементы, основанные на оборудовании. В числе этих функций находятся автоматическое обнаружение прилегающих сетевых элементов и автоматизированная регистрация адреса с этими автоматически обнаруженными сетевыми элементами или сетями.

Службы запроса клиентских сетей оптической сети, использующей UNI-сигнализацию. Сообщения UNI-сигнализации передаются по управляющим каналам IP внутриполосно (In Band — IB) или внеполосно (Out of Band — OB). Различные протоколы, такие как LDP и RSVP-TE, позволяют осуществлять UNI-сигнализацию, но не являются единственно возможными решениями.

Оптический интерфейс "сеть–сеть" оптической управляющей плоскости

Управляющая плоскость OCP представляет собой набор функций модульного программного обеспечения, который отвечает за функции, связанные с управлением работы сети, такие как маршрутизация, сигнализация, инициализация, а также обнаружение ресурсов и служб. Управляющая плоскость OCP разрабатывается производителями оборудования для автоматизации сквозной инициализации оптической сети. Рассматривается также реализация восстановления полносеточной топологии сети в качестве техники восстановления для плоскости OCP.

В настоящее время в современных оптических сетях используются ручные процессы, которые требуют использования нескольких систем управления для установления нескольких сегментов для сквозной инициализации каналов. Плоскость OCP избегает

этой проблемы за счет того, что позволяет создавать оптические сети новыми способами. Для оптических сетей с OCP большая интеллектуальность сетевых элементов (знание ширины полосы пропускания и поддержка уровня службы) уменьшает капитальные и операционные расходы.

Интерфейс NNI представляет собой интерфейс оптической подсети для сигнализации и маршрутизации в сетевом домене. В настоящее время технология GMPLS, вероятно, эволюционирует как предпочитаемая реализация в O-NNI плоскости OCP. Это не означает что G.ASON не будет частью интерфейса NNI. Фактически G.8080 обеспечивает работу интерфейса NNI и других протоколов сигнализации и маршрутизации оптического интерфейса.

В настоящее время сетевыми элементами интерфейс NNI рассматривается как средство сигнализации и обмена информации о маршрутизации между элементами оптической сети (такими как коммутаторы и маршрутизаторы) для установки запросов по световому маршруту через базовую оптическую сеть.

Интерфейс NNI представляет собой другой возникающий протокол промышленного стандарта. В то время как интерфейс NNI находится в состоянии развития, расширение интерфейса UNI и фирменное расширение будут использоваться продавцами оборудования. Например, стандартная IP-маршрутизация с использованием протокола OSPF может быть использована для поддержки инициализации сети, а сигнализация может быть выполнена с использованием протокола RSVP-TE с оптическими, UNI- и фирменными расширениями.

Обеспечение безопасности и восстановление работы сети в сетях следующего поколения

Обеспечение безопасности и восстановление будут эволюционировать в сторону предоставления не только опций "премиум", "защищенная" для каналов частных линий. APS-кольца SDH/SONET обычно имеют наивысший уровень защищенности и доступны в оптических сетях. Интервал 50 мс для оптических сетей APS рассматривается как наивысшее достижение в мире коммуникаций и как типичное решение для большинства пользователей.

Другие типы восстановления могут и будут эволюционировать для того, чтобы предоставить пользователям защищенное восстановление службы в течение нескольких секунд. Полносеточный принцип или иные принципы работы сети позволяют сохранить или переустановить полосу пропускания сети в соответствии с приоритетом, разнообразием и уровнем задержки. При рассмотрении вопросов использования полосы пропускания обратный маршрут не потребуется выделять или планировать, что позволяет сэкономить средства, оптимизировать работу полосы пропускания, одновременно удовлетворяя нужды пользователей.

Незащищенная служба с использованием ручного восстановления представляет собой другую службу, которая может быть предложена пользователям, которые уже используют схемы защиты на 3-м уровне. Эта служба будет обеспечена, когда будет закончена ее модернизация или выполнено ручное восстановление.

Маршруты защиты могут быть также виртуальными (1:n). Когда создан световой маршрут, вычисленный заранее маршрут защиты вычисляется снова, но не резервируется. Такой метод позволяет постоянно обновлять оптимизацию оптической сети.

Зарезервированная служба использует защитную полосу пропускания и предоставляет службы другим пользователям. Зарезервированная служба не является новой для RBOC и ILEC-сообщества. Если потоки данных требуют защиты, то зарезервированная служба на защищенном маршруте недоступна.

Смешанные службы, такие как IP и TDM, также могут использовать плоскость OCP для конвертирования запросов световых маршрутов через оптические сети. Использование плоскости OCP предполагает возможность конвергирования уровней службы и приложений. При этом может быть гарантирована безопасность и конфиденциальность светового маршрута, что позволяет провайдерам служб и промышленным провайдерам управлять службами внутри их доменов и обеспечить расширение в другие домены.

Провайдерам служб требуются различные решения для того, чтобы предоставить своим пользователям UCP и/или любой другой тип протоколов сигнализации. Как правило, оптические сети представляют собой унаследованные комплексы сетей или комплексы нового поколения. Унаследованные комплексы оптических сетей были созданы для потоков данных с коммутацией каналов. Сети следующего поколения обычно создаются для потоков данных как с коммутацией каналов, так и с коммутацией пакетов. Некоторые другие типы оптических структур используют другую физическую маршрутизацию уровня и коммутацию, но в настоящем пособии они не рассматриваются.

Резюме

Оптические сети предоставляют средства передачи данных (включая аудио и видео) через системы оптической передачи и коммутации. Развитие управления и контроля оптическими сетями в настоящее время происходит с активным участием IETF, OIF и ITU. Оптические сети с сигнализацией и коммутацией обеспечивают коммерчески эффективную работу интегрированных данных и их хранения. Надежные и масштабируемые сети, использующие оптические плоскости управления, предоставляют новые типы SLA-соглашений провайдерам служб и дополнительную полосу пропускания провайдерам предприятий.

Некоторые методы реализации оптических сетей будут использоваться как провайдерами, так и пользователями. Поскольку производители и провайдеры служб и промышленные провайдеры принадлежат к одной и более групп стандартов, реализация намеренно резервируется.

Даже в нынешних оптических сетях пропускная способность оптоволоконного кабеля используется не полностью. В качестве среды передачи сигнала оптоволоконный кабель не имеет конкурентов по ширине полосы пропускания. Оптические сети с использованием сигнализации и управляющее оборудование следующего поколения, а также существующее унаследованное оборудование, позволяют провайдерам служб и промышленным провайдерам и пользователям оценить все преимущества оптических сетей. Очевидно, что не все аспекты работы оптических сетей были обсуждены в настоящей главе. Рекомендуется просмотреть дополнительные справочные материалы и посетить Web-сайты организаций, занимающихся разработкой соответствующих стандартов.

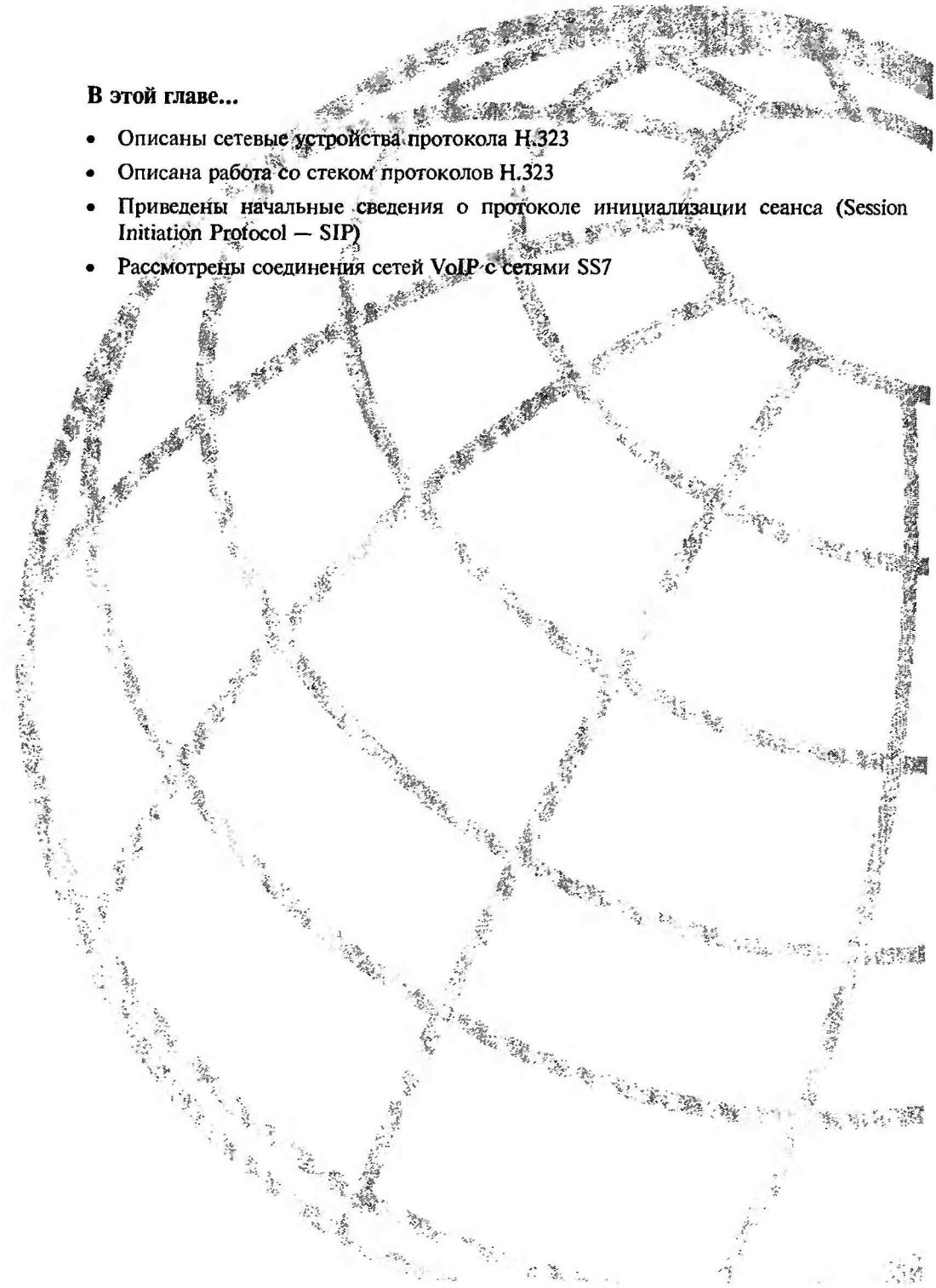
Контрольные вопросы

1. Что представляет собой LSR-интерфейс?
2. Какие три плоскости используются в G.8080 для обеспечения служб сигнализации и установки соединений?
3. В чем состоит цель использования доменов в G.ASON?
4. Какие потоки данных — восходящие или нисходящие — требуют большей ширины полосы пропускания при использовании PON-сетей и почему?
5. Какие два домена используются для администрирования в OTN для модели наложения?
6. Какой тип оптической сети позволяет пользователю непосредственно принимать оптические сигналы независимо от скорости передачи оптической линии и типа фреймов?
7. Что используется в G.ASON в качестве референтной точки между доменами?
8. Какой протокол используется для обеспечения работы канала и обмена информацией с соседним узлом? Почему?

Дополнительные источники

- ITU-T Recommendation G.8080/Y.1304, www.itu.int/rec/Recomendation.asp?type=items&lang=E&parent=T-REC-G.8080-200111-I;
- Draft ietf-ccamp-gmpls-arhitecture-04, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg22930.html
- RFC 2026, www.ietf.org/rfc/rfc2026.txt
- RFC 2748, www.ietf.org/rfc/rfc2748.txt
- RFC 3031, www.ietf.org/rfc/rfc3031.txt
- RFC 3035, www.ietf.org/rfc/rfc3035.txt
- RFC 3036, www.ietf.org/rfc/rfc3036.txt
- UNI 1.0, OIF2001.125, www.oiforum.com/
- NNI 1.0 www.oiforum.com/
- NNI DDRP, OIF2002.023, www.oiforum.com/
- Draft-ietf-mpls-generalized-signaling, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg20113.html
- Draft-ietf-mpls-lsp-hierarchy, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg20272.html
- Draft-ietf-mpls-bundle, www.ietf.org/proceedings/02nov/I-D/draft-ietf-mpls-bundle-04.txt
- Draft-ietf-ccamp-gmpls-sonet-sdh, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg23580.html
- Draft-ietf-ccamp-gmpls-sonet-sdh-extensions, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg18647.html

- Draft-ietf-ccamp-gmpls-routing, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg20086.html
- Draft-ietf-mpls-ldp-state, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg12101.html
- Draft-ietf-mpls-crldp, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg21677.html
- Draft-ietf-mpls-crlsp-modify, www.ietf.org/proceedings/01mar/I-D/mpls-crlsp-modify-03.txt
- Draft-ietf-mpls-generalized-cr-ldp, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg20114.html
- Draft-ietf-mpls-crldp-unnum, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg21677.html
- Draft-ietf-mpls-ldp, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg08973.html
- Draft-ietf-mpls-lmp, www.ietf.org/proceedings/01mar/I-D/mpls-lmp-02.txt
- Draft-nadeau-ccamp-gmpls-tc-mib, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg16480.html
- Draft-nadeau-ccamp-gmpls-label-mib, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg16481.html
- Draft-nadeau-ccamp-gmpls-te-mib, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg16483.html
- Draft-nadeau-ccamp-gmpls-lsr-mib, http://www1.ietf.org/mail-archive/ietf-announce/Current/msg15246.html



В этой главе...

- Описаны сетевые устройства протокола H.323
- Описана работа со стеком протоколов H.323
- Приведены начальные сведения о протоколе инициализации сеанса (Session Initiation Protocol — SIP)
- Рассмотрены соединения сетей VoIP с сетями SS7

Глава 24

Технология передачи голосовых данных по протоколу IP (Voice over IP — VoiceIP)

Даже если читатель является новичком в сетевой индустрии, возможно, что он уже слышал о передаче голосовых данных по протоколу IP (Voice over IP — VoiceIP). Технология VoIP использует передачу голосовых данных по инфрастуктуре IP-сети вместо использования традиционной телефонной сети, базирующейся на мультиплексировании с разделением времени (Time-Division Multiplexing — TDM), также называемой общедоступной коммутируемой телефонной сетью (Public Switched Telephone Network — PSTN). Термин VoIP относится к передаче голосовых данных на сетевом уровне эталонной модели взаимодействия открытых систем (Open Systems Interconnection — OSI), введенной Международной организацией по стандартизации (International Organization for Standardization — ISO).

Технология VoIP в последние годы получает все большее распространение, в частности, благодаря поддержке таких тяжеловесов сетевой индустрии, как корпорация Cisco.

Многие промышленные компании, альтернативные локальные операторы (Competitive Local Exchange Carriers — CLEC) и традиционные локальные операторы (Incumbent Local Exchange Carriers — ILEC) используют VoIP-решения разных уровней. Как и во всей коммерческой сфере, главной движущей силой развития технологии VoIP являются финансовые причины. Реализация VoIP в частных сетях позволяет компаниям экономить средства на выделенных линиях, на управленческих затратах и на требуемом оборудовании.

Например, как показано на рис. 24.1, типичная сеть провайдера службы содержит коммутаторы, межкоммутаторные магистрали (Intermachine Trunks — IMT), представляющие собой высокоскоростные каналы между коммутаторами, оборудование системы сигнализации (Signaling System 7 — SS7), такое как промежуточные точки сигнализации (Signaling Transfer Points — STP). И конечно же, за поддержку работы этой инфраструктуры отвечает специальный персонал. Затраты на все эти составляющие сети весьма велики, особенно для операторов CLEC, у которых просто может сразу не оказаться достаточных средств.

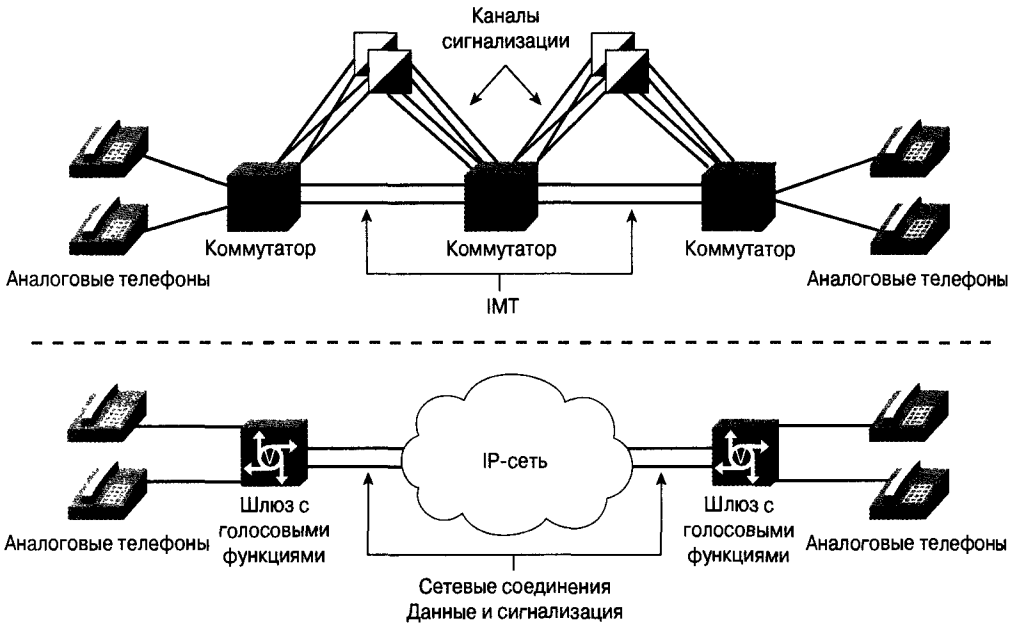


Рис. 24.1. Провайдер службы и базовые инфраструктуры сети VoIP

Внимание!

На рис. 24.1. отображены не все элементы сети, поскольку это потребовало бы слишком много места. Он предназначен лишь для того, чтобы показать базовый способ реализации любой сети.

Оборудование, необходимое для работы технологии VoIP, такое как IP-телефоны, шлюзы с голосовыми функциями и менеджеры вызова, могут быть приобретены и установлены в существующих IP-сетях как небольшая часть сети TDM. Для частных лиц, которым нужна передача голосовых данных или голосовые службы, но которые не имеют достаточных средств, служба VoIP может оказаться приемлемой альтернативной для повышения уровня голосовых служб. Основным мотивом использования VoIP является получаемая при этом экономия на междугородных телефонных службах.

Технология VoIP используется для внутренней передачи голосовых данных как замена местной АТС (Private Branch Exchange — PBX) в офисе и для передачи голосовых данных на большие расстояния (Long-Haul Voice Transport) в сетях предприятий и провайдеров служб. Существует мнение, что VoIP вскоре заменит устаревшие сети TDM, и, возможно, это произойдет. Однако, учитывая большое количество оборудования TDM, уже установленного и работающего по всему миру, более вероятным представляется долгое временное сосуществование VoIP и TDM, а не полная замена TDM.

Другим способом экономии средств является работа с инфраструктурой протокола IP. Это особенно важно для компаний, которые уже имеют реализованную инфраструктуру IP и для которых значительно выгоднее добавить дальние голосовые службы, чем создавать отдельную TDM-сеть для голосовых служб. Целесообразность такого решения определяется текущей нагрузкой потоков данных в сети и необходимостью поддержки голосовых потоков данных. Например, если корпорация имеет офисы в Нью-Йорке и в Нью-Джерси,

то технология VoIP может быть использована для передачи потоков данных между узлами вместо того, чтобы платить за междугородные переговоры за отдельные звонки. Возможность обеспечения такого типа службы также зависит от доступной ширины полосы пропускания и возможности обеспечения соответствующего качества службы (Quality of Service — QoS).

Другим способом уменьшения расходов является не изменение самого оборудования, а изменение характера работы персонала, который обслуживает это оборудование. Хотя персонал обычно состоит из специалистов, которые хорошо знают работу соединений распределенных сетей (Wide-Area Network — WAN), существуют определенные различия между ними и специалистами, которые поддерживают работу маршрутизаторов, поскольку технология VoIP базируется на передаче данных протокола IP. Продолжительность срока переквалификации часто значительно меньше для специалиста, которому требуется только дополнительно изучить технические вопросы, связанные с VoIP, и соответствующие действия по конфигурированию, чем для человека, которому приходится полностью изучить работу сети провайдера и такие технологии, как SS7.

Внимание!

SS7 представляет собой набор протоколов, которые используются провайдерами служб для сигнализации вызовов, поддержки работы канала и учета работы всемирных голосовых служб.

Такого рода совмещение функций наблюдается не во всех корпорациях. Многие компании разделяют функции протокола IP и голосовые службы. В настоящей главе об этом упоминается для того, чтобы показать, что в небольших компаниях могут быть использованы другие способы экономии средств.

Сетевые устройства протокола H.323

Для большинства пользователей аббревиатура VoIP означает почти исключительно использование стека протоколов Международного союза телекоммуникаций (International Telecommunication Union — ITU), называемого H.323, однако такие протоколы, как протокол инициирования сеанса (Session Initiation Protocol — SIP) в сочетании с протоколом описания сеанса (Session Description Protocol — SDP), могут выполнять те же самые функции, которые выполняет управление вызовом протокола VoIP. Протокол SIP обсуждается далее в настоящей главе.

Перед тем как перейти к обсуждению первичных протоколов, которые вместе составляют стек протоколов H.323, важно понять работу устройств сети H.323 и выполняемые ими функции. На рис. 24.2 показаны некоторые типичные устройства H.323 и указано их примерное расположение в сети H.323.

Терминалы H.323

Терминал протокола H.323 идентифицируется спецификацией H.323 как устройство, которое обеспечивает двухстороннее соединение в реальном времени с другим терминалом H.323, шлюзом или многоточечным управляющим блоком (Multipoint Control Unit — MCU). Для терминалов H.323 требуется поддержка передачи голосовых данных, а передача видеоданных и обычных данных не является обязательной.

Терминал H.323 проще описать как устройство, которое непосредственно поддерживает и использует функции протокола H.323 и не требует шлюза для трансляции. Его можно сравнить с терминальным оборудованием 1-го типа (Terminal Equipment Type 1 — TE1) в сети ISDN. Примерами устройств протокола H.323 являются IP-телефоны, маршрутизаторы с голосовыми функциями и серверы доступа с голосовыми функциями. Маршрутизаторы и серверы доступа показаны на рис. 24.2, поскольку они будут обсуждаться в настоящей главе более подробно при рассмотрении вопроса об одноранговых соединениях удаленного доступа.

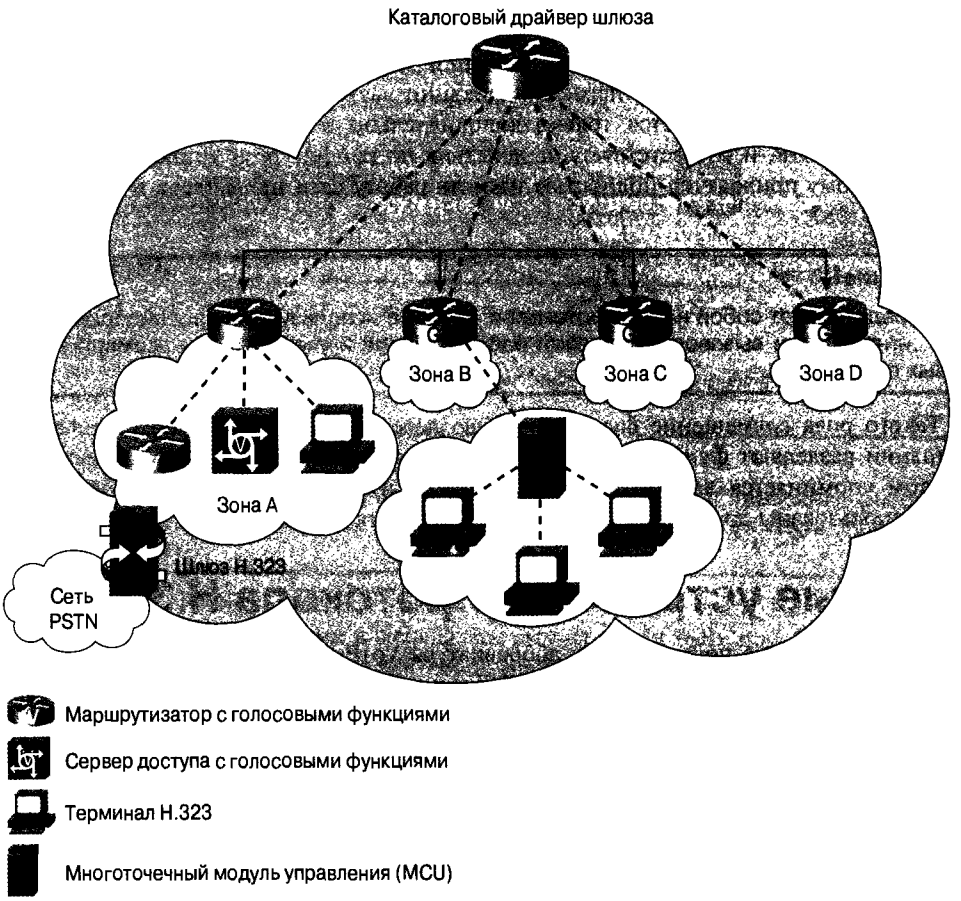


Рис. 24.2 Устройства сети H.323

Драйверы шлюзов протокола H.323

Драйверы шлюзов протокола H.323 представляют собой устройства, которые позволяют расширять сети H.323. При обычном конфигурировании протокола H.323 на маршрутизаторе с голосовыми функциями или на сервере доступа одноранговые соединения удаленного доступа используются для задания пунктов назначения, для номеров или групп номеров, которые должны быть проанализированы и переданы по вышеупомянутым устройствам. Одноранговые соединения удаленного доступа требуются для каждого пункта

иазначения сети H.323, к которому необходимо создать маршрут. В небольших сетях конфигурирование одноранговых соединений удаленного доступа не представляет серьезной проблемы, но при росте сети конфигурирование таких соединений становится серьезной проблемой для администратора. Например, если имеется 45 маршрутизаторов с голосовыми функциями, то необходимо как минимум 1980 одноранговых соединений удаленного доступа для создания полносеточной топологии (44 для каждого устройства), и это не включает в себя дополнительных устройств, которые требуются для маршрутов от нескольких групп к одному и тому же месту назначения.

Для выполнения этой функции вместо конфигурирования столь большого количества одиоранговых соединений удаленного доступа могут быть использованы драйверы шлюзов. Эти устройства отвечают за управление зонами сети H.323. Зоны H.323 представляют собой группы устройств H.323, находяшихся в одном логическом домене управления. Понятие зоны аналогично понятию подсети протокола IP. Зона H.323 может иметь только один драйвер шлюза, однако один драйвер шлюза может выступать в качестве управляющего устройства для нескольких зон. Среди других функций управления, выполняемых драйвером шлюза, следует отметить обеспечение безопасности, управление доступом, управление шириной полосы пропускания, предоставление отчетов о ресурсах системы и о псевдонимах (alias), а также о количестве трансляций или преобразований адресов.

Устройства H.323, такие как маршрутизаторы с голосовыми функциями, добавляются к сети и регистрируются в драйвере шлюза с использованием протокола регистрации, допуска и статуса (Registration, Admission, and Status — RAS) H.225. Действие протокола RAS H.225 обсуждается более подробно в разделе "Протокол H.225 RAS".

Протокол H.225 RAS позволяет устройствам H.323 идентифицироваться в драйвере шлюза, который отвечает за группу телефонных номеров. Драйвер шлюза строит свою таблицу динамически и, при установке вызовов в устройствах H.323, они запрашивают у драйвера шлюза номера устройств получателя вызова H.323. Драйвер шлюза в этом случае либо находит соответствующий номер локально, либо запрашивает соседний драйвер шлюза об устройстве получателя H.323, а затем возвращает эту информацию первоначальному устройству H.323.

Каталоговые драйверы шлюзов протокола H.323

Каталоговые драйверы шлюзов (Directory Gatekeepers — DGK) представляют собой устройства, которые позволяют осуществлять дальнейшее масштабирование структуры сети H.323. Драйверы DGK отвечают за поддержку информации о расположении всех драйверов шлюзов протокола H.323. Для связи между собой драйверам шлюзам требуется знать, где расположены другие драйверы шлюзов. Для одноранговых соединений удаленного доступа H.323 возможна ситуация, когда сеть стала слишком большой и знание расположения всех драйверов шлюзов становится серьезной проблемой для администраторов.

Драйверы DGK конфигурируются со списком других драйверов шлюзов. При поступлении вызова через эти драйверы шлюзов, они в свою очередь запрашивают драйвер DGK относительно расположения удаленного драйвера шлюза, который отвечает за вызов, который не обслуживается в данном локальном домене.

Шлюзы протокола H.323

По самому своему определению, шлюз представляет собой устройство, которое соединяет между собой две сети различного типа. Например, он может осуществлять трансляцию между сетью IP и сетью IPX. В контексте протокола H.323 шлюз представляет собой

устройство, которое соединяет между собой сеть H.323 и сеть, отличную от H.323, например сеть PSTN. В последнее время растущий интерес к VoIP привел к созданию технологий, которые способны соединять сеть провайдера службы SS7 с частными сетями H.323.

Многоточечный управляющий модуль (Multipoint Control Unit — MCU)

Целью использования модуля MCU является обеспечение возможности проведения конференций между тремя и более устройствами H.323. Многоточечные конференции имеют два основных режима работы — централизованный и децентрализованный. В режиме многоточечной централизованной конференции все устройства H.323 осуществляют связь непосредственно с модулем MCU в режиме "точка-точка", а сам модуль MCU управляет конференцией.

В режиме децентрализованной многоточечной конференции каждое устройство H.323 использует многоадресатную рассылку для отправки всей информации другим участникам конференции, не используя при этом модуль MCU. Обычно модули MCU используются только в централизованных многоточечных конференциях, однако они могут быть использованы в гибридных моделях, использующих оба эти метода. Модули MCU могут выступать в качестве моста между централизованными и децентрализованными устройствами, позволяя тем самым осуществлять гибридную конференцию

Стек протоколов H.323

Хотя использование протокола H.323 является наиболее типичным при передаче данных в VoIP, данная спецификация также включает в себя возможность передачи видеоданных и обычных цифровых данных. Первоначальный проект H.323 представлял собой передачу данных различных типов, а не только голосовых данных. В табл. 24.1 описаны некоторые стандарты протоколов, которые включены в стек протоколов H.323, и их назначение.

Таблица 24.1. Спецификации отдельных протоколов стека H.323

Подзаголовок спецификации	Название спецификации	Назначение
Главные системные операции	H.323	Спецификация H.323 описывает общий набор операций, установленный ITU. Она определяет взаимодействие различных протоколов стека H.323. Существует несколько версий этого стандарта. В настоящее время наиболее часто используется версия 4 от 11 ноября 2000 г.
Управление системой	H.225	Протокол H.225 используется для выполнения функций управления вызовом, таких как установка вызова и его прекращение. H.225 основан на спецификации Q.931 для ISDN
Управление системой (продолжение)	H.225 RAS	Сообщения протокола H.225 RAS используются для связи между шлюзами H.323 и драйверами шлюзоа H.323. Эти сообщения описывают возможность масштабирования, уровень безопасности, управление полосой пропускания и учет

Окончание табл. 24.1

Подзаголовок спецификации	Название спецификации	Назначение
	H.245	Протокол H.245 описывает использование управляющего канала для обеспечения надежной внутриполосной трнспортировки при обмене сообщениями. H.245 позволяет инициирующей и терминирующей сторонам достичь соглашения о выполняемых функциях, таких, например, как методы сжатия/декомпрессии (compression/decompression — CODEC)
Видеоспецификации	H.261	Протокол H.261 определяет методы и параметры, используемые для кодирования и декодирования видеосигналов. Они включают в себя скорость передачи, алгоритм кодировки источника, частоту выборок и способ обработки ошибок
	H.263	Протокол H.263 определяет способ сжатия видеопотоков при низких скоростях передачи. Он основан на спецификации H.261
Аудиоспецификации	G.711, G.723.1, G.729	Эти кодеки не охватывают всего набора используемых кодеков, но применяются наиболее часто. Они позволяют осуществлять сжатия различной степени в IP-сетях

Внимание!

Описание видеоспецификаций H.261 и H.263 выходит за рамки настоящей глаавы и поэтому далее не представлено.

Спецификация H.323

Спецификация H.323 описывает работу сети H.323 в целом и взаимодействие друг с другом различных протоколов, объединяемых под названием H.323. Ее важность обусловлена тем, что без нее отдельные протоколы работали бы независимо друг от друга.

Спецификация H.323 также определяет, какие спецификации должны использоваться для передачи видео- и обычных данных, какие параметры являются обязательными, а какие нет.

Вызовы протокола H.323 устанавливаются в разделах, известных как ветви вызова. Ветвь вызова представляет собой логическое соединение между двумя терминалами H.323. Каждая оконечная точка вдоль пути установки вызова имеет две идентифицируемые ветви вызова — входную и выходную. На рис. 24.3 показаны две ветви вызова между двумя шлюзами при вызове.

Основным правилом является наличие двух ветвей вызова для каждой оконечной точки, которая выполняет обработку вызова на его маршруте. Важно помнить, что только оконечные точки, которые обрабатывают сообщения вызова, имеют ветви вызова. Иными словами, маршрутизаторы, которые используются для передачи IP-пакетов между двумя шлюзами, не имеют ветвей вызова. Поэтому вызов, который проходит от одного шлюза H.323 через пять IP-маршрутизаторов к другому шлюзу H.323, имеет четыре ветви вызова.

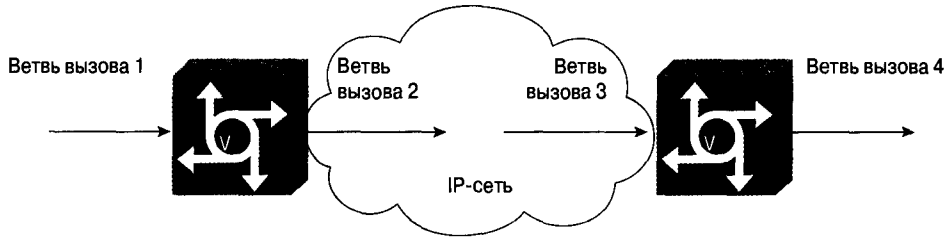


Рис. 24.3. Ветви вызова протокола H.323

Спецификация H.225

Спецификация H.225 представляет собой протокол, отвечающий за установку и прекращение вызова между двумя оконечными точками протокола H.323 (см. рис. 24.4). Спецификация H.225 основана на Q.931. Она работает совместно с протоколами H.245, RTP и RTCP при завершении установки вызова и полностью определяет характер голосового потока. Важно отметить, что канал H.225 открывается до того, как для установки вызова будут использоваться другие каналы и полностью отделен от H.225 RAS и H.245. Канал H.225 использует порт 1720 для первоначальной установки вызова, а после этого он может использовать динамические порты.

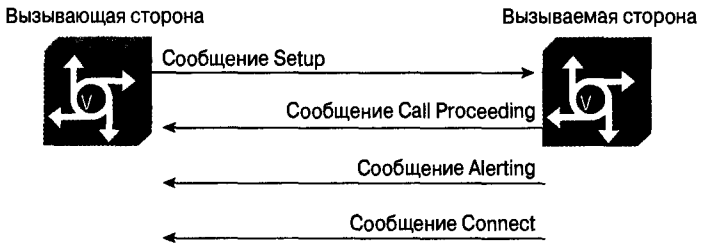


Рис. 24.4. Сообщения об установке вызова протокола H.225

Пустые секции линий на рис. 24.4 используются для обмена возможностями H.245 и для создания потока RTP/RTCP при передаче голосовых данных. Оба этих процесса происходят после обмена первоначальными сообщениями об установке вызова протокола H.225. Вышеупомянутые процессы рассматриваются в разделах "Протокол H.245" и "Протоколы RTP и RTCP".

Как показано на рис. 24.4, протокол H.225 использует несколько типов сообщений для базовых операций установки вызова между оконечными точками H.323:

- установка (setup);
- протекание вызова (call proceeding);
- уведомление (alerting);
- сообщение об установке вызова (connect).

Сообщение Setup

Первым сообщением, которое передается в процессе установки вызова H.225, является сообщение Setup. Это сообщение идет в прямом направлении, т.е проходит от

инициатора вызова (вызывающая сторона) к терминатору вызова (вызываемая сторона). Сообщение Setup содержит информацию, аналогичную той, которая содержится в сообщении Setup спецификации Q.931, однако следует отметить некоторые ключевые моменты.

Некоторые обязательные информационные элементы (Informational Element — IE) спецификации Q.931 требуются также и в сообщении Setup протокола H.225 — дискриминатор протокола, референтная точка (ссылка) вызова, тип сообщения, возможности носителя и элемент IE "пользователь-пользователь". Все остальные элементы IE являются необязательными или запрещенными. В табл. 24.2 описываются некоторые наиболее важные поля в информационном элементе (IE) "пользователь-пользователь".

Таблица 24.2. Некоторые поля элемента IE "пользователь-пользователь" сообщения Setup протокола H.225

Подзаголовок	Описание
ProtocolIdentifier	Задает версию H.225, которая поддерживается данным вызовом
SourceAddress	Список псевдонимов конечной точки, которая является инициатором вызова
SourceInfo	Задает тип конечной точки, инициирующей вызов
DestinationAddress	Адрес пункта назначения для данного запроса на установку вызова
ConfbrenceID	Уникальный идентификатор конференции. Такие идентификаторы присваиваются каждой конференции
ConferenceGoal	Указывает цель конференции: создание, присоединение, приглашение, обмен информацией о возможностях или предоставление дополнительных служб
CryptoTokens	Может быть использован в качестве простого метода аутентификации между шлюзами или между шлюзом и драйвером шлюза. Этот маркер заново вычисляется на каждой аетви вызова при его установке
FastStart	Используется только в тех случаях, когда между конечными точками будет использоваться процедура быстрого соединения
NeededFeatures	Список функций, которые необходимо включить для завершения вызова
DesiredFeatures	Список дополнительных функций, которые могут быть включены в данный вызов. Эти функции не являются обязательными для полной реализации вызова
SupportedFeatures	Список функций, которые поддерживаются инициатором вызова
h245SecurityCapability	список функций, которые могут быть использованы для обеспечения безопасности канала H.245 между двумя конечными точками
CallIdentifier	Уникальный идентификатор вызова, назначаемый инициатором вызова

Внимание!

Поля SourceAddress и DestinationAddress элемента IE, по существу, представляют собой узлы инициатора вызова и пункта назначения. Однако номер адреса источника (номер E.164) также включен в номер элемента IE вызывающей стороны, как в сообщениях Setup Q.931. Кроме того, адрес пункта назначения включен в номер элемента IE вызываемой стороны. DestinationAddress является обязательным полем для устройств H.323, соответствующих версии 2 или более поздних.

Следует отметить, что существует четыре различных версии протокола H.323 и они различаются тем, как обрабатывается связь между протоколами. Большую важность имеет поле FastStart. Как было показано в табл. 24.2, поле FastStart работает в связи с процедурой быстрого соединения, впервые появившейся в версии 2. Процедура быстрого соединения обеспечивает возможность открывать логический канал для обмена информацией о возможностях, тем самым уменьшая количество циклических обменов, требуемых для установки вызова.

В версии 1 для установки вызова требуется в общей сложности 7 или 8 циклических обменов между устройствами H.323. Процедура быстрого соединения версии 2 позволяет сократить количество таких обменов сообщениями до двух. Эта процедура была создана для сокращения времени, требуемого для установки соединения.

Сообщение Call Proceeding

Сообщение Call Proceeding отправляется в обратном направлении, т.е. от вызываемой к вызывающей стороне. Это сообщение указывает, что процесс установки соединения начался. Это может рассматриваться как подтверждение того, что сообщение Setup было получено вызываемой стороной и обрабатывается. Как и в сообщении Setup, несколько полей являются обязательными — дискриминатор протокола, ссылка на вызов, тип сообщения и элемент IE "пользователь-пользователь". Следует обратить внимание на отсутствие поля информации о возможностях носителя. Это поле отсутствует, поскольку вызывающая сторона обычно отвечает на установку возможностей носителя в первоначальном сообщении Setup. В сообщениях Call Proceeding, Alerting и Connect поле возможностей носителя элемента IE является необязательным. В табл. 24.3 описаны некоторые важные поля, которые включены в элемент IE "пользователь-пользователь" сообщения Call Proceeding.

Таблица 24.3. Некоторые поля элемента IE "пользователь-пользователь" сообщения Call Proceeding протокола H.225

Подзаголовок	Описание
ProtocolIdentifier	Указывает используемую версию протокола H.245
DestinationInfo	Позволяет вызываемой стороне указать, используется ли на маршруте вызова шлюз
callIdentifier	Уникальный идентификатор вызова, назначаемый инициатором вызова
h245Address	Указывает конкретный транспортный адрес, на котором вызываемая конечная точка или драйвер шлюза, обрабатывающий вызов, желает установить сигнализацию H.245
h245SecurityMode	Поле h245SecurityMode используется в сообщениях Call Proceeding, Alerting и Setup в том случае, если в первоначальном Setup-запросе для канала H.323 имеется запрос на обеспечение безопасности
fastConnnectRefused	Вызываемая сторона возвращает это поле вызывающей стороне в том случае, если она не поддерживает процедуру быстрого соединения
FeatureSet	Список поддерживаемых функций для данного вызова

Когда сообщение Call Proceeding возвращается вызывающей стороне, некоторые его поля являются ответами на запросы вызывающей стороны в сообщении Setup вызова.

Прежде всего, следует отметить наличие поля callIdentifier. Важность этого поля обусловлена тем, что обеим сторонам требуется возможность проследить, какие сообщения соответствуют идентификатору ID вызова. Когда вызываемая сторона получает сообщение Setup с набором h245SecurityCapability, она отвечает путем установки соответствующего h245SecurityMode в сообщениях Call Proceeding, Alerting и Connect. Следует также отметить поле fastConnnectRefused. Вызываемая сторона использует это поле для того, чтобы уведомить вызывающую сторону о том, что процедура быстрого соединения не поддерживается производителем оборудования или используемой версией.

Поле h245Address используется в сообщениях Call Proceeding и Alerting. В этом поле указывается адрес, который необходим при использовании канала сигнализации H.245. Сообщение Setup может использовать это поле, но только в том случае, если вызывающая сторона поддерживает сигнализацию H.245 перед директивой Connect. Чаще это поле используется в сообщениях Call Proceeding и Alerting, а не в сообщении Setup.

Сообщение Alerting

Сообщение Alerting также посылается в обратном направлении для уведомления вызывающей стороны о том, что соответствующая конечная точка идентифицирована и идет сигнал звонка. Так же, как и в сообщении Call Proceeding, некоторые поля являются обязательными — дискриминатор протокола, ссылка вызова, тип сообщения и элемент IE "пользователь-пользователь". В элементе IE "пользователь-пользователь" имеются поля, которые нужно отметить для сообщения Alerting. В табл. 24.4 описаны некоторые наиболее общие поля, используемые в сообщениях Alerting.

Таблица 24.4. Некоторые поля элемента IE "пользователь-пользователь" сообщения Alerting протокола H.225

protocolIdentifier	Указывает используемую версию протокола H.245
destinationInfo	Позволяет вызываемой стороне указать, используется ли на маршруте вызова шлюз
callIdentifier	Уникальный идентификатор вызова, назначаемый инициатором
h245Address	Указывает конкретный транспортный адрес, на котором вызываемая конечная точка или драйвер шлюза, обрабатывающий вызов, желает установить сигнализацию H.245
h245SecurityMode	Поле h245SecurityMode используется в сообщениях Call Proceeding, Alerting и Setup в том случае, если в первоначальном Setup-запросе для канала H.323 имеется запрос на обеспечение безопасности
alertingAddress	Задает адрес стороны, которая оповещается о данном вызове
screeningIndicator	Определяет, будет ли виден в данном сообщении адрес уведомляемого устройства
Capacity	Список возможностей вызываемой стороны для текущего вызова

Сообщение Alerting имеет несколько знаменательных полей. Поля alertingAddress и screeningIndicator работают совместно в том случае, когда вызываемая сторона должна быть видна (screened) вызывающей стороне. Использование видимости (screening) адресов позволяет установить определенный уровень безопасности в процессе установки вызова.

Полем capacity характеризуется текущая возможность вызова вызываемой стороны. Важность этого очевидна. Если конечная точка вызываемой стороны больше не имеет

ресурсов, то вызов не может быть завершен. Соответствующий отчет о ресурсах и функции управления могут быть выполнены драйвером шлюза. Передача функций отчета о ресурсах и управления драйверу шлюза позволяет последнему принимать более быстрые решения относительно маршрутизации вызова в том случае, когда отсутствуют доступные ресурсы.

Сообщение Connect

Сообщение Connect информирует вызывающую сторону о том, что вызываемая сторона ответила на вызов и может быть создан сквозной голосовой маршрут, после чего можно начать передачу. Сообщение Connect в основном использует те же самые поля, которые используются сообщениями Call Proceeding и Alerting, с добавлением нескольких новых полей. Поле connectedAddress сообщает вызывающей стороне псевдоним (alias) вызываемой стороны. Поле presentationIndicator определяет, будет ли показано вызывающей стороне поле connectedAddress.

Сообщения Release и Release Complete

Именно сообщениями Release (REL) и Release Complete (RLC) определяются наиболее значительные отличия протокола H.225 от спецификации ISDN Q.931; особенно это заметно в том, что конечные точки протокола H.323 не используют сообщения REL:

Полная последовательность disconnect/release/release complete в данном случае не используется, поскольку к сообщению release может быть добавлен единственный информационный элемент "пользователь-пользователь". Поскольку он не применяется в среде пакетных сетей, используется одношаговый метод отправки только сообщения Release Complete.

-ITU H.225 Спецификация 11/2000, стр. 40

На рис. 24.5 показано единичное сообщение RLC, отправляемое вызывающей стороной вызываемой стороне в том случае, когда вызывающая сторона желает прекратить вызов. Конечные точки H.323 используют сообщение RLC только в том случае, когда необходимо прекращение вызова.

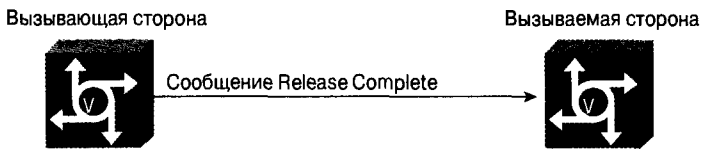


Рис. 24.5. Прекращение соединения H.225 с использованием сообщения RLC

В табл. 24.5 описаны некоторые поля элемента "пользователь-пользователь" сообщения Release Complete.

Таблица 24.5. Поля сообщения Release Complete и коды сообщения Release

Reason	Указывавт причину првкращения вызова
BusyAddress	Псеадоним адреса занятой вызывавмой стороны
Capacity	Описывает возможности отправляющего вызов устройства. В отличие от сообщвния RLC, мощность представляет собой мощность вызова посылающего устройства после того, как текущий вызов был прекращен

Ниже приводятся некоторые наиболее часто используемые коды, описывающие причины прекращения вызова.

- **Nobandwidth.** Отсутствует доступный канал для завершения вызова.
- **Gatekeeperresources.** Отсутствуют доступные ресурсы.
- **UnreachableDestination.** Отсутствует маршрут к пункту назначения. Обычно это означает, что отсутствует IP-маршрут к пункту назначения вследствие либо особенностей маршрутизации, либо из-за отсутствия однорангового соединения.
- **DestinationRejection.** Обычное прекращение вызова.
- **InvalidRevision.** Конечная точка, которая отвергает этот вызов, считается несовместимой.
- **UnreachableGatekeeper.** Драйвер шлюза недоступен, обычно вследствие проблем в сетевой инфраструктуре.
- **GatewayResources.** В коммутирующем оборудовании переполнение, обычно в шлюзе пункта назначения или в конечной точке.
- **BadFormatAddress.** Неверный или нераспознаваемый числовой формат.
- **InConf.** Конечная точка, которая была запрошена в сообщении Setup, уже "находится в конференции". Вызываемая сторона занята.
- **FacilityCallDeflection.** Обычное сообщение о прекращении вызова.
- **SecurityDenied.** Не пройдена проверка безопасности и вызов отвергнут.
- **CalledPartyNotRegistered/callerNotRegistered.** Эти сообщения рассылаются в том случае, когда конечная точка не зарегистрирована в драйвере шлюза и посылается запрос вызова, а также в том случае, когда точка не зарегистрирована в соответствующем драйвере шлюза.
- **NeededFeatureNotSupported.** Одна из необходимых для вызова функций не поддерживается вызываемой стороной.
- **TunneledSignalingRejected.** Туннельная сигнализация H.225 была запрошена вызывающей стороной, но не поддерживается последней.

Туннельная сигнализация H.225 может быть использована для различных приложений. Для сетей H.323, которые подсоединены к провайдеру службы SS7, характерно то, что как только сигнализация вызова SS7 достигает сети H.323, многие функции SS7 теряются. Туннельная сигнализация H.225 может быть использована при туннелировании этих функций через сеть H.323 для предоставления их в распоряжение вызываемой стороны или между вызывающей и вызываемой сторонами.

В процедуре быстрого соединения в туннеле H.225 может быть открыт управляющий канал H.245 для уменьшения количества требуемых циклов обмена сообщениями между конечными точками.

Протокол H.245

Протокол H.245 используется между устройствами сети H.323 для выполнения различных функций, связанных с управлением установкой вызова. При упоминании протокола H.245 обычно возникает ассоциация с его использованием для обмена возможностями. Хотя это и является весьма важным аспектом работы протокола H.245, однако не является его единственной функцией. Другими возможными применения-

ми H.245 являются определение ведомого/ведущего терминала, контроль управляющего канала, определение циклической (круговой задержки), сигнализация поддержки петли и запрос режима.

Обмен возможностями

Обмен возможностями между конечными точками происходит до того, как между ними будет открыт логический управляющий канал H.245. Обмен возможностями определяет возможности, которые каждая конечная точка вызова предпочитает и может обрабатывать. Обмениваемыми возможностями являются списки кодеков и, при необходимости, спецификации видео или обычных данных.

Возможности упорядочиваются по полю capabilityTable, а затем по полю alternativeCapabilitySet. Назначение поля alternativeCapabilitySet состоит в сообщении конечной точке пункта назначения всех доступных операционных возможностей, и в определении той возможности, которая должна быть выбрана. Например, это может быть список всех поддерживаемых аудиокодеков, из которого должен быть выбран только один. В каждый конкретный момент не может поддерживаться более чем один операционный кодек.

После того, как создаются AlternativeCapabilitySet, они группируются в simultaneous CapabilitySet. Эти наборы определяют, какие AlternativeCapabilitySet могут быть использованы совместно. Например, они могут задавать видео- или аудиокодеки, которые могут быть совместно использованы.

Возможности условно подразделяются на возможности передачи, приема и приема-передачи, хотя такая систематизация имеет чисто логический характер.

Определение ведомого/ведущего

Определение ведомого/ведущего, как указывается в спецификации H.323, используется для урегулирования конфликтов между конечными точками протокола H.323. Конечные точки протокола H.323 устанавливают тип терминала, который определяет тип терминала для каждой из них, и генерируют случайное число, которое будет заключено в поле statusDeterminationNumber. Могут быть выбраны четыре типа терминалов, как показано в табл. 24.6.

Таблица 24.6. Типы терминалов, используемые при определении ведомого/ведущего

Таблица значений типов терминалов	Типы терминалов H.323			
Набор функций	**Терминал**	**Шлюз**	**Драйвер шлюза**	**MCU**
Терминал без MC	50	60	-	-
Терминал имеет MC, но без MP	70	80	120	160
Терминал имеет MC и MP обычных данных	-	90	130	170
Терминал имеет MC и MP аудио- и обычных данных	-	100	140	180
Терминал имеет MC и MP аудио-, видео- и обычных данных	-	110	150	190

Данная таблица демонстрирует, какой тип терминала будет иметь более высокий приоритет (станет ведущим). Если в какой-либо позиции таблицы стоит прочерк, то он означает неспособность данного типа терминала использовать приведенный набор функций. Конечная точка с более высоким, согласно таблице, значением типа терминала становится ведущей в соединении. Возможен случай, когда конечная точка является ведущей в одном соединении и ведомой в другом. Если оба типа терминала одинаковы, то ведущей становится конечная точка с более широким набором функций.

В основном определение ведомого/ведущего используется при решении вопроса о предпочтительном порядке отдельных пунктов, таких как аудиокодеки. Например, если ведущий перечисляет в порядке предпочтительности кодеки G.723, а затем G.729, а ведомый предлагает G.729, а затем G.723, то ведомый должен изменить порядок предпочтений своих кодеков, для того чтобы он соответствовал порядку ведущего.

Контроль управляющего канала

После того как происходит обмен возможностями и определяются ведомая и ведущая стороны соединения, протокол H.245 открывает управляющий канал. Этот логический управляющий канал используется для передачи управляющих сообщений и всегда обозначается как логический канал 0. Этот канал остается открытым до прекращения вызова. При необходимости протокол H.245 также отвечает за закрытие управляющего канала.

На рис. 24.6 показаны этапы установки вызова.

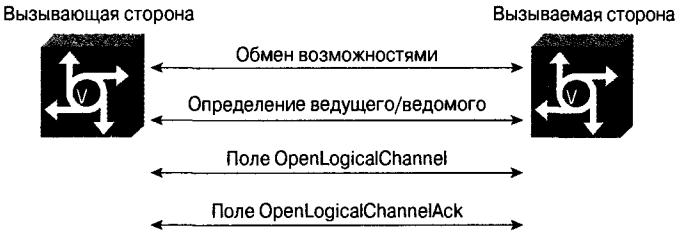


Рис. 24.6. Сообщения об установке вызова протокола H.245

Управляющий канал открывается после использования сообщения OpenLogicalChannel. Поскольку именно в передаче голосовых данных состоит наиболее частое применение протокола H.323, в дальнейшем основное внимание будет уделено этой процедуре для передачи голоса. В тех случаях, когда аудио используется с потоком RTP, параметр MediaControlChannel включается в сообщение OpenLogicalChannel. Прямое сообщение MediaControlChannel включает в себя адрес обратного канала RTCP. Принимающая конечная точка отвечает сообщением OpenLogicalChannelAck, которое содержит MediaTransportChannel и MediaControlChannel. MediaTransportChannel содержит транспортный канал RTP для медиа-канала, а MediaControlChannel содержит транспортный адрес для прямого RTCP-канала.

Определение задержки цикла

Определение задержки цикла в сети H.323 связано с различными функциями. Определяется задержка при обмене сообщениями между конечными точками, а также проверяется, что удаленная конечная точка по-прежнему функционирует и осуществляет связь с сетью H.323. Эта функция может рассматриваться как "прощупывание пульса" для проверки работоспособности сети H.323.

Сигнализация на основе поддержки петли

Метод сигнализации на основе поддержки петли в протоколе H.245 позволяет управляющему каналу создавать петли для тестирования сети. Определены три типа петель.

- **Системные петли**. Относятся ко всем имеющимся логическим каналам.
- **Петли среды**. Тип передающей среды, используемой для вызова.
- **Петли логического канала**. Петля конкретного логического канала.

Внимание!

В протоколе H.323 определено использование только петель среды. Системные петли и петли логического канала запрещены.

Запрос режима

Под запросом режима понимается способность получателя запросить режим, который будет использоваться передатчиками. Для конечных точек доступны два метода — одноадресатная и многоадресатная рассылки. Одноадресатная рассылка используется для терминальных соединений "точка-точка" протокола H.323, а многоадресатная рассылка используется для соединений терминала с модулем MCU при запросах централизованных или децентрализованных конференций.

Протоколы RTP и RTCP

Протокол реального времени (Real-Time Protocol — RTP) отвечает за создание проходов (avenue), по которым будет проходить среда вызова (аудио-, видео- или обычных данных). Протокол RTP определен группой IETF в спецификации RFC 1889. Протокол RTP, наряду с управляющим протоколом RTP (RTP Control Protocol — RTCP) широко используется в сетях H.323 для операций как одноадресатной, так и многоадресатной рассылки.

Потоки данных протокола RTP, проходящие между конечными точками, имеют односторонний характер. Для двусторонней связи необходимы потоки протокола RTP в обоих направлениях, как показано на рис. 24.7.

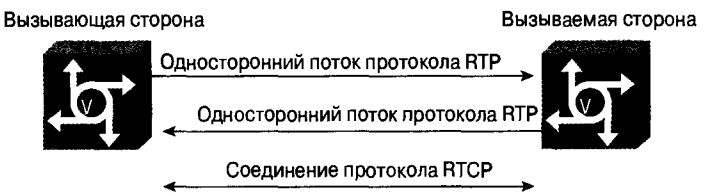


Рис. 24.7. Потоки данных протокола RTP и соединение протокола RTCP

На рис. 24.7 также показано соединение протокола RTCP. Этот протокол используется для информирования конечных точек о качестве распределения данных, которое обеспечивается каналом. Потоки RTP открываются на четных номерах портов UDP, которые находятся в диапазоне неиспользуемых номеров портов. Протокол RTCP использует следующий нечетный больший по номеру UDP-порт в том же самом диапазоне.

Конечные точки, которые участвуют в соединении с использованием протокола RTP, создают RTP-сеанс. Этот RTP-сеанс включает транспортные адреса пункта назначения для каждого участника в одноадресатной конференции или общий транс-

портный адрес пункта назначения в многоадресатных конференциях. Транспортный адрес пункта назначения состоит из сетевого адреса и пары портов для RTP и RTCP. Таким образом, для одноадресатной конференции между конечными точками каждая конечная точка имеет свой собственный сетевой адрес, однако такие точки используют одну и ту же пару портов для протоколов RTP и RTCP.

В протоколе RTP отсутствует механизм обеспечения качества обслуживания QoS. В этом вопросе протокол RTP полагается на другие протоколы, такие как протокол резервирования ресурсов (Resource Reservation Protocol — RSVP).

Протокол H.450

Протокол H.450 представляет собой набор спецификаций, предназначенных для обеспечения служб для конечных пользователей в сети H.323. Эти службы предназначены для того, чтобы имитировать службы, которые предлагаются в сети провайдера SS7 для того, чтобы провайдер протокола H.323 мог конкурировать с существующими службами сети PSTN. В табл. 24.7 описаны спецификации протокола H.450 и их назначение.

Таблица 24.7. Службы протокола H.450, предлагаемые пользователю

Спецификация	Название функции	Описание
H.450.2	Передача вызова	Передает вызов от одной конечной точки к другой
H.450.3	Перенаправление вызова	Перенаправляет вызов от одной конечной точки на другую
H.450.4	Задержка вызова	Вызов задерживается, чтобы ответить позже с этой же конечной точки
H.450.5	Парковка вызова	Переводит вызов в состояние удержания, для того чтобы ответить позже с этой же или с другой конечной точки
H.450.6	Ожидание вызова	Возможность принимать уведомление о входящем звонке после того, как на конечной точке было установлено соединение с другим абонентом
H.450.7	Индикатор ожидания сообщения (Message Waiting Indicator — MWI)	Указывает, что пользователя ожидает сообщение
H.450.8	Идентификация имени (ID вызывающей стороны) (определитель номера)	Идентифицирует пользователя, устанавливающего вызов (идентификация вызывающей стороны)
H.450.9	Завершение вызова	Завершает вызов, который был отвергнут, поскольку конечная точка оказывается занятой после того, как данная конечная точка становится доступной
H.450.10	Предложение вызова	Предлагается принять решение ответить или отвергнуть вызов после того, как был установлен другой вызов
H.450.11	Вмешательство в разговор	Прерывает разговор между сторонами в H.323 для установки нового вызова с какой-либо из них

Аудиокодеки

Аудиокодеки используются для передачи аудиоданных (обычно голосовых) с определенной степенью сжатия и с переменной скоростью. Использование кодеков является очень важным дополнением при передаче данных в сетях VoIP, поскольку оно позволяет более эффективно использовать ресурсы.

Внимание!

Существует несколько интерпретаций аббревиатуры "кодек". Некоторые считают, что она образована от слов "кодер/декодер", другие полагают, что от слов "компрессия/декомпрессия". Хотя, вероятно, и те, и другие по-своему правы, но в контексте протокола H.323 более уместно говорить о "компрессии/декомпрессии".

Кодеки обрабатываются процессорами цифровых сигналов (Digital Signal Processor — DSP) в аппаратном обеспечении H.323. Процессоры DSP представляют собой устройства, которые могут обрабатывать формы цифровых сигналов с очень высокими скоростями.

В традиционных TDM-сетях голосовые вызовы используют отдельные каналы 64 Кб/с, называемые цифровыми сигналами нулевого уровня (Digital Signal Level 0 — DS0). Голосовые вызовы не обязательно используют всю полосу 64 Кб/с, однако поскольку в настоящее время отсутствуют методы перераспределения неиспользуемой полосы, излишняя часть остается неиспользуемой.

Стандартный вызов протокола H.323 также по умолчанию использует эквивалент канала 64 Кб/с. Наиболее часто используются кодеки G.711a или G.711mu. Они определяют использование голосовыми вызовами всех 64 Кб/с в режиме A-law(E1) или mu-law(T1). Поэтому если шлюз поддерживает 254 канала DS0, то одновременно могут обслуживаться максимум 24 голосовых вызова.

Кодеки делятся на две группы — средней сложности и высокой сложности. Эти группы определяются степенью сложности алгоритма, используемого для кодеков. Кодеки высокой сложности требуют большей вычислительной мощности, чем кодеки средней сложности, и, следовательно, позволяют одновременно поддерживать меньшее количество вызовов на устройстве H.323. Кодеки средней сложности позволяют поддерживать по четыре вызова на каждом DSP, в то время как кодеки высокой сложности — только два. В табл. 24.8 приведены кодеки высокой и средней сложности и их индивидуальная степень сжатия.

Таблица 24.8. Группы кодеков и соответствующие битовые скорости

CODEC	Уровень сложности	Скорость передачи в Кб/с	Задержка при обработке, мс
G.711 A-law и mu-law	Средний	64	5
G.726	Средний	32, 24 или 16	1
G.729a	Средний	8	15
G.729ab	Средний	8	15
G.723.1 MP-MLQ	Высокий	6.3	30
G.723.1 ACELP	Высокий	5.3	30
G.723.1 ANNEX A MP-MLQ (VAD)	Высокий	6.3	30

Окончание табл. 24.8

CODEC	Уровень сложности	Скорость передачи в Кб/с	Задержка при обработке, мс
G.723.1 ANNEX A ACELP (VAD)	Высокий	5.3	30
G.728 LD-CELP	Высокий	16	менее 2
G.729	Высокий	8	15
G.729B	Высокий	8	15
G.729 ANNEX B (VAD)	Высокий	8	15

ACELP — Algebraic Code-Excited Prediction
LD-CELP — Low-Delay Code-Excited Linear Prediction
CS-ACELP — Conjugate Structure Algebraic Code Excited Linear Prediction
MP-MLQ — Multipulse Multilevel Quantization

Внимание!

Кодек G.729 (gG.729r8) является стандартным для IOS Cisco.

Следует обратить внимание на аббревиатуру VAD. Она означает, что обнаружение голосовой активности интегрировано в кодек и не может быть удалено.

Обнаружение голосовой активности VAD представляет собой функцию, которая помогает устройствам H.323 функционировать более эффективно. Например, если два пользователя говорят по сети H.323, то имеются промежутки времени, когда ни одна сторона не говорит. Следует помнить о том, что транспортная сеть представляет собой IP-инфраструктуру, поэтому даже молчание передается в виде IP-пакетов, что приводит к напрасным затратам.

Обнаружение молчания VAD смягчает эту проблему обнаружением периодов молчания и прекращением передачи пакетов в такие периоды. В эти периоды молчания слышен "комфортный шум" для того, чтобы не создавалось впечатления, что связь прервана. На рис. 24.8 показано основное различие между устройствами при использовании VAD и при отключении VAD.

Не все кодеки могут взаимодействовать друг с другом. Необходимо обратить особое внимание на то, чтобы на обоих концах соединения были выбраны соответствующие кодеки. Если выбранные кодеки не совместимы, то вызов не состоится. Если тип удаленного кодека неизвестен, то в IOS Cisco могут быть созданы классы, позволяющие конечным точкам обсудить использование кодеков. Конфигурирование классов кодеков описано далее в настоящей главе. Ниже приводятся пары кодеков, которые могут взаимодействовать друг с другом.

- G.729 G.729
- G.729 G.729
- G.729A G.729A
- G.729 ANNEX B G.729A ANNEX B
- G.729 ANNEX B G.729 ANNEX B
- G.729A ANNEX B G.729A ANNEX B
- G.723.1 (5,3 Кб/с) и G.723.1 (5,3 Кб/с)
- G.723.1 (5,3 Кб/с) и G.723.1 (5,3 Кб/с)

- G.723.1 (5,3 Кб/с) и G.723.1 (5,3 Кб/с)
- G.723.1 Annex A (5,3 Кб/с) и G.723.1 Annex A (5,3 Кб/с)
- G.723.1 Annex A (5,3 Кб/с) и G.723.1 Annex A (5,3 Кб/с)
- G.723.1 Annex A (5,3 Кб/с) и G.723.1 Annex A (5,3 Кб/с)

Как и в случае с любой голосовой сетью (IP-сетью или иной), важным является вопрос о задержке. Слишком большая задержка приводит к тому, что качество звука значительно ухудшается, он прерывается и возможным становится даже прекращение соединения. Имеется два основных вида задержки (обычно измеряемых в мкс) — задержка распространения и задержка обработки.

Задержка распространения возникает в процессе передачи данных от одной точки к другой. Это время, необходимое для прохождения информации по сети. Задержка обработки — это время, которое требуется конечным точкам для обработки информации. Например, количество времени, которое требуется для сжатия или декомпрессии вызова в кодеке, является задержкой обработки. В табл. 24.8 перечислены значения задержки сжатия или обработки для каждого кодека.

Протокол H.225 RAS

Драйверы шлюзов и каталоговые драйверы шлюзов представляют собой необязательные компоненты, которые позволяют облегчить масштабирование сети H.323 путем централизации управления конечными точками протокола H.323. Драйверы шлюзов используют набор RAS-сообщений, определенных в спецификации H.225 для связи между собой, также для связи с конечными точками протокола H.323. Ранее в настоящей главе протокол H.225 упоминался как протокол, входящий в стек H.323. В настоящей главе он рассматривается отдельно от протокола H.225 ввиду его применения в сетях H.323. Однако в действительности протокол H.225 RAS не является отдельным протоколом, а является частью спецификации H.225.

Широко используются два основных типа сигнализации драйвера шлюза — направленная сигнализация вызова и маршрутизируемая сигнализация драйвера шлюза (Gatekeeper Routed Signaling — GRS). Направленная сигнализация использует драйвер шлюза в качестве пункта назначения, однако полагается на маршруты шлюзов при установке вызовов между конечными точками. Сигнализация GRS использует драйверы шлюза в качестве конечной точки так же, как и маршрут сигнализации вызова. Проще всего описать разницу между ними тем, что направленная сигнализация отображает только обмен сообщениями RAS между шлюзом и драйвером шлюза (отсутствует установка вызова H.225).

Внимание!

Поскольку драйверы шлюзов Cisco поддерживают только направленную сигнализацию вызова, в дальнейшем этот метод используется для всех обменов сообщениями при вызове.

В табл. 24.9 перечислены типы RAS-сообщений и показано, используются ли они для связи между шлюзом и драйвером шлюза (1), между драйвером шлюза и шлюзом (2) или между драйверами шлюзов (3).

Как видно из таблицы, группы RAS-сообщений имеют однотипную структуру. Первичными используемыми типами являются сообщения Request, Confirm и Reject, за исключением сообщений о сборе информации.

Таблица 24.9. Типы RAS-сообщений и направление сообщений

GRQ	Запрос драйвера шлюза	1
GCF	Подтвврждвние драйвера шлюза	2
GRJ	Отказ драйвера шлюза	2
RRQ	Запрос на регистрацию	1
RCF	Подтвержденив рвгистрации	2
RRJ	Отказ в регистрации	2
URQ	Запрос о прекращении регистрации	1
UCF	Подтверждение прекращения регистрации	2
URJ	Отказ в првкращении регистрации	2
ARQ	Запрос принятия	1
ACF	Подтверждение принятия	2
ARJ	Отказ в принятии	2
LRQ	Запрос на определение расположения	3
LCF	Подтвврждение определения расположения	3
LRJ	Отказ в определении расположения	3
RIP	Запрос обрабатывается	2
DRQ	Запрос на отсоединение	1 или 2
DCF	Подтверждение отсоединения	1 или 2
DRJ	Отказ в отсовдинении	1 или 2
BRQ	Запрос на изменение ширины полосы пропускания	1
BCF	Подтверждение изменения ширины полосы пропускания	2
BRJ	Отказ в изменении ширины полосы пропускания	2
IRQ	Запрос информации	2
IRR	Предостааление информации	1
IACK		2
INACK	Негатианое подтверждение информации	2
RAIc	Индикатор доступности ресурсов	1
RAC	Подтверждение доступности ресурсов	2

Обнаружение драйвера шлюза

Под обнаружением драйвера шлюза понимается процесс, в котором шлюз устанавливает месторасположение драйвера шлюза. Это обнаружение должно быть выполнено до регистрации шлюза на его драйвере. Как правило, это может быть выполнено двумя способами. Шлюз может определить расположение драйвера шлюза с помощью одноадресатного или многоадресатного запроса, как показано на рис 24.9.

- Если посылается одноадресатное сообщение GRQ, то принимающий драйвер шлюза отвечает непосредственно запрашивающему шлюзу сообщением GCF или GRJ.
- Если посылается многоадресатное сообщение, то сообщением GCF шлюзу отвечает только драйвер шлюза, который согласен на обнаружение. Если такой не

определяется, то ответное сообщение не посылается. Если отвечает несколько драйверов шлюзов, то используется только первый полученный ответ.

Регистрация шлюза

Под процессом регистрации шлюза понимается процесс, при котором шлюз H.323 регистрируется на драйвере шлюза и сообщает ему обо всех номерах и адресах, за которые он отвечает. Если шлюз отправил драйверу шлюза сообщение RRQ, то процедура обнаружения считается завершенной. Ответом является сообщение RCF для подтверждения добавления шлюза или сообщение RRJ для отклонения запроса на регистрацию.

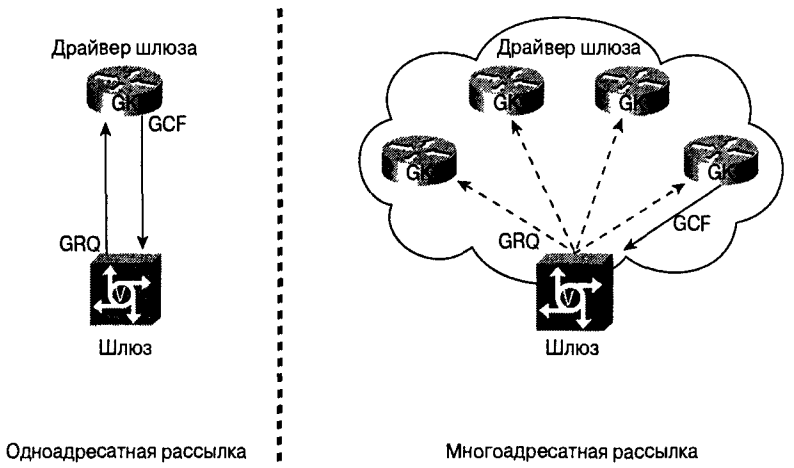


Рис. 24.9. Обнаружение драйвера шлюза с помощью одноадресатной или многоадресатной рассылки

Драйвер шлюза может отклонить запрос на регистрацию по различным причинам, в том числе исходя из соображений безопасности. Кроме того, драйвер шлюза может быть сконфигурирован на принятие или отклонение регистрации на основе номера подсети или IP-адреса запрашивающей стороны.

В версии 2 протокола H.323 процесс регистрации был усовершенствован по сравнению с версией 1, в которой шлюз требовал регистрации каждые 30 сек, что в больших сетях могло приводить к значительному потреблению полосы пропускания. В версии 2 применен новый метод регистрации, получивший название легковесной регистрации. В нем предусмотрено, чтобы шлюз посылал частичную регистрацию после того, как закончена первоначальная регистрация. Следует обратить внимание на то, что при этом в конфигурации шлюза не происходит никаких изменений. В противном случае вновь требуется полная регистрация.

Отмена регистрации шлюза

Если шлюзу требуется отменить регистрацию на драйвере шлюза, то он должен послать драйверу шлюза сообщение URQ. Для того чтобы произошла отмена регистрации, шлюз должен получить ответное сообщение UCF. В случае выхода из строя драйвера шлюза, необходимо принять меры по восстановлению, которые позволят шлюзу зарегистрироваться на другом драйвере шлюза после таймаута или ликвидации сбоя.

Прием вызова

После того как регистрация успешно завершена, шлюз готов к размещению вызовов. Случай, когда вызовы размещаются между несколькими шлюзами, использующими один и тот же драйвер шлюза, называется внутризонным вызовом. На рис. 24.10 показана процедура, используемая для размещения вызовов шлюзами, использующими драйвер шлюза.

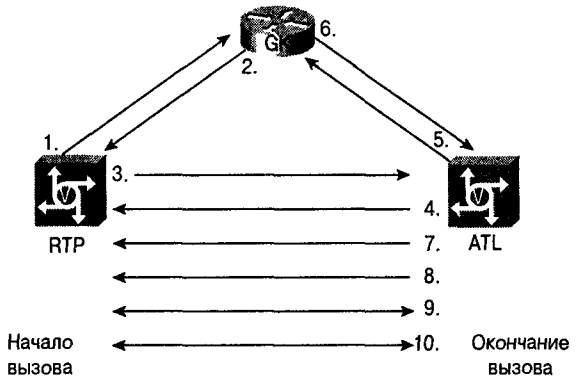


Рис. 24.10. Процедура запроса на прием вызова (ARQ) для внутризонных вызовов

Этап 1. При размещении вызова шлюз посылает локальному драйверу шлюза сообщение ARQ. Сообщение ARQ используется для получения разрешения на установку вызова. Драйвер шлюза может заблокировать вызов и послать сообщение ARJ или разрешить завершение вызова и отправить шлюзу сообщение ACF. В сообщении ARQ содержится запрашиваемый псевдоним (alias) или номер по протоколу H.323.

Внимание!

Обычно драйвер шлюза используется для контроля полосы пропускания. На многих драйверах шлюзов можно ограничить такие параметры, как полоса пропускания шлюза или количество звонков. Например, если шлюзу А разрешено обслуживать одновременно только семь одновременных вызовов, то при получении запроса на восьмой вызов, драйвер шлюза отправляет сообщение ARJ.

Этап 2. В этом случае разрешено продолжение установки вызова. Пи этом драйвер шлюза просматривает запрос на вызов и ищет преобразование номера в IP-адрес, который хранится в его динамической базе данных. Эта база данных строится по мере того, как шлюзы регистрируются в драйвере шлюза и сообщают номера, за которые они отвечают. После того как найден соответствующий IP-адрес, драйвер шлюза отправляет эту информацию, вложенную в сообщение ACF, шлюзу, инициирующему вызов.

Этап 3. Шлюз, инициирующий вызов, принимает сообщение ACF и пытается установить вызов непосредственно с удаленным шлюзом.

Этап 4. При получении запроса на установку вызова терминирующий шлюз отправляет сообщение Call Proceeding инициирующему вызов шлюзу.

Этап 5. Перед отправкой сообщений Alerting и Connect инициирующему шлюзу, терминирующий шлюз должен также сделать запрос драйверу шлюза с помощью сообщения ARQ для получения разрешения ответить на вызов. Ограничения на ширину

полосы пропускания могут применяться как ко входящим, так и к исходящим вызовам, поэтому шлюз должен удостовериться в том, что прием вызова разрешен.

Этап 6. Драйвер шлюза отвечает сообщением ACF, разрешая тем самым терминирующему шлюзу принять вызов.

Этап 7. Терминирующий шлюз посылает сообщение Alerting назад инициирующему шлюзу.

Этап 8. Терминирующий шлюз посылает сообщение Connect назад инициирующему шлюзу.

Этап 9. Происходит обмен сообщениями протокола H.245.

Этап 10. Открываются потоки протокола RTP и управляющий канал протокола RTCP для сквозного голосового маршрута.

Внимание!

Выше приведены все этапы установки вызова. Следует, однако, помнить о том, что при использовании процедуры быстрого соединения последовательности сообщений протоколов H.225 и H.245 объединяются и, соответственно, количество циклов передачи сообщений между конечными точками уменьшается.

Запрос о расположении терминирующей конечной точки

Если вызываемый номер не обслуживается локальным драйвером шлюза, то необходимо, чтобы локальный драйвер шлюза обратился к удаленному драйверу шлюза для поиска терминирующей конечной точки. Поскольку вызов передается другому драйверу шлюза, он называется межзонным вызовом. Сообщение, передаваемое удаленному драйверу шлюза, имеет форму LRQ. Этим сообщением драйвер шлюза как бы спрашивает: "Этот номер у меня отсутствует. Вы не знаете, где он находится?". На рис. 24.11 проиллюстрирован межзонный вызов.

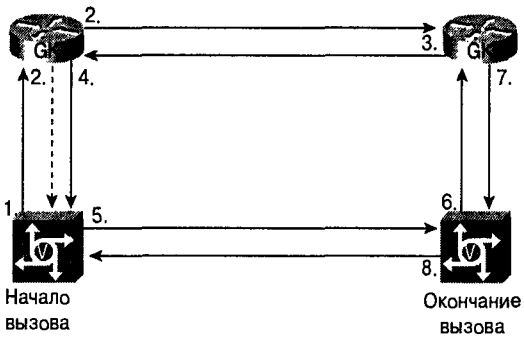


Рис. 24.11. Межзонный вызов с использованием драйверов шлюзов

Этап 1. Инициирующий шлюз посылает своему драйверу шлюза сообщение ARQ.

Этап 2. Драйвер шлюза обнаруживает, что набираемый номер принадлежит удаленному драйверу шлюза, и посылает сообщение LRQ соответствующему драйверу шлюза. Одновременно он посылает RIP-сообщение инициирующему шлюзу для уведомления его о том, что идет процесс обнаружения соответствующей конечной точки.

Этап 3. Терминирующий драйвер шлюза просматривает входное сообщение LRQ и ищет в своей динамической базе данных преобразование вызываемого номера в

IP-адрес. После определения соответствующего IP-адреса шлюза, драйвер шлюза возвращает эту информацию, вложенную в сообщение LCF, инициирующему драйверу шлюза.

Этап 4. Инициирующий драйвер шлюза транслирует сообщение LCF в сообщение ACF и посылает его инициирующему шлюзу.

Этап 5. Инициирующий шлюз принимает сообщение ACF и использует его для установки вызова непосредственно к терминирующему шлюзу.

Этап 6. Терминирующий шлюз принимает сообщение ACF и запрашивает разрешение ответить на вызов, используя свое собственное сообщение ARQ.

Этап 7. Посылая сообщение ACF, терминирующий драйвер шлюза разрешает терминирующему шлюзу ответить на вызов.

Этап 8. Терминирующий шлюз завершает процесс сигнализации при вызове и устанавливает соединение.

Отсоединение (прекращение вызова)

Если сторона, участвующая в разговоре, установленном с помощью драйвера шлюза, желает прекратить вызов, то ей требуется послать драйверу шлюза сообщение DRQ. Драйвер шлюза также может послать сообщение DRQ шлюзу, если он сам желает прекратить вызов. После получения сообщения DRQ от шлюза, драйвер шлюза может ответить сообщением DCF для завершения отсоединения или сообщением DRJ для отказа на запрос шлюза.

Сообщение DRQ также может быть использовано для отправки учетной информации о вызове, который прекращается драйвером шлюза.

Изменение ширины полосы пропускания

Модификация полосы пропускания (Bandwidth Modification, BRQ, BCF, BRJ) позволяет шлюзу обновить или изменить использование полосы пропускания у драйвера шлюза. Если соединение первоначально было установлено через драйвер шлюза, то предполагается, что вызов использует все 64 Кб/с, независимо от используемого кодека. Если полоса пропускания шлюза ограничена, то он может послать драйверу шлюза сообщение BRQ для обновления полосы пропускания после установки соединения, сообщая тем самым: "Использую кодек G.729, поэтому для данного вызова мне требуется не 64 Кб/с, а только 8 Кб/с". Драйвер шлюза отвечает сообщением BCF или сообщением BRJ.

Запрос информации

Драйвер шлюза может запросить у шлюза информацию о вызове или статусе, используя сообщение IRQ. Шлюз отвечает драйверу шлюза сообщением IRR, которое включает в себя соответствующую информацию о статусе. Шлюз может посылать драйверу шлюза сообщения IRR и без запроса, для того чтобы сообщить о своей активности и готовности к установке соединений.

Если заполнено поле needResponse в сообщении IRR, посылаемом драйверу шлюза без запроса, то драйвер шлюза посылает сообщения IACK или INACK в качестве положительного или отрицательного ответа, соответственно.

Доступность ресурсов

Шлюз генерирует сообщения RAI для того, чтобы сообщить драйверу шлюза о своих текущих ресурсах для установки вызовов. Это сообщение может быть использовано для

информационных целей или для того, чтобы сообщить драйверу шлюза о том, что посылающий шлюз не может больше принимать вызовы. Драйвер шлюза отвечает сообщением RAC для подтверждения состояния и прекращения направления вызовов на этот шлюз. Когда состояние переполнения ликвидируется, шлюз отправляет другое сообщение RAI, информируя о том, что он вновь готов принимать запросы на вызовы.

Протокол инициализации сеанса (Session Initiation Protocol — SIP)

Протокол SIP (RFC 2543) является частью стека протоколов управления многосторонним мультимедийным сеансом, разработанного IETF (IETF-Multiparty Multimedia Session Control — IETF-MMSC). Он используется для сквозной сигнализации и управления вызовом в пакетных сетях для обеспечения голосовых, видео и других служб реального времени для двух или более конечных точек. Протокол SIP основан на коде, записанном в формате ASCII, и функционирует на уровне приложения эталонной модели OSI. Приводимые ниже свойства этого протокола считаются его достоинствами по сравнению с протоколом H.323.

- **Простота использования, реализации и поиска ошибок.** Поскольку протокол SIP основан на коде ASCII, его сообщения представляют собой обычный текст. Это простые текстовые сообщения небольшого размера, они записываются в легкодоступной форме, что позволяет быстро находить ошибки.
- **Поддержка уже существующих протоколов.** Протокол SIP представляет собой спецификацию IETF, которая прозрачно работает с уже существующими протоколами, такими как система имен домена (Domain Name System — DNS), протокол описания сеанса (Session Description Protocol — SDP) и протокол реального времени RTP.
- **В этом протоколе предусмотрена интеграция с уже существующими приложениями.** При разработке протокола SIP была заложена возможность совместной работы с различными приложениями данных, таких как чаты и электронная почта.
- **В протоколе SIP предусмотрена высокая мобильность пользователя.** Пользователь имеет возможность использования службы независимо от его положения в SIP-сети.

Сообщения протокола SIP

Сообщения протокола SIP записываются в коде ASCII. В настоящее время при форматировании используется синтаксис протокола HTTP версии 1.1, который является стандартом IETF для кодировки сообщений. При использовании этого формата пользователь обнаруживает, что URL SIP-адресов во многом напоминают адреса в WWW. Причина в том, что таким путем обеспечивается простота декодирования и использования, а также поиск ошибок. Если вместо IP-адреса используется имя узла, то для преобразования имени можно сделать запрос на DNS-сервер.

Сообщения протокола SIP можно разделить на две большие группы — запросы и ответы. Запросы представляют собой сообщения от клиентов UAC серверам UAS. Ответами являются обратные сообщения от серверов UAS к клиентам UAC.

В сетях SIP запросы также называются методами. В RFC 2543 определены следующие шесть основных типов методов.

- **INVITE.** Запрос на установку нового SIP-сеанса. Этот метод установки сеанса используется в SIP-сетях.
- **REGISTER.** Регистрация конечной точки протокола SIP. Метод REGISTER используется при регистрации SIP-терминала на прокси-сервере для идентификации терминала и используемых им номеров.
- **ACK.** Окончательное подтверждение запроса INVITE. До получения сообщения ACK все методы после INVITE считаются промежуточными и рассматриваются как часть процесса установки вызова.
- **OPTIONS.** Запрос о возможностях. Метод OPTIONS используется для запроса сервера или другого агента UA о его возможностях в данном сеансе.
- **CANCEL.** Отменяет запрос на установку сеанса, который еще не был завершен. Это сообщение посылается в тех случаях, когда вызов протокола SIP был установлен, но сеанс был закончен (пользователь отсоединился [повесил трубку]) до получения ответа.
- **BYE.** Запрос на прекращение соединения или на отсоединение. Это сообщение аналогично сообщению Disconnect в сети ISDN.

В примере 24.1 показано применение метода INVITE. В табл. 24.10 описаны первичные заголовки.

Пример 24.1. Вывод для метода INVITE протокола SIP

```
INVITE sip:20290333000l0.15.2.6:5060;user=phone SIP/2/0
Via: SIP/2.0/UDP 10.15.1.6:5000
From: < sip:2019033300010.15.1.6>;tag=1E11E574-8FC
To: <sip: 20290333000l0.15.2.6;user=phone>
Date:Thu, 12 Dec 2002 20:08:06 GMT
Call-Id: D2A1FE73-C3AB11D3-8039C64F-9EF784A8@10.15.1.6
Supported: timer, 100rel
Min-SE: 1800
Cisco-Guid: 3533831795-3282768339-2151073359-2667021480
User-Agent: Cisco-SIPGateway/IOS-12.x
Cseq: 101 INVITE
Max-Forwards: 6
Timestamp: 947189286
Contact: <sip:20190330000@10.15.1.6:5060;user=phone>
Expires: 180
Allow-Events: telephoine-event
Content-Type: application/sdp
Content-Length:233
```

Таблица 24.10. Первичные заголовки SIP-сообщения INVITE

Заголовок	Описание
INVITE sip:2029033300010.15.2.6:5060; user=phone SIP/2/0	Для голосового вызова по адресу 10.15.2.6:5060 используется SIP-метод INVITE. 5060 является общеизвестным портом, а вызывается номер 20290333000. Пользовательским типом является телефон и используется версия SIP 2.0

Окончание табл. 24.10

Заголовок	Описание
Via: SIP/2.0/UDP 10.15.1.6:5000	VIA содержит версию протокола SIP, транспортный протокол и версию инициатора вызова с его общеизвестным портом (5600). Если бы этот сеанс проходил через прокси-серверы, то каждый из них добавлял бы VIA-заголовок со своим собственным адресом
From: < sip:2019033300010.15.1.6>; tag=1E11E574-8FC	Идентифицирует источник вызова. В данном случае URL протокола SIP задается как number@ipaddress, однако имя узла может быть задано в таком же формате, например, johndoe@cisco.com
To: <sip: 2029033300010.15.2.6;user= phone>	Идентифицирует адресата вызова. Также включены URL протокола SIP и тип пользователя-источника
Date:Thu, 12 Dec 2002 20:08:06 GMT	Время и дата метода
Call-Id: D2A1FE73-C3AB11D3-8039C64F-9EF784A8@10.15.1.6	Уникальный идентификатор вызова, используемый для наблюдения за состоянием вызова. Состоит из случайного числа, за которым следует адрес узла в формате @host
Min-SE: 1800	Таймер сеанса
User-Agent: Cisco-SIPGateway/IOS-12.x	Строго идентифицирует тип агента, размещающего вызов. В данном случае это Cisco-шлюз, использующий версию IOS Cisco 12.2.
Cseq: 101 INVITE	Cseq означает "номер командной последовательности". Он содержит тип SIP-метода и числовое значение, используемое для однозначной идентификации этого метода. При каждом новом запросе этот номер увеличивается на единицу
Max-Forwards: 6	Максимальное количество раз отправки этого сообщения по сети
Contact: <sip:2019033000@10.15.1.6: 5060;user=phone>	Место, где терминирующий агент (вызываемая сторона) может найти инициирующего агента (вызывающую сторону)
Expires: 180	Значение таймаута метода
Content-Type: application/sdp	Задает предполагаемое содержание (контент) и тип передаваемой информации (голос, видео и т.д.). Аббревиатура SDP означает "Протокол описания сеанса" (Session Description Protocol). Это поле используется для обсуждения среды (обмен возможностями). Это поле обсуждается в последующем разделе
Content-Length:233	Длина данного сообщения

RFC 2543 также определяет шесть классов сообщений. Каждый класс сообщений относится либо к текущему, либо к законченному действию. Они задают различные типы сообщений о ходе сеанса либо о наличии ошибок. В табл. 24.11 перечислены главные числовые группы сообщений-ответов протокола SIP и описано их использование в сети.

Таблица 24.11. Коды классов ответов SIP

Класс сообщения	Описание
100 PROVISIONAL	Серия 100 в сообщении означает, что запрос находится в процессе обработки, т.е. на него еще не был получен ни положительный, ни отрицательный ответ. Ниже приводятся некоторые типовые сообщения: 100 — попытка вызова; 180 — звонок; 181 — вызов направляется; 182 — вызов установлен в очередь; 183 — сеанс продолжается
200 SUCCESS	Сообщения серии 200 указывеют на успешное завершение конкретного запроса. Фактически в этом классе имеется только одно сообщение 200 OK
300 REDIRECTION	Запрос на SIP-сеанс необходимо отправить по другому адресу
400 CLIENT ERROR	Необходимо устранить ошибку у клиента
500 SERVER ERROR	Необходимо устранить ошибку на сервере
600 GLOBAL FAILURE	Пользователь получил отказ от сети и все остальные попытки также будут отвергнуты

Протокол описания сеанса

Протокол SIP работает совместно с некоторыми другими стандартными протоколами. Среди них наиболее важным, вероятно, является протокол описания сеанса (Session Description Protocol — SDP). Протокол SDP используется для обмена возможностями между оконечными точками. Синтаксис этого протокола находится непосредственно вслед за сообщениями SIP INVITE, 183 Session Progress и ответом 200 OK для INVITE. Роль протокола SDP в сети SIP аналогична роли протокола H.245 в сетях H.323. Протокол SDP позволяет агентам UA обсудить свойства среды, включая такие как аудиокодеки и информацию протокола RTP. В примере 24.2 показан вывод параметров протокола SDP для метода SIP INVITE. В табл. 24.12 подробно обсуждается каждое из этих полей.

Пример 24.2. SDP-параметры SIP-сообщения INVITE

```
v=0
0=CiscoSystemsSIP-GW-UserAgent 762 3453 IN IP4 10.15.1.6
s=SIP Call
c=IN IP4 10.15.1.6
t=0 0
m=audio 16952 RTP/AVP 18 100
a=rtmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtmap:100 X-NSE/8000
a=fmtp:100  192-194
a=ptime:10
```

Таблица 24.12. SDP-параметры SIP-сообщения INVITE

Заголовок	Описание
v=0	Используемая версия протокола SDP
0=CiscoSystemsSIP-GW-UserAgent 762 3453 IN IP4 10.15.1.6	Информация об инициаторе вызова, включая тип агента UA, тип сети и контактное имя
s=SIP Call	Имя сеанса
c=IN IP4 10.15.1.6	Информация о типе среды, как в протоколах IPv4 или IPv6, и адрес соединения. Под адресом соединения понимается адрес отправлющего агента UA
t=0 0	Время начала и остановки
m=audio 16952 RTP/AVP 18 100	Тип среды и транспортный порт, которые будут использоваться для вызова
a=rtmap:18 G729/8000 a=rtmap:100 X-NSE/8000 a=ptime:10	Атрибуты, используемые в поле типа среды. В данном случае одним из таких атрибутов является используемый кодек (G729)

Сетевые устройства протокола SIP

При передаче сообщений между конечными точками протокол SIP использует модель "клиент/сервер". При этом определяются два участника — клиент агента пользователя (User Agent Client — UAC) и сервер агента пользователя (User Agent Server — UAS). UAC представляет собой клиентское устройство, которое инициирует SIP-запрос. UAS представляет собой сервер, который отвечает на SIP-запрос.

Все устройства сети SIP должны быть способны функционировать как в качестве клиента UAC, так и в качестве сервера UAS. Как показано на рис. 24.12, когда Bill посылает запрос Nancy, он является клиентом UAC, а Nancy является сервером. Однако если Nancy посылает запрос Bill, то их роли меняются на противоположные.

Агентами пользователя (User Agent — UA) являются оконечные устройства SIP-сети, такие как SIP-телефоны или шлюзы. В последнее время стали использоваться и другие агенты пользователя UA, такие как клиенты чатов, поддерживающие протокол SIP, или даже мобильные телефоны и персональные цифровые организаторы (Personal Digital Assistant — PDA).

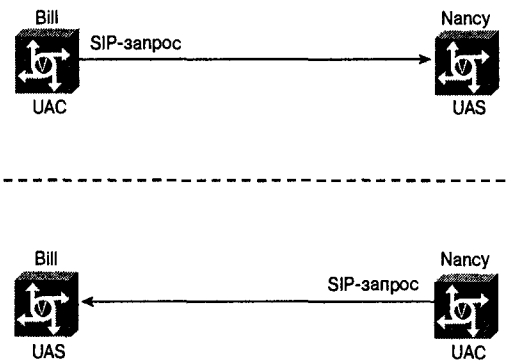


Рис. 24.12. Связь между клиентом UAC и сервером UAS в сети SIP

В спецификации RFC 2543 определены также SIP-серверы. Они обычно выполняют одну из описываемых ниже функций или все одновременно:

- регистрация;
- перенаправленис;
- функции прокси-сервера.

Сеансы протокола SIP могут быть установлены непосредственно между агентами пользователя UA или через посредников, таких как сервер регистрации (registrar server), сервер перенаправления (redirect server) или прокси-сервер (proxy server).

Сервер регистрации протокола SIP управляет регистрацией оконечных точек и связанных с ними номеров в основном так же, как драйверы шлюзов выполняют регистрацию шлюзов H.323. Агенты UA SIP не обязательно должны использовать сервер регистрации, но сервер регистрации делает управление агентами UA более простым. Сервер перенаправления протокола SIP перенаправляет сеансы SIP в другие места. Он применяется для направления вызовов в тех случаях, когда линия занята, не получен ответ, а также для ручного перенаправления на другие номера. Во многом аналогично тому, как сигнализация направленного вызова использует драйверы шлюзов протокола H.323, сервер перенаправления протокола SIP выясняет новый пункт назначения сеанса SIP и сообщает его агенту UA SIP. После этого агент UA SIP отвечает за отправку сообщения INVITE в новый пункт назначения.

Прокси-сервер SIP представляет собой активного посредника между агентами UA. Он получает входные запросы и ответы сеанса, выполняет преобразование имени и/или номера, обеспечивает функционирование служб безопасности и выступает от имени всех подсоединенных агентов UA SIP.

Прокси-сервер SIP может хранить состояния или не хранить их. Сохраняющий состояния прокси-сервер SIP хранит подробную информацию о состоянии транзакций сообщений, а в некоторых случаях также и о состоянии вызова. Не сохраняющий состояний прокси-сервер просто отправляет сообщения после того, как они получены, и не следит за тем, куда отправлены эти сообщения.

Прокси-серверы SIP могут также выполнять *разветвление (forking)* сеанса, при котором запросы сеанса SIP одновременно направляются в несколько пунктов назначения. Прокси-серверу SIP может потребоваться выполнение этой функции для нахождения соответствующего пункта назначения в том случае, когда используется служба "follow me" ("следуй за мной"). Поскольку при разветвлении сообщения посылаются в несколько пунктов назначения, прокси-сервер должен быть способен следить за состоянием каждого из них. После получения ответов от нескольких сторон прокси-сервер должен отфильтровать ненужные ответы и направить выбранный ответ агенту UA, который инициировал данный запрос. На рис. 24.13 показано разветвление вызова и фильтрация ответов.

Внимание!

Хотя определения функций SIP-сервера различаются, как правило, SIP-серверы обладают всеми тремя этими функциями.

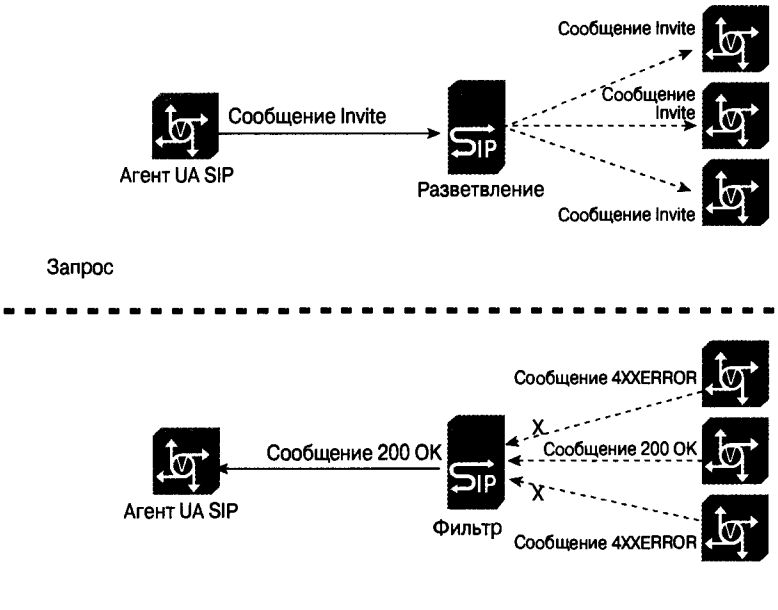


Рис. 24.13. Разветвление сеанса SIP и фильтрация ответов

Обмен сообщениями при установке вызова в протоколе SIP

Первым рассматривается случай, когда обмен сообщениями происходит между двумя агентами UA протокола SIP, показанный в верхней части рис. 24.14.

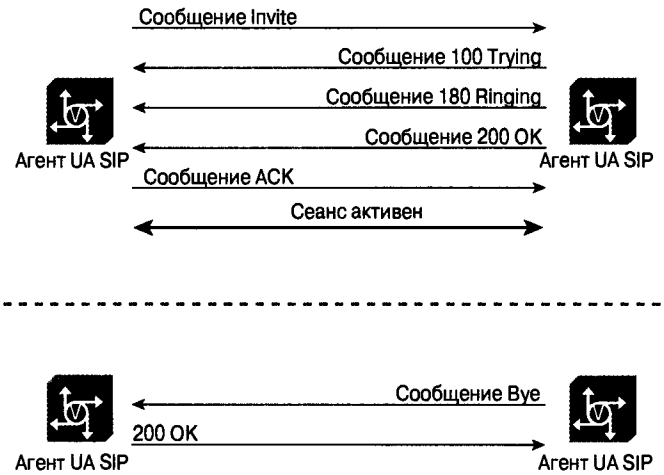


Рис. 24.14. Обмен сообщениями между агентами UA протокола SIP

Ниже описаны пять этапов, которые проиллюстрированы в верхней части рис. 24.14.

- Когда вызывающая сторона инициирует сеанс SIP, она посылает сообщение INVITE, аналогичное запросу, обсуждавшемуся ранее.
- Вызываемая сторона (агент UA SIP) отвечает сообщением 100 Trying для того, чтобы уведомить запрашивающую сторону о том , что сообщение было получено.
- После того как вызывающая сторона находит доступные ресурсы, она посылает сообщение 180 Ringing для извещения об этом вызывающей стороны.
- Отвечая на звонок (снимая трубку) вызываемая сторона посылает сообщение 200 OK вызывающей стороне.
- На это сообщение необходимо ответить сообщением ACK. В этот момент сеанс SIP становится активным.

В нижней части рис. 24.14 показана процедура прекращения вызова или отсоединения. Это несложная процедура, поскольку прекращающая сеанс сторона просто посылает сообщение BYE. На это сообщение другая сторона отвечает сообщением 200 OK.

Во втором случае обмена сообщениями в качестве посредника между двумя агентами UA выступает прокси-сервер SIP (см. рис. 24.15). В простом прокси-режиме единственным отличием является то, что прокси-сервер перехватывает и регистрирует сообщения, которыми обмениваются агенты UA.

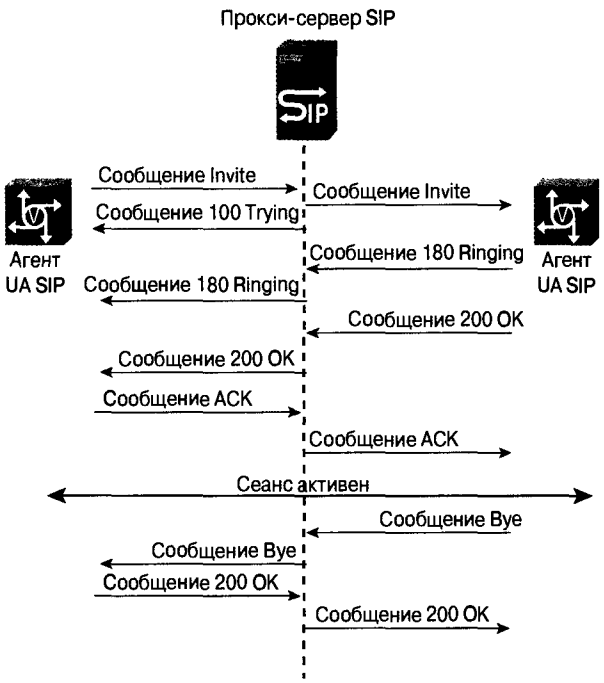


Рис. 24.15. Обмен сообщениями между агентами UA при наличии прокси-сервера

Если прокси-сервер вовлечен в SIP-сеанс, то у него есть возможность включить функцию, называемую *маршрутом записи*. Заголовок маршрута записи позволяет прокси-серверу оставаться на маршруте сигнализации в течение всего времени активности сеанса. Если вызов проходит более чем через один прокси-сервер, то каждый последующий прокси-сервер может быть добавлен к заголовку маршрута записи. В результате этого можно проследить обратный путь к источнику сеанса.

Последним рассматривается случай, когда в обмене сообщениями участвует сервер перенаправления. В этом случае обмен сообщениями имеет несколько иной характер. На рис. 24.16 показан обмен сообщениями между двумя агентами UA с использованием сервера перенаправления.

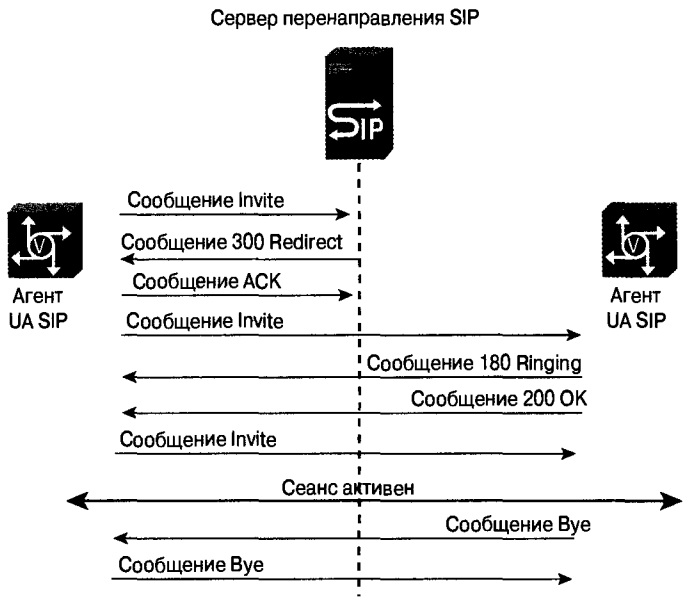


Рис. 24.16. Потоки данных вызова от одного агента UA SIP к другому при использовании сервера перенаправления SIP

Сервер перенаправления используется во многом так же, как и драйвер шлюза с сигнализацией направленного вызова. Сервер перенаправления используется только для того, чтобы идентифицировать расположение терминирующего агента UA. После того как это расположение устанавливается с помощью сообщения серии 300 множественного выбора, инициирующий агент UA отвечает за коммуникацию непосредственно с терминирующим агентом UA. Все остальные типы коммуникаций, включая прекращение сеанса, обрабатываются самими агентами UA.

Соединение сети VoIP с сетью SS7

Технология VoIP применима для многих приложений. Во многих случаях требуется установка соединения с унаследованной сетью провайдера службы, которая не является сетью VoIP. Сеть провайдера службы SS7 является международную сетью, которая достигает даже наиболее удаленных точек планеты. Сеть SS7 покрывает практически все области любой страны.

По всему миру протянуты наземные кабели, длина которых составляет миллионы километров и подсоединение к этой инфраструктуре дает пользователям сетей VoIP большие возможности. Для провайдеров IP-служб использование частной IP-сети может служить способом экономии при передаче данных на большие расстояния. Для Internet-провайдеров потоки данных удаленного доступа могут быть выгружены из сети провайдера до того, как они начнут потреблять ценные ресурсы в течение продолжительного времени. Слияние сетей обычных и голосовых данных дает возможность создавать сложные комбинации различных служб, такие как двухступенчатый удаленный доступ (телефонные карточки), управление пулом ресурсов (Resource Pool Management — RPM) и даже клиентов, основанных на протоколе SIP сообщений.

Хотя технологии H.323 и SIP относятся в настоящее время к популярным методам развития голосовых служб, остается фактом то, что сети провайдеров служб создавались по всему миру в течение нескольких десятилетий. Учитывая это, следует предположить, что, хотя сети H.323 и SIP будут предоставлять все более современные службы конечным пользователям, однако, по всей видимости, в ближайшем будущем они будут лишь дополнять обычную телефонную службу, но не заменят ее полностью.

Резюме

Технология передачи голосовых данных по протоколу IP (Voice over IP — VoIP) стала в последние годы популярной среди предпринимателей, работников сетевых служб предприятий и провайдеров служб с многомиллионными оборотами. Возможность передачи голосовых данных по частным инфраструктурам IP позволяет компаниям экономить на дорогостоящих унаследованных соединениях, основанных на TDM и на поминутной оплате междугородных и международных переговоров. В действительности, эти компании стали своими собственными провайдерами служб передачи голоса на большие расстояния.

В сфере технологии VoIP конкурируют между собой две похожие технологии: H.323 и SIP. Для многих технология VoIP автоматически означает использование стека протоколов H.323. Союз ITU разработал стек протоколов H.323 в качестве стека мультимедийных протоколов для сетей, основанных на передаче пакетов. Технология передачи голосовых данных активно разрабатывалась и внедрялась по всему миру. С каждым днем провайдеры служб вводят все большее количество голосовых портов в свои сети H.323.

Стек протоколов H.323 определяет ряд различных устройств, которые используются для данного стека. Терминалы H.323 представляют собой оконечные устройства, которые непосредственно взаимодействуют с сетью H.323, такие как IP-телефоны или пакеты программного обеспечения с функциями H.323 на персональных компьютерах PC. Драйверы шлюзов H.323 и каталоговые драйверы являются необязательными устройствами, которые позволяют расширять (масштабировать) сети H.323. Драйверы шлюзов ведут учет того, какие шлюзы могут обработать конкретные номера, а каталоговые драйверы следят за тем, где расположены различные драйверы шлюзов (а также какие шлюзы они содержат).

Шлюзы H.323 представляют собой устройства, которые соединяют между собой сети типа H.323 и сети, не принадлежащие к этому типу, такие, например, как шлюзы, соединяющие частную сеть H.323 с TDM-сетью провайдера службы. Модули многоточечного управления представляют собой устройства, управляющие конференциями в сетях H.323. Многие устройства включают в свои коды некоторые функции,

аналогичные функциям модуля MCU и по этой причине использование устройств MCU в конкретной реализации встречается все реже.

Стек протоколов H.323 представляет собой набор протоколов, которые совместно работают для обеспечения надежной установки вызова, его прекращения и для управления вызовом. Спецификация H.323 используется как общее название, под которым понимаются все включенные в нее спецификации. Протокол H.225 используется для установки и прекращения вызова. Он в целом (loosely) основан на спецификации сигнализации Q.931 ISDN и во многом имеет те же самые характеристики.

Протокол H245 используется для обмена информацией о возможностях. Такой обмен включает в себя, например, обмен аудиокодеками (CODEC). Другим преимуществом сети VoIP является ее способность использовать одну и ту же величину полосы пропускания для передачи большего количества вызовов с использованием кодеков. Кодеки сжимают голосовой поток в определенной степени и с определенным качеством. Кодек G.729 может передавать в восемь раз больше вызовов в одном канале DS0, чем канал в сети традиционного провайдера службы. Вместе с протоколом H.245 работают также протоколы RTP и RTCP.

Протокол RTP используется специально для управления голосовыми маршрутами между оконечными точками. Этот протокол обеспечивает службы реального времени, которые требуются для передачи голосовых вызовов по IP-сетям. Протокол RTCP обеспечивает обратную связь (feedback) в потоках данных протокола RTP.

Протокол SIP представляет собой более новую технологию, которая была создана IETF. Она включена в IETF-MMSC. Первоначальной версией протокола SIP была спецификация RFC 2543. Протокол SIP был создан с целью устранить некоторые недостатки, характерные для технологии H.323. Он был разработан как истинно мультимедийный протокол, который работает прозрачно для пользователя с уже отработанными протоколами, такими как DNS и SDP.

Протокол SIP представляет собой основанную на ASCII явную текстовую структуру, которая использует схему кодировки HTTP1.1. Это позволяет легко выполнять декодирование и поиск ошибок в сетях SIP. Сообщения протокола SIP послужили в качестве модели "клиент/сервер" с использованием клиентов UAC и серверов UAS. Каждое устройство в сети SIP должно обладать функциями обоих этих режимов.

Агенты UA протокола SIP представляют собой устройства, которые обычно ассоциируются с устройствами конечного пользователя, такими как SIP-телефоны. Однако они могут включать в себя также SIP-шлюзы. Агенты UA SIP могут устанавливать сеансы непосредственно друг с другом или через прокси-сервер SIP.

Прокси-серверы SIP выполняют три различные функции. Они могут быть использованы в качестве сервера-регистратора (registrar server), прокси-сервера или сервера перенаправления, а также в виде комбинации всех трех. Прокси-серверы SIP обеспечивают централизованное управление агентами UA, определение маршрутов вызова, безопасность, трансляцию номеров и сетевые службы протокола SIP.

В течение уже нескольких лет идет процесс постепенного слияния сетей IP и сетей провайдеров служб. Эта интеграция неизбежна в связи с возрастающим спросом на покрытие и службы и требованиями меньшей стоимости. Решения с использованием сигнализации SS7 соединяют IP-сети следующего поколения с унаследованными сетями провайдеров служб. Хотя службы VoIP получают повсеместное распространение, маловероятно, чтобы они в ближайшее время полностью заместили инфраструктуру провайдеров служб.

Контрольные вопросы

1. Что называется драйвером шлюза в сети H.323?
2. Какова цель использования протокола SDP?
3. В чем состоит главный мотив того, что компании реализуют сети H.323 и/или сети протокола SIP?
4. На каком протоколе основаны сообщения протокола H.225: Q.921, Q.931, Q932 или Q.703?
5. Какое устройство отвечает за обработку голосовых потоков и выполнение сложных алгоритмов CODEC?
6. Какое сообщение должно следовать за сообщением 200 OK?

Дополнительные источники

H.323

- www.cisco.com/pcgi-bin/Support/browse/psp_view.pl?p=Internetworking:H.323&s=Implementation_and_Configuration
- www.cisco.com/en/US/tech//tk652/tk90/technologies_tech_note09186a008010fed1/shtml#intro
- www.cisco.com/en/US/products/sw/iosswrel/ps1833/products_feature_guide_chapter09186a00800ca70f.html#1019911
- www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a0080094ae2.shtml#topic2
- www.cisco.com/en/US/products/hw/routers/ps221/products_configuration_guide_chapter09186a0080089519.html#35804
- www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800a8993.shtml#sourceofdelay

SIP

- www.ietf.org/rfc/rfc2543.txt
- www.cisco.com/en/US/products/sw/voicesw/ps2157/products_administration_guide_chapter09186a0080089519.html#35804

Соединения SS7 для голосовых шлюзов

- www.cisco.com/en/US/tech/tk653/tk653/technologies_white_paper09186a0080113758shtml

Глоссарий

Call leg. Ветвь вызова. Логическое соединение между двумя терминалами H.323. Каждая конечная точка вдоль маршрута установки вызова имеет две ветви вызова — входную и выходную.

CLEC. Competitive Local Exchange Carrier. Альтернативный локальный оператор. Провайдер первичной службы, который конкурирует с уже существующими компаниями RBOC в предоставлении голосовых служб, служб обычных данных и иных служб. Большинство из них было создано после того, как Акт о телекоммуникациях (Telecommunications Act) в 1996 году создал конкуренцию в этой традиционно монопольной сфере.

CODEC. Compression/decompression (coder/decoder). Сжатие/декомпрессия (или кодировщик/декодировщик). Способ сжатия голосовых потоков в разной степени для более эффективного использования полосы пропускания в сети H.323.

Протокол H.225. Спецификация ITU, основанная на спецификации Q.931 сетей ISDN. Обеспечивает обмен сообщениями при установке и прекращении вызова между двумя оконечными точками для протокола H.323. Для полной установки вызова работает с протоколами H.245, RTP и RTCP. Для прекращения вызова используется отдельный RLC.

Протокол H.245. Спецификация ITU, используемая для обмена возможностями между конечными точками в процессе установки вызова в сетях протокола H.323.

Протокол H.323. Стек протоколов, созданный ITU для мультимедийной передачи в сетях, использующих передачу пакетов. Широко используется для передачи данных в технологии VoIP. Спецификация H.323 описывает взаимодействие всех включенных в стек протоколов.

H.323 directory gatekeeper. Каталоговый драйвер шлюза протокола H.323. Позволяет расширять сеть H.323 до более высокого уровня, чем драйвер шлюза. Каталоговый драйвер шлюза ведет учет различных драйверов шлюзов и номеров, которые должны на них направляться.

H.323 gatekeeper. Драйвер шлюза протокола H.323. Устройство, позволяющее расширять сеть протокола H.323 путем поддержки списка шлюзов H.323 и номеров, которые эти шлюзы могут обслуживать.

H.323 gateway. Шлюз протокола H.323. Устройство, соединяющее сеть типа H.323 с сетью иного типа, например с сетью PSTN.

H.323 terminal. Терминал протокола H.323. Устройство, которое взаимодействует с сетью H.323 непосредственно, например, IP-телефон.

ILEC. Incumbent Local Exchange Carrier. Традиционный локальный оператор. Традиционный провайдер телефонной службы в США. Также называется компанией RBOC.

MCU. Multipoint Control Unit. Многоточечный управляющий модуль. Позволяет осуществлять конференции между тремя и более устройствами сети H.323.

OSI model. Open Systems Interconnection model. Эталонная модель взаимодействия открытых систем. ISO создала модель OSI в 1984 году для облегчения взаимодействия различных типов оборудования, разработанных различными производителями, путем создания семиуровневой общей схемы, на которую ориентируются все производители.

RBOC. Regional Bell Operating Company. Региональная операционная компания Bell. Эти региональные телефонные компании были созданы после распада AT&T в конце 1983 года. Примерами компаний RBOC являются Bell South, South West Bell и Bell Atlantic.

RTCP. Real-Time Control Protocol. Протокол управления в реальном времени. Этот протокол предоставляет конечным точкам отчет о качестве распределения данных.

RTP. Real-Time Protocol. Протокол реального времени. Осуществляет в реальном времени передачу голосовых данных в среде протокола IP как для одноадресатных, так и для многоадресатных потоков данных. Потоки данных протокола RTP являются односторонними (однонаправленными), поэтому вызов между двумя конечными точками содержит два потока RTP.

SIP. Session Initiation Protocol. Протокол инициализации сеанса. Один из стеков протоколов IETF-MMSC. Используется для сквозной сигнализации при вызове и для управления в пакетной сети для обеспечения голосовых, видео и других служб реального времени между двумя или более конечными точками.

SIP Method. Метод SIP. Сообщение-запрос протокола SIP.

SS7. Signaling System 7. Система сигнализации 7. Система сигнализации, используемая в международном масштабе для сигнализации при установке и прекрашении вызова, для управления каналом и мощностью службы (в международном масштабе известна как С7).

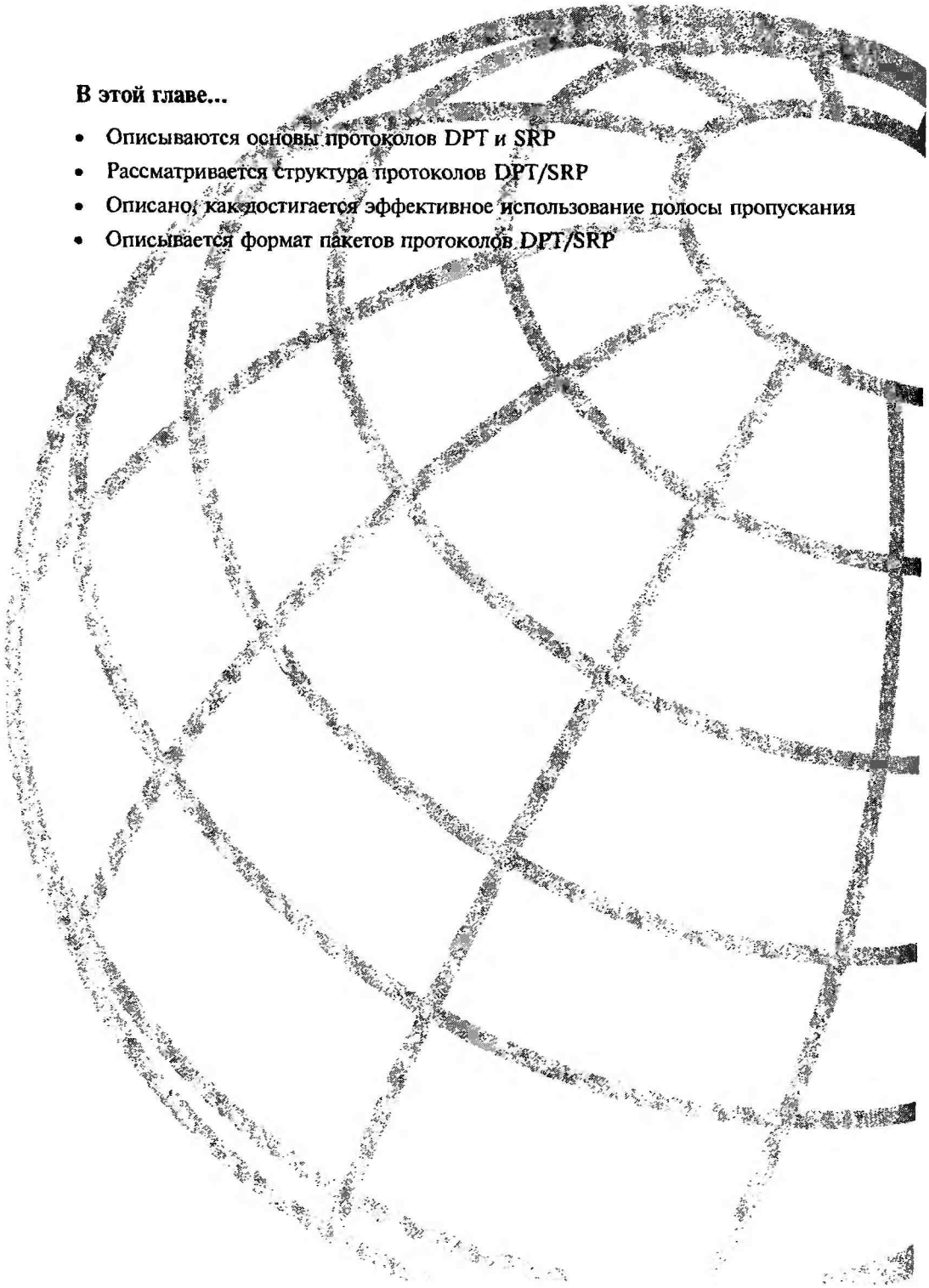
TDM. Time-Division Multiplexing. Мультиплексирование с разделением времени. Процесс деления времени на отдельные порции, называемые таймслотами (timeslot). Каждый таймслот представляет собой некоторый промежуток времени, который предоставляется отдельному каналу для передачи данных по сети. Например, канал T1 имеет 24 таймслота. В процессе передачи сначала передается таймслот №1, затем таймслот №2, №3 и т.д.

UAC. User Agent Client. Клиент агента пользователя. Инициирует запрос в сети SIP.

UAS. User Agent Server. Сервер агента пользователя. Устройство, отвечающее на запросы.

VAD. Voice Activity Detection. Обнаружение голосовой активности. Предусмотрено в сетях H.323 для более эффективного использования сетевых ресурсов. При обычном вызове VoIP данные периодов молчания также передаются по сети. При использовании VAD промежутки молчания обнаруживаются и не передаются.

VOIP. Voice over Internet Protocol. Протокол передачи голоса в сети Internet по протоколу IP. Этот термин используется для описания передачи голосовых данных по инфраструктуре протокола IP. Хотя большинство пользователей ассоциируют VoIP исключительно с использованием стека протоколов H.323, однако при этом могут быть использованы и другие стандарты, такие, например, как SIP.



В этой главе...

- Описываются основы протоколов DPT и SRP
- Рассматривается структура протоколов DPT/SRP
- Описано, как достигается эффективное использование полосы пропускания
- Описывается формат пакетов протоколов DPT/SRP

Глава 25

Протоколы динамической транспортировки пакетов и эффективного использования полосы пропускания

В настоящей главе приводятся начальные сведения о протоколе динамической транспортировки пакетов (Dynamic Packet Transport — DPT) и о протоколе эффективного использования полосы пропускания (Spatial Reuse Protocol — SRP). В ней рассмотрены структура DPT и функции протокола SRP, включая оптимизацию использования полосы пропускания, приоритетность пакетов, алгоритм установления справедливой очередности и анализ топологии. Описаны форматы пакетов управляющей плоскости и плоскости данных. В заключение рассмотрена поддержка протоколом DPT многоадресатной рассылки.

Корпорация Cisco разработала технологию DPT на основе протокола SRP MAC-уровня в целях создания оптимизированной для передачи пакетов кольцевой технологии, эффективно использующей полосу пропускания. Эта технология обеспечивает масштабируемость узлов, поддержку метода "plug-and-play", поддержку приоритетов для потоков данных, справедливое использование полосы пропускания всеми узлами кольца и быстрое восстановление в случае сбоев в кольце.

Протокол SRP рассматривается как часть стандарта IEEE 802.17 "Эластичное пакетное кольцо" (Resilient Packet Ring — RPR). Этот протокол не зависит от среды передачи. Технология DPT реализует протокол SRP по оптоволоконному кабелю в формате фреймов SONET/SDH; вследствие этого протокол DPT может быть прозрачно реализован в сетях SONET/SDH, WDM или по инфраструктуре темного оптоволоконного кабеля. Поддержка как многомодового, так и одномодового оптоволоконного кабеля позволяет реализовать протокол DPT в точке присутствия POP, а также в качестве каналов MAN- и WAN-сетей, обычно со скоростью линии OC-12c/STM-4c (622 Мбит/с) и выше.

Структура протокола DPT

При использовании протокола DPT узлы (также называемые станциями) подсоединяются к двум оптоволоконным кольцам с противоположным направлением движения пакетов. Эти два кольца называются внутренним и внешним. Оба кольца являются частью одной и той же подсети протокола IP. В отличие от других технологий

двойного кольца, таких как FDDI, в данном случае отсутствует холостое кольцо или резервное кольцо и оба кольца передают пакеты одновременно.

На рис. 25.1 показано подсоединение DPT-узлов к этим двум кольцам.

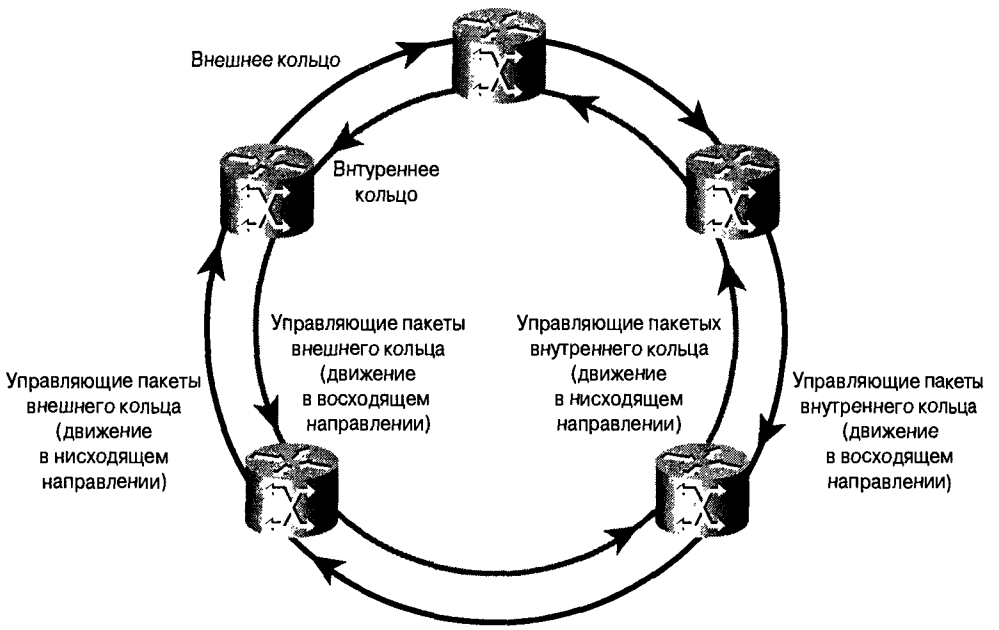


Рис. 25.1 Соединения протокола DPT

Как показано на рис. 25.1, каждый узел посылает пакеты данных в одном направлении (нисходящем) по одному кольцу и управляющие пакеты в противоположном направлении (восходящем) по другому кольцу. Управляющие пакеты обеспечивают выполнение таких функций как анализ реально существующей в данный момент топологии и восстановление при сбоях. Решение о том, в каком направлении посылать пакеты для достижения другого узла, принимается в процессе работы протокола преобразования адресов (Address Resolution Protocol — ARP). ARP-пакет посылается по одному из колец, а получатель отвечает по маршруту с наименьшим количеством переходов, который определяется процессом анализа топологии. Инициатор ARP-сообщения использует то кольцо, по которому был получен ARP-ответ, для отправки будущих пакетов узлу-получателю.

При реализации метода "plug-and-play" к кольцу на любой стадии процесса могут быть добавлены дополнительные узлы; при этом нет необходимости реконфигурировать какой-либо из существующих узлов или изменять систему управления. Пока добавляется новый узел, кольцо сворачивается (wrap) в месте разрыва соединения. Эта функция эластичности кольца обсуждается далее в настоящей главе.

Оптимизация использования полосы пропускания в протоколе SRP

В отличие от других кольцевых технологий, используемых для пересылки пакетов, таких как Token Ring, в протоколе SRP отсутствует маркер, который циркулирует

по кольцу, поэтому несколько станций могут передавать данные по кольцам одновременно. В протоколе SRP используется распаковка пакета у получателя, которая происходит, когда принимающая станция удаляет пакет из кольца. При этом нет необходимости ждать, пока передавшая пакет станция получит прошедший по всему кольцу пакет и удалит его. Вследствие этого достигается более эффективное использование полосы пропускания.

На рис. 25.2 показаны несколько пакетов, одновременно циркулирующих по кольцам.

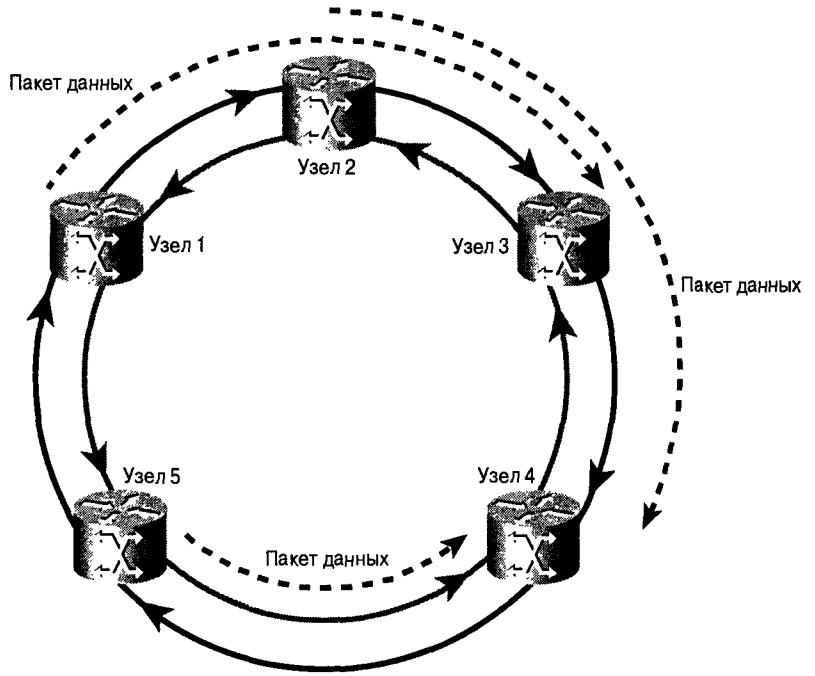


Рис. 25.2 Многократное использование полосы пропускания по протоколу SRP

На рис. 25.2 протокол SRP проиллюстрирован механизм, позволяющий узлу 1 посылать данные узлу 3. В то же самое время узел 2 посылает данные узлу 4, поскольку эти пакеты находятся в различных сегментах внешнего кольца. Тем временем узел 5 также посылает пакет узлу 4 по внутреннему кольцу. При этом каждый узел может полностью использовать всю доступную скорость передачи среды.

Следует отметить, что пакеты многоадресатной рассылки распаковываются в источнике, а не у получателя; это делается для того, чтобы все узлы могли получить пакет многоадресатной рассылки. Если бы пакеты многоадресатной рассылки распаковывались у получателя, то первый же узел с функциями многоадресатной рассылки, получивший пакет, удалил бы его из кольца. Вместо этого каждый узел делает копию пакета многоадресатной рассылки для своего собственного употребления и направляет оригинальный пакет на следующий узел. Когда пакет многоадресатной рассылки прибывает на узел, который его первоначально отправил, этот пакет удаляется из кольца.

Когда узел получает пакет данных, он может выполнить одну из описанных ниже операций.

- **Удалить пакет из кольца**. Пакет прошел по кольцу и был удален отправившим его узлом (например, пакет многоадресатной рассылки, возвратившийся к источнику этого пакета).
- **Получить пакет и удалить его**. Эта операция выполняется в том случае, если адрес пакета соответствует адресу 3-го уровня данного узла.
- **Получить пакет и переслать его далее**. Эта операция выполняется для пакета многоадресатной рассылки, который должен быть передан также и другим адресатам.
- **Переслать пакет по кольцу**. Эта операция выполняется в том случае, когда пакет адресован не этому узлу.
- **Направить пакет на другое кольцо**. Это происходит в том случае, когда в кольце имеется сбой или произошел обрыв соединения по иной причине и происходит сворачивание кольца.
- **Пропустить пакет по кольцу без обработки**. Это происходит в том случае, когда управляющая плоскость узла не функционирует.

Приоритеты пакетов в протоколе SRP

Протокол SRP обеспечивает четыре очереди при передаче — две очереди для потоков данных, исходящих от узла (или передаваемых узлом) и две очереди для транзитных потоков данных кольца через данный узел. Две очереди передачи называются очередями с высоким и низким приоритетами. Аналогичным образом для транзитных потоков данных каждого узла кольца также имеются две очереди — с высоким и с низким приоритетами. Поля IP-очередности при отбрасывании и приоритеты протокола SRP совместно создают восемь уровней приоритетов, которые преобразуются в очередь с высоким приоритетом или в очередь с низким приоритетом. Такое преобразование может выполняться различными способами.

Из этих четырех очередей пакеты передаются в следующем порядке:

1. транзитные пакеты с высоким приоритетом;
2. передаваемые пакеты с высоким приоритетом;
3. передаваемые пакеты с низким приоритетом;
4. транзитные пакеты с низким приоритетом.

Для того чтобы транзитные потоки данных не были отброшены в случае передачи узлом новых данных, используются пороговые значения и механизмы обратной связи. Этот механизм определен в алгоритме установки справедливой очередности протокола SRP.

Алгоритм установки справедливой очередности протокола SRP

Алгоритм установки справедливой очередности протокола SRP (SRP Fairness Algorithm — SRP-fa) используется для того, чтобы ни один узел не монополизировал кольцо, что не позволило бы другим узлам получить доступ к своей части полосы

пропускания. Однако если на данный момент есть свободная полоса пропускания, то узел может всю ее использовать.

Такая гибкость достигается при помощи особого алгоритма, функционирующего на каждом узле. Если на узле возникает переполнение, то он с помощью управляющих пакетов сообщает об этом соседнему устройству в восходящем направлении. Соседний узел восходящего направления использует полученную информацию обратной связи для уменьшения скорости передачи по кольцу.

Этот последний узел может, в свою очередь, обратиться к своему соседнему узлу, лежащему в восходящем направлении. Подробности работы алгоритма достаточно сложны. Более подробное его описание можно найти в источниках, приведенных в разделе "Дополнительные источники" в конце настоящей главы.

Внимание!

Алгоритм SRP-fa функционирует только для потоков данных с низким приоритетом.

Гибкость протокола DPT

Для быстрого восстановления кольца в случае сбоя на узле или обрыва в оптоволоконном кабеле кольца протокола DPT используют интеллектуальную защитную коммутацию (Intelligent Protection Switching — IPS). Коммутация IPS может обнаруживать сбои на 1-м уровне и обеспечивает самовосстановление сети в течение 50 мс, не вызывая реконвергенции на 3-м уровне. Восстановление кольца достигается за счет его сворачивания.

Восстановление кольца может происходить автоматически вследствие отсутствия сигнала или ухудшения его качества, а также выполняться вручную оператором. Если произошел обрыв в обоих кольцах, то узлы на одной стороне оборвавшегося соединения немедленно сворачиваются. Если произошел обрыв только в одном кольце, то узел в нисходящем направлении от обрыва обнаруживает отсутствие сигнала и отправляет узлу в восходящем направлении управляющее сообщение IPS по другому кольцу. После этого узел, лежащий в восходящем направлении также сворачивается. В обоих случаях узлы, обнаружившие сбой, уведомляют об этом другие станции путем отправки управляющих сообщений.

На рис. 25.3 показан случай обрыва двойного оптоволоконного кабеля и узел, в управляющей плоскости 3-го уровня которого произошел сбой и DPT-интерфейс которого функционирует в сквозном режиме.

При нормальной работе и отсутствии сбоев, пакеты данных от узла 1, направленные узлу 4, отправляются по внутреннему кольцу через узел 5. В случае, когда происходит обрыв оптоволоконного кабеля и кольцо сворачивается, узел 1 отправляет пакеты данных узлу 4 по тому же самому внутреннему кольцу, как и раньше, поскольку процесс анализа топологии еще не информирован о наличии более короткого маршрута. После этого узел 5 перенаправляет этот пакет назад во внешнее кольцо, где каждый узел передает этот пакет через транзитный буфер, пока он не достигнет узла 4. Следует отметить, что узел 4 не получает и не распаковывает пакет непосредственно из внешнего кольца. Вместо этого он вновь перенаправляет пакет во внутреннее кольцо, по которому он будет перемещаться до тех пор, пока он не будет обработан обычным образом.

В заголовке каждого SRP-пакета поле идентификатора кольца указывает, был ли пакет изначально отправлен по внутреннему или по внешнему кольцу. В ситуации

сворачивания промежуточные узлы замечают, что идентификатор ID кольца относится к другому кольцу и не пытаются его обработать, а лишь пересылают дальше. Любой узел, включая предполагаемого получателя, начинает обрабатывать пакет только тогда, когда он возвращается в первоначальное кольцо.

В какой-то момент процесс анализа топологии определяет новый порядок колец, и потоки данных от узла 1 направляются непосредственно через внешнее кольцо к узлу 4, а не следуют по неоптимальному свернутому маршруту через узел 5.

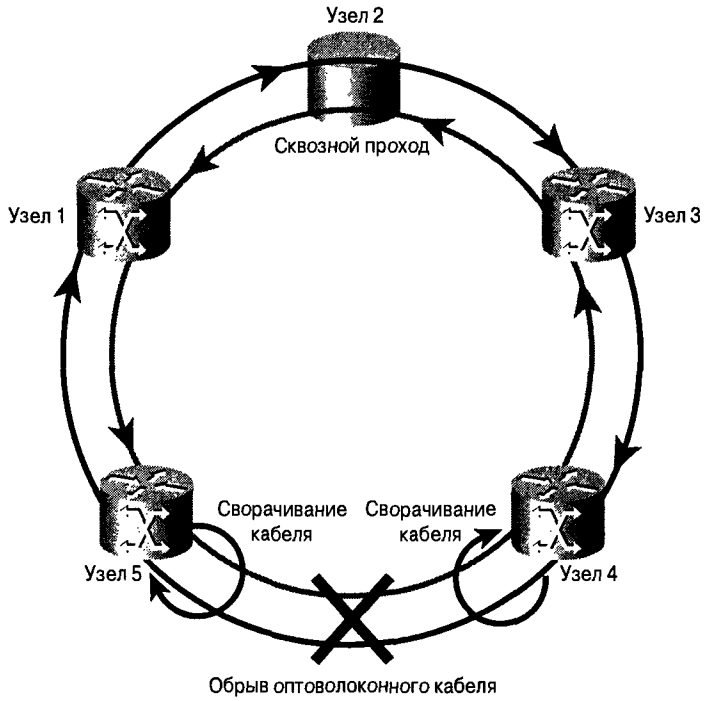


Рис. 25.3 Гибкость протокола DPT

На рис. 25.3 также показано, что узел 2 потерял программный контроль над своей управляющей плоскостью вследствие сбоя или вмешательства оператора. Поскольку интерфейс DPT по-прежнему действует, он функционирует в сквозном режиме, просто повторяя все пакеты, которые он получает и направляя их в кольцо, минимизируя таким образом нарушение работы сети и сохраняя полосу пропускания, поскольку оба кольца по-прежнему функционируют. Если на узле 2 произошел сбой питания, то узлы 1 и 3 рассматривают это как двойной обрыв кабеля и выполняют сворачивание для восстановления работоспособности кольца.

После устранения неисправности кольцо автоматически разворачивается.

Анализ топологии

Каждый узел кольца периодически посылает во внешнее кольцо пакеты анализа топологии. Он также добавляет свой MAC-адрес и указывает был ли его интерфейс свернут. Пакет анализа топологии в конечном итоге возвращается к узлу-источнику.

Когда два последовательных пакета анализа топологии отправлены и получены с одной и той же информацией о кольце, узел строит топологическую карту кольца. Эта карта используется для ответа на ARP-запросы по кратчайшему маршруту к MAC-источнику. Если оба маршрута оказываются равными по длине, то для выбора кольца выполняется хэширование.

Форматы пакетов протоколов DPT/SRP

Существует два формата пакетов — для управляющих пакетов и для пакетов данных. Максимальный блок передачи (Maximum Transfer Unit — MTU) протокола SRP имеет размер 9216 байтов, а минимальный 55 байтов. Стандартным размером блока Cisco в настоящее время является значение 4470 байтов. Оба типа пакетов имеют одинаковый общий заголовок.

Общий формат заголовка протокола SRP версии 2

Все SRP-пакеты имеют общий 16-битовый формат заголовка, показанный на рис. 25.4.

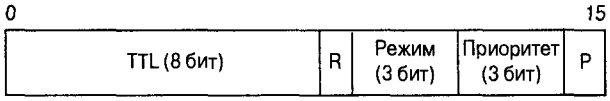


Рис. 25.4. Общий формат заголовка протокола SRP версии 2

Этот заголовок имеет следующие поля:

- **Время существования пакета (Time to live — TTL).** 8 битов. Значение этого поля уменьшается на единицу каждый раз, когда пакет проходит через какой-либо узел. Для предотвращения бесконечного движения пакета по сети при достижении полем TTL нулевого значения пакет удаляется из кольца. Для обработки ситуаций сворачивания значение TTL должно быть вдвое больше числа узлов в кольце. Поэтому максимальное количество узлов в кольце равно 256/2=128.
- **Идентификатор кольца (ring identifier — R).** 1 бит. Указывает с какого кольца был отправлен пакет — с внутреннего или с внешнего. Значению 0 соответствует внешнее кольцо, а значению 1 — внутреннее кольцо.
- **Режим (Mode).** 3 бита. Указывает тип пакета — управляющий пакет или пакет данных. Возможные значения приведены в табл. 25.1.
- **Приоритет (Priority, Pri).** 3 бита. Значение приоритета пакета в диапазоне от 0 до 7, которое заимствуется из поля очередности при отбрасывании протокола IP. Протокол SRP имеет только два уровня приоритетов, в которые преобразуются восемь уровней очередности, используемых протоколом IP.
- **Четность (Parity).** 1 бит. Значение четности, вычисляемое на основе общего заголовка протокола SRP.

Таблица 25.1. Значения режимов

Значение	Описание
000	Зарезервировано
001	Зарезервироаано
010	Зарезервировано
011	Ячейка данных ATM
100	Управляющее сообщение (передается узлу)
101	Управляющее сообщение (помещается в локальный буфер узла)
110	Используемый пакет
111	Пакет данных

Пакет данных протокола SRP

На рис. 25.5 показан формат пакета данных протокола SRP. Следует обратить внимание на то, что поле Mode (режим) в заголовке равно 0 x 7 (соответствует бинарному значению 111), указывая на то, что пакет является пакетом данных.

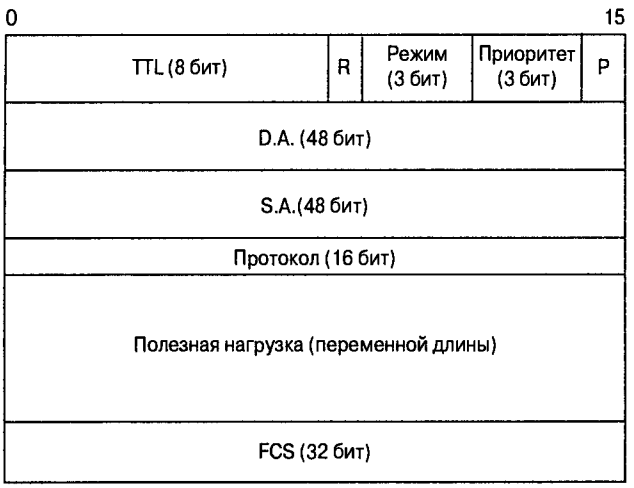


Рис. 25.5. Формат пакета данных протокола SRP версии 2

Данный формат, по сравнению с общим заголовком SRP-пакета, содержит приведенные ниже дополнительные поля:

- **MAC-адрес пункта назначения (Destination MAC-address — DA).** 48 битов. Глобально уникальный MAC-адрес, устанавливаемый IEEE.
- **MAC-адрес источника (Source MAC-address — SA).** 48 битов. Глобально уникальный MAC-адрес, устанавливаемый IEEE.
- **Тип протокола. (Protocol type).** 16 битов. Следует обратить внимание на то, что значение этого поля не может быть равно 0 x 2007, поскольку это значение используется для управляющих пакетов. Возможные значения приведены в табл. 25.2.

- **Полезная нагрузка (payload).** Это поле имеет переменную длину и содержит передаваемые полезные данные.
- **Контрольная сумма фрейма (Frame Check Sum — FCS).** 32 бита. 32-битовая контрольная сумма CRC.

Таблица 25.2. Типы протоколов

Значение	Описание
0x2007	Управление SRP (обсуждается в последующем рвзделе)
0x0800	Протокол IP V4
0x0806	Протокол ARP

Управляющий пакет протокола SRP

На рис. 25.6 показан формат управляющего пакета протокола SRP. Следует отметить, что в общем заголовке полю TTL обычно задается значение, равное единице, поскольку управляющее сообщение в любом случае будет обработано следующим узлом. Поле приоритета должно быть установлено равным 7 для того, чтобы управляющие пакеты всегда имели в кольце максимальный приоритет.

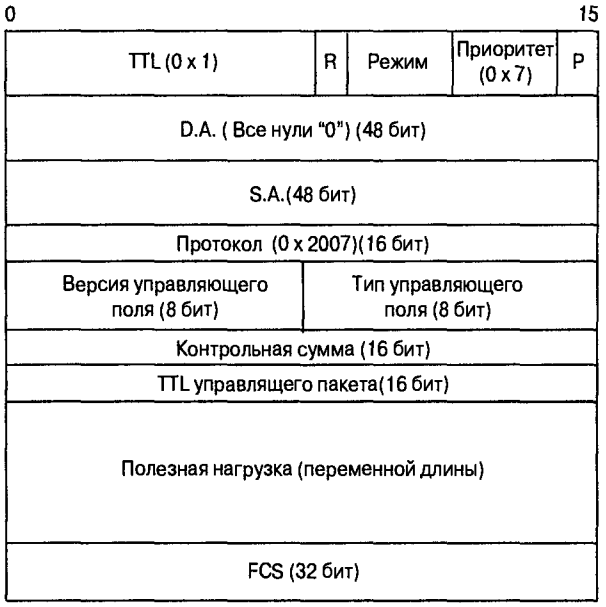


Рис. 25.6. Управляющий пакет протокола SRP версии 2

Данный формат, по сравнению с общим заголовком SRP-пакета содержит приведенные ниже дополнительные поля.

- **MAC-адрес пункта назначения (Destination MAC-address — DA).** 48 битов. Глобально уникальный MAC-адрес, устанавливаемый IEEE.

- **MAC-адрес источника (Source MAC-address — SA).** 48 битов. Глобально уникальный MAC-адрес, устанавливаемый IEEE.
- **Тип протокола. (Protocol type).** 16 битов. Для управляющих пакетов протокола SRP это значение равно 0 x 2007.
- **Версия типа управления (Control Version).** 8 битов. Номер версии для поля типа управляющего пакета. В настоящее время все типы управляющих сообщений относятся к версии 0.
- **Тип управляющего пакета (Control Type).** 8 битов. Возможные значения приведены в табл. 25.3.
- **Контрольная сумма (Control Checksum).** 16 битов.
- **Контроль времени существования пакета (Control TTL).** 16 битов. Это значение должно быть установлено таким же, как и TTL общего заголовка SRP, который инициатор управляющего сообщения использует для пакетов данных (т.е. как минимум вдвое большим числа узлов в кольце). TTL общего заголовка SRP попрежнему устанавливается равным 1.
- **Полезная нагрузка (payload).** Это поле имеет переменную длину.
- **Контрольная сумма фрейма (Frame Check Sum — FCS).** 32 бита. 32-битовая CRC.

Таблица 25.3. Значения типов управляющих пакетов

Значение	Описание
0x00	Зарезервировано
0x01	Анализ топологии
0x02	IPS-сообщение
0x03 до 0xFF	Зарезервировано

Поддержка многоадресатной рассылки

Протокол SRP непосредственно поддерживает многоадресатную рассылку пакетов протокола IP (пакетов класса D). Для многоадресатной рассылки зарезервированы MAC-адреса 00:00:5E:xx:xx:xx. Кроме этого, младший бит в старшем байте устанавливается как бит многоадресатной рассылки, младшие 23 бита IP-адреса класса D преобразуются в оставшуюся часть MAC-адреса.

Все IP-адреса узлов, обладающих функциями многоадресатной рассылки, отображаются в DA-адреса типа 01:00:5E:xx:xx:xx, которые используются как для отправки, так и для получения пакетов. Как уже говорилось ранее, пакет многоадресатной рассылки в конечном итоге распаковывается источником, после того как полностью пройдет все кольцо.

Резюме

Корпорация Cisco разработала протокол динамической транспортировки пакетов/эффективного использования полосы пропускания в качестве эффективной технологии, оптимизированной для передачи пакетов. Узлы подсоединены к двум кольцам оптоволоконных кабелей, имеющих противоположные направления. Оба этих кольца осуществляют передачу пакетов. Поскольку пакеты распаковываются только в

пункте назначения, а для доступа к кольцу не используется маркер, несколько узлов сети могут вести одновременную передачу по различным сегментам кольца, что позволяет увеличить доступную полосу пропускания.

Формат пакета SRP поддерживает восемь уровней приоритетов, которые копируются из битов очередности при отбрасывании протокола IP и могут быть использованы для установки внутренней очередности пакетов при передаче их узлом. В действительности интерфейсы протокола SRP имеют только два уровня очередности — очереди с низким и высоким приоритетами для передачи собственных и транзитных потоков данных. 8 уровней приоритета протокола IP преобразуются в эти два уровня очередности. Алгоритм справедливой очередности протокола SRP обеспечивает равноправный доступ к кольцу при переполнении, но при отсутствии переполнения позволяет использовать большую часть всей полосы пропускания.

Протокол DPT/SRP обладает значительной гибкостью и поддерживает технологию "plug-and-play" благодаря своей способности самовосстановления за счет сворачивания кольца при обрыве и функциям режима сквозной передачи.

Контрольные вопросы

1. Чем отличается протокол DPT/SRP от других кольцевых технологий, таких как Token Ring и FDDI?
2. Каким образом устанавливаются приоритеты пакетов в протоколе DPT/SRP?
3. Какой механизм используется для определения того, какое кольцо должен использовать узел для отправки пакета другому узлу?
4. Как происходит самовосстановление кольца DPT/SRP в случае обрыва кабеля?

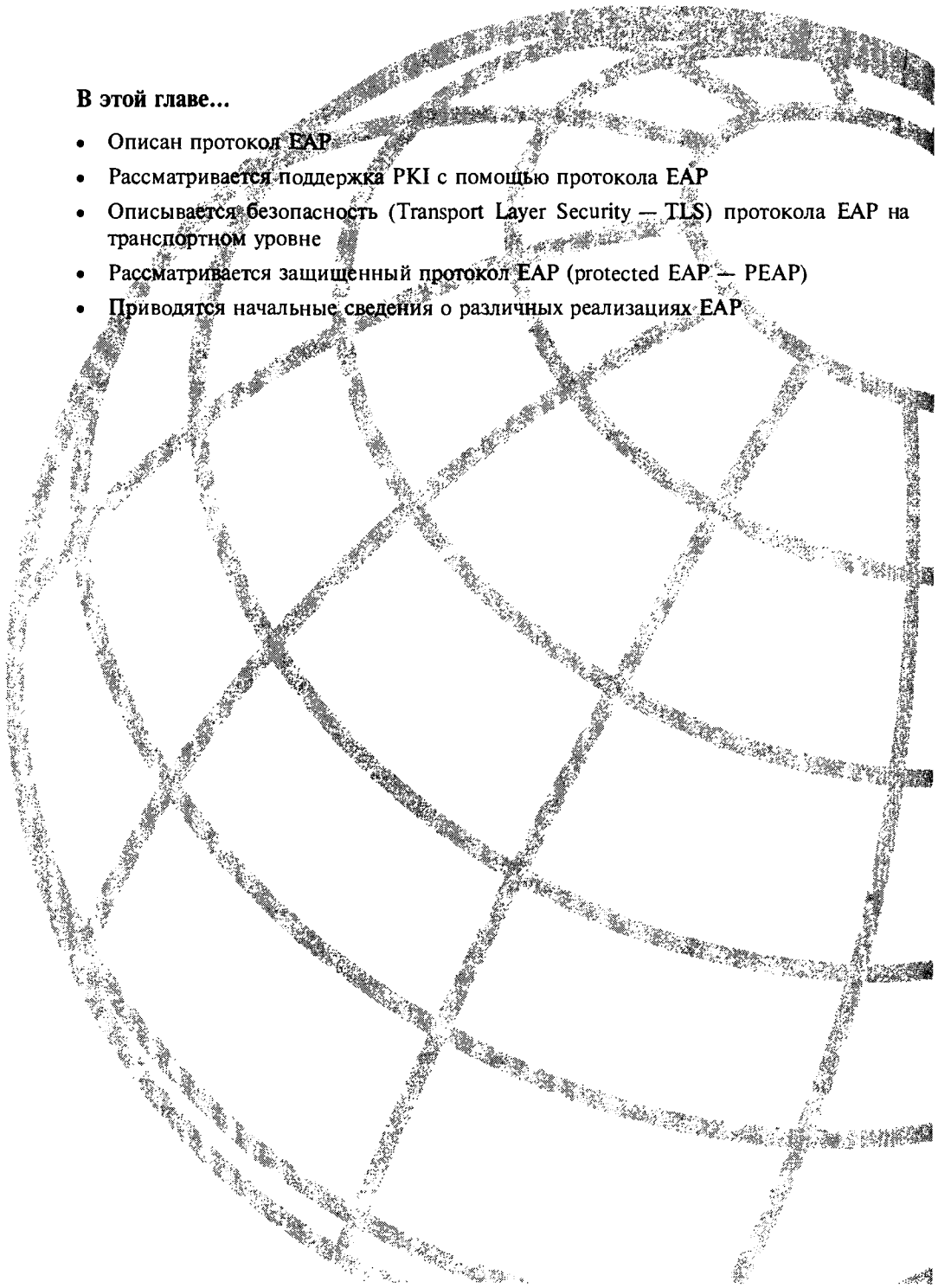
Дополнительные источники

- Белая книга: Технология и функционирование протокола динамической транспортировки пакетов (Dynamic Packet Transport Technology and Performance). Cisco Systems, 2000.
- Белая книга: Технология эффективного использования полосы пропускания (Spatial Reuse Protocol Technology), Cisco Systems, 2000.
- Информационный выпуск RFC 2892: The Cisco SRP MAC Layer Protocol. — August 2000.

Глоссарий

Transiting traffic. Транзитные потоки данных. Пакеты, которые узел DPT получает на своем DPT-интерфейсе и в неизмененном виде отправляет следующему DPT-узлу на кольце. Примером может служить пакет с MAC-адресом пункта назначения для станции, отличной от данного узла.

Transmitted traffic. Передаваемые потоки данных. Пакеты, для которых данный узел DPT является станцией MAC-источника. В их число входят как пакеты, генерируемые самим узлом, так и потоки данных, которые узел получает на других своих интерфейсах и пересылает с DPT-интерфейса.



В этой главе...

- Описан протокол EAP
- Рассматривается поддержка PKI с помощью протокола EAP
- Описывается безопасность (Transport Layer Security — TLS) протокола EAP на транспортном уровне
- Рассматривается защищенный протокол EAP (protected EAP — PEAP)
- Приводятся начальные сведения о различных реализациях EAP

Глава 26

Протокол расширяемой аутентификации (Extensible Authentication Protocol — EAP)

Протокол расширяемой аутентификации (Extensible Authentication Protocol — EAP) был разработан для поддержки нескольких механизмов аутентификации. Соединения протокола "точка — точка" (Point-to-Point Protocol — PPP) обычно обсуждают протокол аутентификации на стадии установки соединения протокола управления каналом (Link Control Protocol — LCP). Такой подход требует, чтобы протокол PPP поддерживал используемый метод аутентификации.

Хотя для соединений протокола PPP аутентификация на этапе установки соединения протокола LCP не требуется, конечные точки обсуждают какой протокол аутентификации будет использован для установки соединения. При этом могут быть выбраны разные варианты: без аутентификации, аутентификация по протоколу PAP или по протоколу CHAP. В протоколе EAP обсуждение механизма аутентификации откладывается до того момента, когда будет собрано больше информации о соединении. В последнее время возникали опасения в отношении целостности механизмов аутентификации и протокол EAP представляет собой попытку создать базу безопасной работы этой части управления доступом к сети. Многие производители встраивают поддержку протокола EAP в приложения как клиента, так и сервера.

В настоящей главе рассматривается сам протокол EAP, определенный в спецификации RFC 2284. В данной главе рассматриваются некоторые его специфические черты, определенные в данной спецификации RFC, что облегчит понимание основ данного протокола. В ней наряду с проблемами защиты сети описываются преимущества использования протокола EAP, которые в ряде случаев делают этот протокол столь привлекательным. Для решения этих задач защиты сети может оказаться полезной служба входного доступа пользователя с удаленной аутентификацией (Remote Authentication Dial-In User Service — RADIUS). В настоящей главе описывается, каким образом служба RADIUS может быть использована в качестве конечной службы поддержки аутентификации пользователя. На основе этой более полной картины процесса аутентификации в протоколе EAP будут рассмотрены различные сетевые реализации протокола EAP.

Протокол EAP

Спецификация протокола EAP несложна. Процесс аутентификации состоит всего лишь из нескольких этапов. Далее будут подробно рассмотрены эти этапы и различные опции, которые доступны для клиента и аутентификатора.

Протокол EAP начинает свою работу, после того, как установка связи (канала) закончена. Обсуждение протокола EAP происходит в информационном поле пакета данных канального уровня протокола PPP. На рис. 26.1 показаны различные поля пакетов протокола EAP и длина каждого поля в октетах.

Рис. 26.1 Формат пакета протокола EAP

На рис. 26.1 показаны пять различных элементов пакета EAP. Первые три поля являются обязательными. В зависимости от типа посылаемого EAP-пакета остальные поля могут присутствовать или отсутствовать. Каждое поле обсуждается в ниже приведенном списке.

- **Код**. Поле кода пакета EAP идентифицирует тип посылаемого EAP-пакета. Это поле имеет длину один октет и содержит одно из четырех значений:
  - — Запрос;
  - — Ответ;
  - — Успешно;
  - — Неудачно.
- **Идентификатор**. Поле идентификатора имеет длину один октет. Оно содержит номер идентификатора для данного пакета. Это поле используется для установления соответствия между пакетами запросов и пакетами ответов. Может возникнуть необходимость в том, чтобы клиент повторил запрос. При повторной передаче требуется использовать тот же самый идентификатор, как и в предыдущей попытке, с тем, чтобы аутентификатор мог различить пакеты повторной передачи и пакеты нового запроса.
- **Длина**. Поле длины составляет два октета и определяет длину EAP-пакета. Значение поля длины равно сумме длин следующих полей EAP-пакета: полей кода, идентификатора, длины и данных. Все остальные данные после поля длины рассматриваются как заполнитель канального уровня протокола PPP и игнорируются протоколом EAP.
- **Тип**. Поле "тип" EAP-пакета указывает тип, содержащихся в нем данных. Значение этого поля зависит от поля кода пакета. Код запроса или ответа указывает, что значение поля типа было установлено. Это поле типа имеет длину один октет. Тип "негативное подтверждение" (Negative Acknowledgment — NAK)

может быть использован только в ответном пакете для указания того, что запрошенный тип аутентификации не поддерживается. Поддержка вышеперечисленных четырех типов требуется от всех реализаций протокола EAP. Отметим, что если пакет представляет собой пакет с сообщением об успешности или неудачности кода, то это поле не является обязательным. Возможными типами являются следующие:

1. **Идентичность**. Аутентификатор обычно использует тип идентичности в первом пакете процесса аутентификации для запроса идентификационных данных клиента. Он представляет собой первоначальный запрос клиенту на отправку его аутентификационных данных.
2. **Уведомление**. Представляет собой сообщение от аутентификатора, которое будет отображено у клиента. Оно может быть сообщением-предупреждением или сообщением об истечении срока действия пароля. Отправка такого сообщения не является обязательной, хотя реализация протокола EAP должна поддерживать использование таких сообщений.
3. **Негативное подтверждение (Negative Acknoledgement — NAK)**. Этот тип поля действителен только в ответных пакетах. Он используется в тех случаях, когда запрашивается неприемлемый тип аутентификации. Например, аутентификатор может запросить аутентификацию PAP, а клиент поддерживает только аутентификацию CHAP. В этом случае клиент отправляет негативное подтверждение NAK для того, чтобы аутентификатор запросил альтернативный тип аутентификации.
4. **Запрос MD-5**. Это поле представляет собой запрос к одноранговому устройству, подобно запросу CHAP в стандартном обсуждении аутентификации протокола PPP. Это одноранговое устройство должно ответить либо другим запросом MD-5, либо негативным подтверждением NAK.
5. **Одноразовый пароль (One-Time Password—OTP).** Это сообщение является запросом относительно аутентификации через систему OTP. Ответом на пакет типа OTP должно быть либо негативное подтверждение NAK, либо сообщение о типе пароля OTP.
6. **Типовая карта маркера (Generic Token Card).** Этот тип определен для использования с различными реализациями карты маркера. Аутентификатор отправляет этот тип сообщения, в котором содержится запрос ввода данных пользователем.
7. **Тип-данные**. Поле "тип-данные" может иметь длину 0 байтов, либо больше, в зависимости от поля типа EAP-пакета. Как правило, это поле в пакете запроса содержит сообщение для отображения клиенту. Если этот пакет представляет собой пакет негативного подтверждения NAK, то поле "тип-данные" содержит информацию о том, какой метод аутентификации является приемлемым. Если поле типа (Type field) представляет собой запрос MD-5, то содержимое поля тип-данные должно соответствовать следующим полям протокола CHAP PPP: значение-размер (Value-size), значение (Value) и имя (Name) (см. спецификацию RFC [1994] для PPP CHAP). Если поле типа представляет собой запрос OTP или типовую карту маркера, то поле тип-данные содержит информацию, которую запрашивает сервер для аутентификации.

Использование службы RADIUS для аутентификации EAP

Одним из наиболее привлекательных качеств протокола EAP является его способность добавлять RADIUS в качестве службы удаленной (back-end) аутентификации . При использовании RADIUS-сервера, аутентификация EAP несколько отличается от традиционной RADIUS-аутентификации. В традиционной службе аутентификации RADIUS сервер доступа к сети (Network Access Server — NAS) запрашивает у пользователя метод аутентификации, который будет использоваться. Когда клиент отвечает на запрос сервера NAS, последний создает пакет запроса на доступ, который будет отправлен серверу RADIUS путем трансляции этого метода аутентификации в соответствующий RADIUS-атрибут для сервера. Сервер RADIUS отвечает ответным пакетом, содержащим либо разрешение на доступ либо отказ в нем. Когда сервер NAS получает ответ, он интерпретирует результаты согласно выбранному методу аутентификации и отправляет их клиенту, принимая или отвергая аутентификацию пользователя. Такой способ несколько отличается от использования EAP в качестве механизма аутентификации.

В тех случаях, когда сервер NAS использует RADIUS в качестве удаленного сервера для EAP-аутентификации, от самого NAS не требуется поддерживать используемый метод аутентификации. В этом случае NAS функционирует как прокси-сервер для аутентификации между клиентом и сервером RADIUS и прозрачно передает сообщение аутентификации между клиентом и удаленным сервером. Сервер NAS больше не участвует в процессе аутентификации. Он функционирует в режиме прокси-сервера, поддерживая обмен EAP-сообщениями двух удаленных одноранговых устройств. Эта общая платформа аутентификации в настоящее время позволяет производителям разрабатывать и использовать различные методы аутентификации, которые понятны и клиенту, и серверу, не заботясь об их поддержке сервером NAS, который требуется только для того, чтобы объединить EAP-сообщения и отправить их RADIUS-серверу.

Для поддержки протокола EAP были добавлены два новых атрибута службы RADIUS. Совместно они обеспечивают поддержку службой RADIUS протокола EAP.

Первый атрибут представляет собой EAP-сообщение (EAP-Message). Он используется для отправки информации протокола EAP от клиента к серверу и наоборот. Сервер NAS может посылать информацию в одном или нескольких EAP-сообщениях. Он может также использовать данный атрибут для ответа на пакеты вызова, согласия или отказа. Предполагается, что этот метод аутентификации будет использоваться для усиленной криптографии и для других чувствительных методов аутентификации.

Вторым добавленным RADIUS-атрибутом является атрибут "сообщение-аутентификатор" (Message-Authenticator). Этот атрибут поддерживает целостность пакетов службы RADIUS и отражает попытки атак на RADIUS-сервер EAP путем защиты данных, находящихся внутри пакета. Этот атрибут должен использоваться каждый раз, когда в RADIUS-пакетах запроса, согласия или вызова имеется атрибут EAP-Message. Если имеется атрибут "EAP-сообщение", а атрибут "сообщение-аутентификатор" отсутствует, то пакет должен быть отброшен, потому что целостность пакета проверить в этом случае невозможно. В табл. 26.1 описаны два новых атрибута RADIUS и приведены их номера согласно IETF.

Таблица 26.1. Номера атрибутов IETF для аутентификации EAP RADIUS

Номер IETF	Атрибут	Описание
79	EAP-сообщение	Инкапсулирует EAP-информацию, которая будет передаваться между клиентом и RADIUS-сервером
80	Сообщение – аутентификатор	Обеспечивает целостность сообщения путем зашифровки EAP-сообщений с помощью секретного RADIUS-ключа

Типичное обсуждение аутентификации

Теперь, когда есть понимание того, как функционирует протокол EAP и стала ясна роль удаленного RADIUS-сервера в процессе аутентификации, следует рассмотреть типичное обсуждение аутентификации с клиентом протокола EAP, сервером NAS и сервером RADIUS. В разных сетевых структурах используются различные реализации протокола EAP. Каждая реализация следует основным базовым предпосылкам для потока аутентификационных данных. На рис. 26.2 показан основной поток пакетов аутентификации для RADIUS EAP, включая клиента, NAS-сервер и RADIUS-сервер.

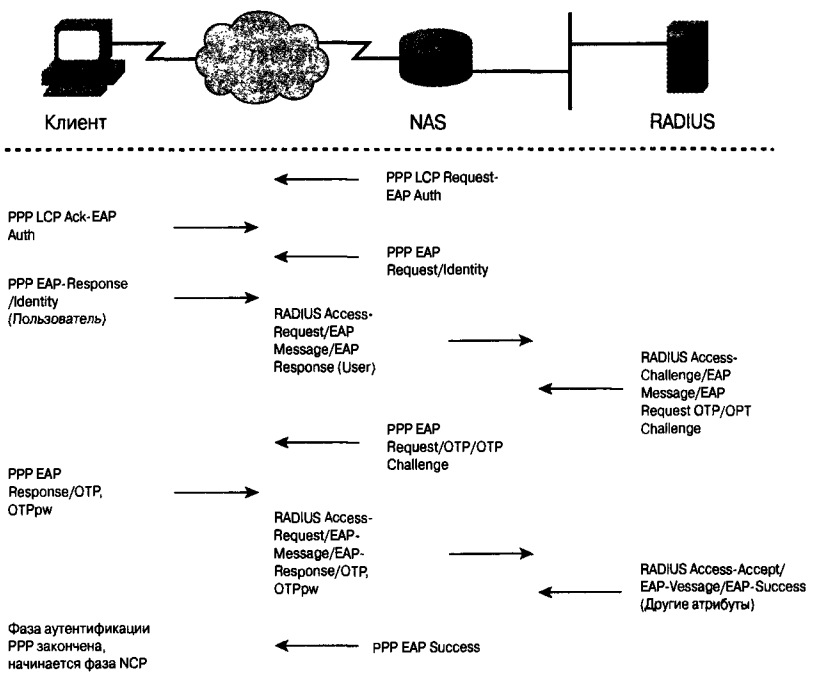


Рис. 26.2 Поток аутентификационных пакетов протокола EAP RADIUS

Поддержка инфраструктуры PKI с помощью протокола EAP

Можно ли использовать цифровые сертификаты при аутентификации пользователя с помощью протокола EAP? Инфраструктура общедоступных ключей (Public Key In-

frastructure — PKI) использует такие цифровые сертификаты. Она предназначена для работы с асимметричными криптографическими ключами с целью обеспечить достоверность передаваемых данных. Эти данные могут быть данными аутентификации для конкретного пользователя и конкретного применения, которые действительны только на определенный период времени.

Два разрабатываемого в настоящее время стандарта протокола EAP используют цифровые сертификаты EAP-TLS и PEAP. Каждый из них имеет свои перспективы. Нельзя сказать, чтобы какой-либо из них был лучше или хуже другого. Однако, каждый из этих методов имеет присущие ему ярко выраженные свойства и соответствует различным требованиям. По самой своей природе использование цифровых сертификатов для аутентификации пользователя представляет некоторую сложность. В настоящее время возрастают требования к новым реализациям протокола EAP и в последующих двух разделах обсуждаются новые расширения этого протокола.

Безопасность протокола EAP на транспортном уровне (EAP-Transport Layer Security — EAP-TLS)

Безопасность на транспортном уровне (Transport Layer Security — TLS) представляет собой новейшую версию группы IETF для протокола безопасного уровня сокета (Secure Socket Layer—SSL). Протокол TLS представляет собой версию 3.0 протокола SSL. Протокол TLS аутентифицирует пользователя, как для сервера аутентификации, так и для клиента. Каждый из них использует свой частный ключ и сертификат для проверки своего партнера по связи. Сначала сервер посылает свои идентификационные данные. Клиент проверяет сертификат с помощью надежного сервера проверки полномочий сертификата (Certificate Authority — CA). После того как произошла идентификация сервера клиентом, последний посылает свой сертификат серверу для идентификации пользователя, пытающегося пройти аутентификацию. Сервер проверяет действительность сертификата на своем CA-сервере для подтверждения полномочий пользователя. Такая проверка известна как взаимная аутентификация. При этом каждая сторона проверяет аутентичность другой стороны для того, чтобы получить положительный результат проверки EAP, не передавая пароли по каналу.

Защищенный протокол EAP (Protected EAP—PEAP)

Защищенный протокол EAP (Protected EAP — PEAP), использует те же принципы, что и протокол EAP-TLS. Однако, при использовании PEAP аутентификация имеет несколько иной характер. PKI используется только для аутентификации клиентом сервера. Этот процесс называется сертифицированием со стороны сервера. Такой тип аутентификации преследует три цели. Во-первых, это позволяет клиенту сделать запрос серверу с тем, чтобы последний доказал свою идентичность с сертификатом. Это во многом напоминает любой общедоступный Web-сайт, который использует протокол SSL. Когда пользователь посещает Web-сайт с использованием протокола SSL (HTTPS в браузере), от сервера требуется предоставить свой сертификат для доказательства, что он является узлом, с которым пытаются установить соединение. Второй целью использования протокола PEAP является достижение большей гибкости в аутентификации пользователя. Иногда бывает непрактичным выпускать отдельный сертификат для каждого клиента, который последствии будет использоваться для его аутентификации. Протокол PEAP позволяет использовать альтернативные методы аутентификации со стороны пользователя, включая OTP-пароли.

Третьей и последней целью использования сертификата со стороны сервера является зашифровка сеанса с помощью сертификата сервера до того, как пользователь направит свое имя серверу. Это предотвращает ситуацию, когда атакующие извлекают имя пользователя из пакета аутентификации.

Реализации протокола EAP

Теперь, когда описан протокол EAP и его различные расширения, можно рассмотреть различные приложения этого мощного механизма аутентификации. Сфера использования этого протокола все время расширяется. Протокол EAP был введен в модели аутентификации при беспроводном доступе. Преимущества обязательной аутентификации на 2-м уровне для доступа к сети очевидны. Использование этого механизма не позволяет узлам получать адрес 3-го уровня до окончания аутентификации. Эта концепция была расширена на среды LAN-коммутации. Использование протокола EAP для управления доступом к порту коммутатора на 2-м уровне позволяет сетевым администраторам иметь полный контроль над тем, какие пользователи получают право на доступ к локальной сети LAN. Кроме того, этот метод аутентификации обеспечивает средства контроля сети VLAN пользователя, независимо от физического порта коммутатора. Для поддержки атрибутов такого административного контроля системные администраторы используют службу RADIUS.

В дополнение к этим реализациям, протокол EAP был расширен на методы удаленного доступа. Протокол EAP может быть применен к традиционным соединениям удаленного доступа, а также к соединениям VPDN в тех случаях, когда конечной точкой является маршрутизатор. От сервера NAS требуется только поддержка протокола EAP как одного из типов PPP-аутентификации. Как уже говорилось ранее, метод аутентификации, используемый в протоколе EAP, не обязательно должен поддерживаться самим сервером NAS. Последний лишь выполняет функции прокси-сервера для аутентификации сервера RADIUS. На рис. 26.3 показаны все упомянутые выше реализации протокола EAP — для беспроводной связи, удаленного доступа и коммутируемой LAN-сети.

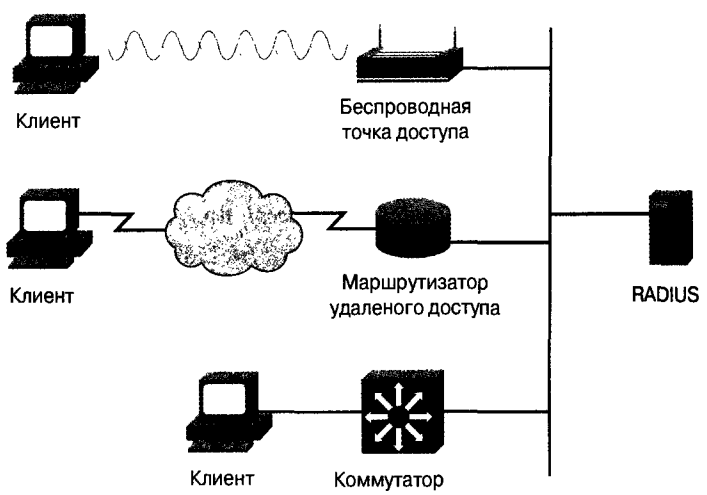


Рис. 26.3 Физические топологии для различных реализаций аутентификации протокола EAP

По мере расширения использования протокола EAP для аутентификации все чаще используется встроенная поддержка этих механизмов аутентификации. В настоящее время операционные системы Microsoft Windows поставляются с уже встроенной поддержкой EAP-аутентификации для сетевых соединений. Дистрибьютерские пакеты Linux также поддерживают протокол EAP в качестве метода идентификации. Корпорация Cisco Systems также уже включила в свои операционные системы поддержку всех этих методов аутентификации. Другие производители также работают в этом направлении.

Резюме

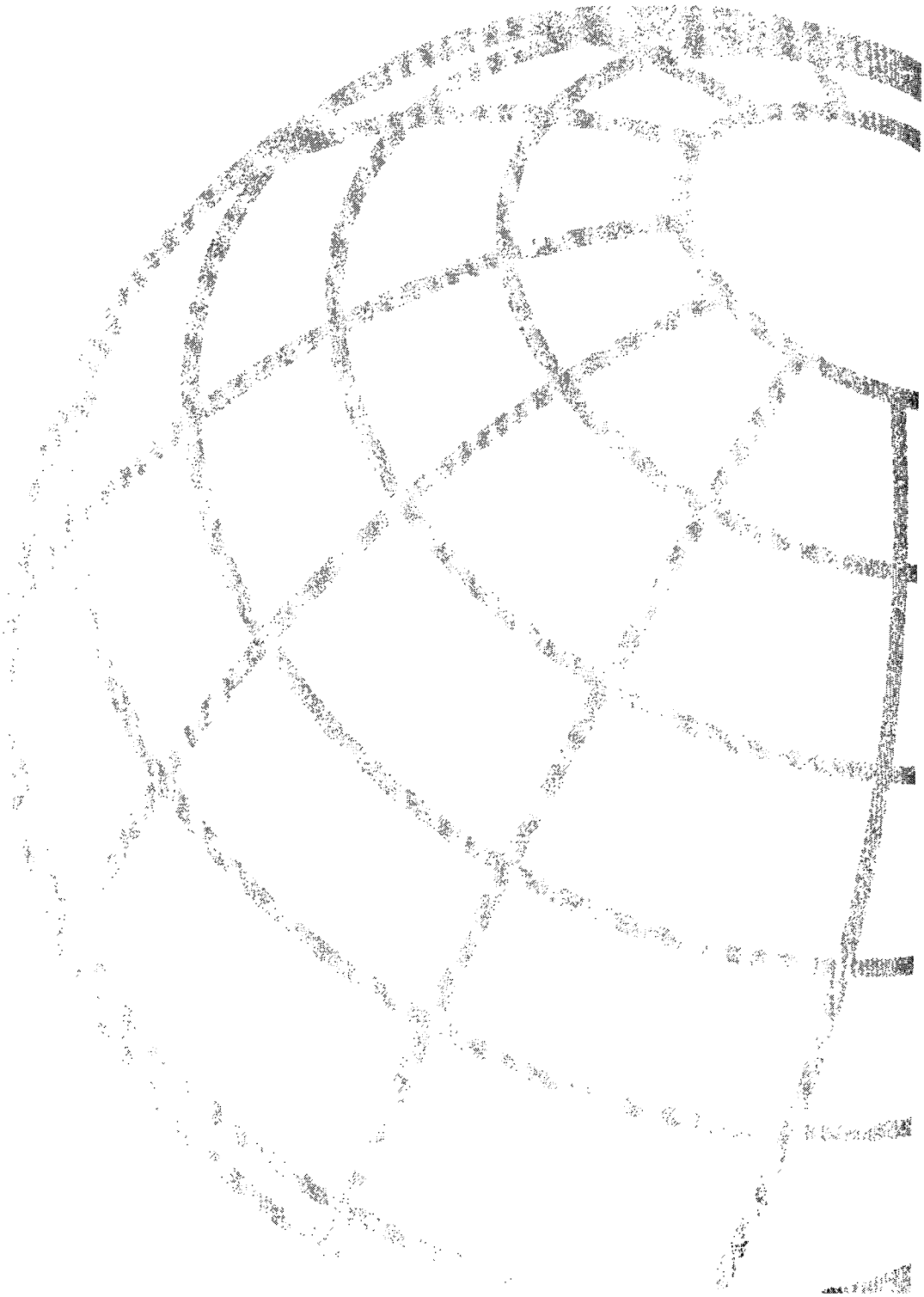
Как было показано в настоящей главе, протокол EAP представляет собой мощное средство аутентификации пользователя в сетях доступа. Его популярность все более возрастает по мере того, как сетевые администраторы и производители осознают его гибкость. Используя протокол EAP сетевые администраторы могут использовать механизмы строгой аутентификации, которые удовлетворяют всем требованиям проводимой политики безопасности, начиная с традиционных сертификатов MD5-Challenge до цифровых сертификатов. В настоящее время протокол EAP охватывает различные реализации от беспроводной до коммутируемой LAN-аутентификации. Можно уверенно предположить, что протокол EAP вскоре станет стандартом, роль которого в завтрашних сетях будет все более увеличиваться.

Контрольные вопросы

1. Какое поле EAP-пакета указывает, является ли сообщение запросом, ответом на запрос, положительным или отрицательным ответом?
2. В чем первичное преимущество использования EAP в качестве механизма аутентификации?
3. Какие два атрибута RADIUS используются при EAP – аутентификации?
4. Поддерживает ли EAP сертификаты со стороны сервера, со стороны клиента или оба типа сертификатов?

Дополнительные источники

- RFC 2284, *PPP Extensible Authentication Protocol*, ftp://ftp.isi.edu/in-njtes/rfc2284.txt
- RFC 2716, *PPP EAP-TLS Authentication Protocol*, ftp://ftp.isi.edu/in-njtes/rfc2716.txt
- RFC 2689, *RADIUS Extensions,* www.ietf.org/rfc/rfc2689.txt
- Internet Draft: Protected EAP Protocol, www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-0.5.txt



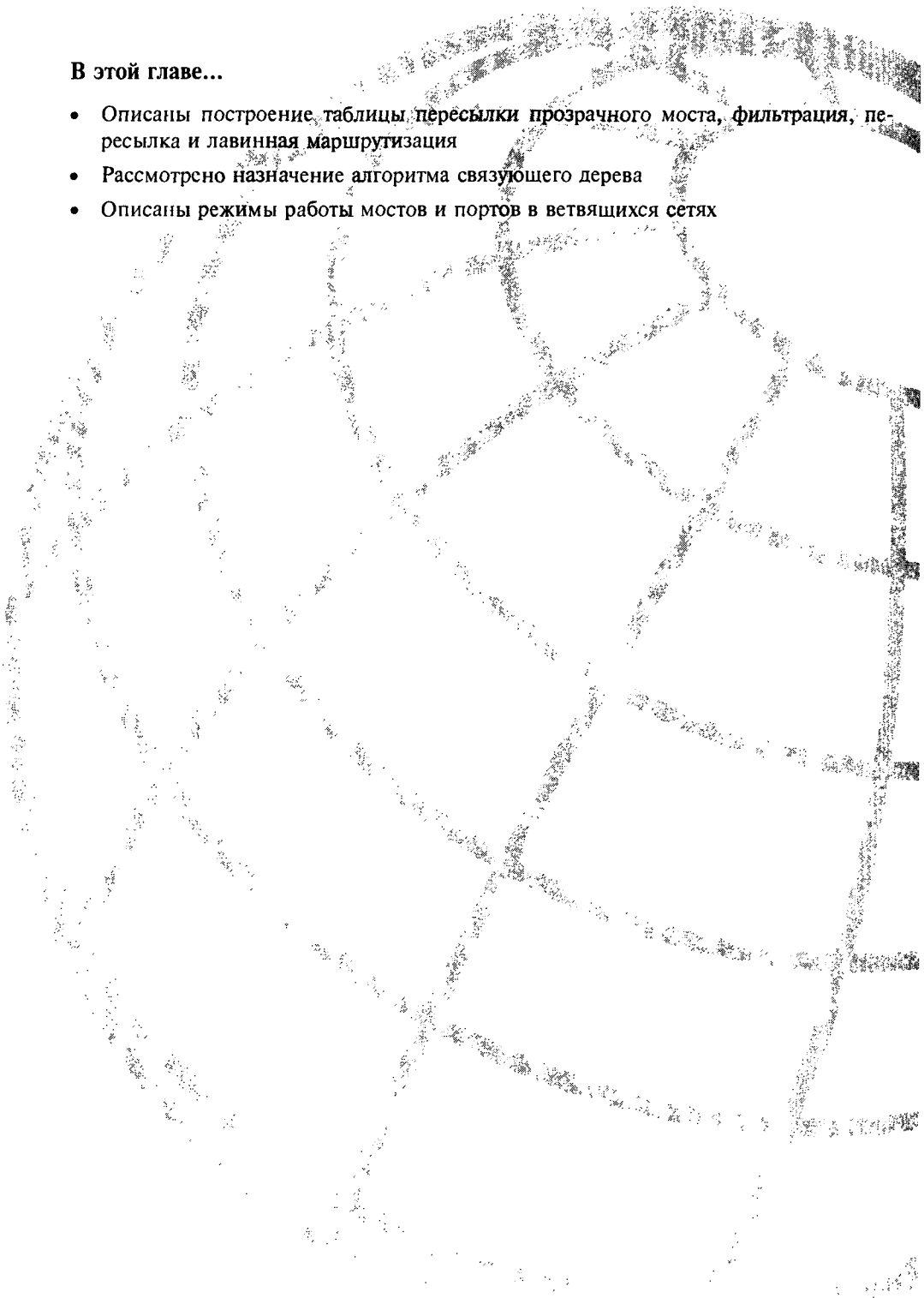
Часть V

Мосты и переключатели

Глава 27. Прозрачные мостовые соединения
Глава 28. Мостовое соединение разнородных сетей
Глава 29. Мостовая маршрутизация от источника
Глава 30. Коммутируемые локальные сети и сети VLAN
Глава 31. Коммутация в режиме ATM
Глава 32. Коммутация MPLS
Глава 33. Технология DLSw

В этой главе...

- Описаны построение таблицы пересылки прозрачного моста, фильтрация, пересылка и лавинная маршрутизация
- Рассмотрено назначение алгоритма связующего дерева
- Описаны режимы работы мостов и портов в ветвящихся сетях



Глава 27

Прозрачные мостовые соединения

Первые прозрачные мосты были разработаны в начале 80-х годов корпорацией Digital Equipment (Digital). Digital предложила свою разработку на рассмотрение институту IEEE, который включил ее в свой стандарт IEEE 802.1. Прозрачные мосты широко распространены в сетях Ethernet/IEEE 802.3. В настоящей главе рассматривается обработка потоков данных и компоненты протоколов прозрачных мостовых соединений.

Функционирование прозрачного мостового соединения

Прозрачные мосты получили свое название благодаря тому, что их присутствие и работа прозрачны для узлов сети. При включении прозрачные мосты изучают расположение рабочих станций путем анализа адресов источников входящих фреймов из всех присоединенных к ним сетей. Например, если на порт 1 моста поступает фрейм из узла A, то мост делает вывод, что к узлу A может быть достигнут доступ через сегмент, подключенный к порту 1. Действуя таким образом прозрачные мосты формируют таблицу, аналогичную представленной на рис. 27.1.

Адрес узла	Номер сети
15	1
17	1
12	2
13	2
18	1
9	1
14	3
.	.
.	.
.	.

Рис. 27.1. Прозрачный мост создает таблицу, описывающую доступность узлов сети

Мост использует эту таблицу для пересылки поступающих данных. При поступлении фрейма на один из своих интерфейсов мост просматривает свою внутреннюю таблицу в поисках адреса получателя этого фрейма. Если в таблице имеется запись, соответствующая этому адресу, и при этом соответствующий порт отличается от того, на который фрейм поступил, то фрейм пересылается через этот порт. Если соответствующей записи не найдено, то фрейм передается через все порты, кроме того, на который поступил. Такой процесс называется лавинной маршрутизацией. Широковещательная и многоадресная рассылки также выполняются путем лавинной маршрутизации.

Прозрачные мосты надежно изолируют межсегментую передачу данных, уменьшая тем самым трафик отдельных сегментов. Этот процесс называется *фильтрацией* и осуществляется в тех случаях, когда MAC-адреса источника и получателя принадлежат одному интерфейсу моста. Обычно фильтрация повышает скорость реагирования сети, что непосредственно ощущается пользователем. То, насколько сокращается объем передачи данных и повышается скорость реагирования, зависит от соотношения межсегментного и общего трафика, а также от объема передачи широковещательных и многоадресатных данных.

Мостовые петли

Если между двумя локальными сетями существует несколько маршрутов через мосты и локальные сети, то алгоритм прозрачного моста без протокола межмостовой передачи не срабатывает. Такая мостовая петля показана на рис. 27.2.

Предположим, узел А посылает фрейм узлу В. Оба моста получают этот фрейм и делают правильный вывод, что узел А находится в сегменте 2. Затем каждый мост отправляет фрейм в сегмент 2. К сожалению, дело не ограничится тем, что узел В получит две копии данного фрейма: одну — от моста 1 и одну — от моста 2. Теперь оба моста будут считать, что узел А находится в том же сегменте, что и узел В. Когда узел В будет отвечать на фрейм узла А, этот ответ получат оба моста и отфильтруют его, поскольку, согласно адресной таблице мостов, получатель (узел А) находится в том же сегменте сети, где и источник фрейма.

Распространение широковещательных сообщений в сетях с петлями представляет серьезную проблему. Предположим, что первый фрейм, поступивший от узла А (рис. 27.2), является широковещательным. Тогда оба моста будут пересылать фреймы бесконечно, используя всю доступную полосу пропускания сети и блокируя передачу других пакетов в обоих сегментах.

Но топология с петлями, приведенная на рис. 27.2 и вызывающая в данном случае проблемы, иногда может быть и полезной. Петля предполагает существование нескольких маршрутов в объединенной сети, а сеть с несколькими маршрутами между источником и получателем вследствие своей топологической гибкости отличается повышенной устойчивостью к сбоям.

Алгоритм связующего дерева

Алгоритм связующего дерева (Spanning-Tree Algorithm — STA) был разработан корпорацией Digital Equipment, основным производителем оборудования Ethernet, чтобы сохранить преимущества петель, одновременно избегая связанных с ними проблем. Впоследствии алгоритм корпорации Digital был рассмотрен комитетом IEEE 802 и опубликован в спецификации IEEE 802.1d. Следует отметить, что алгоритм Digital и алгоритм IEEE 802.1d несовместимы.

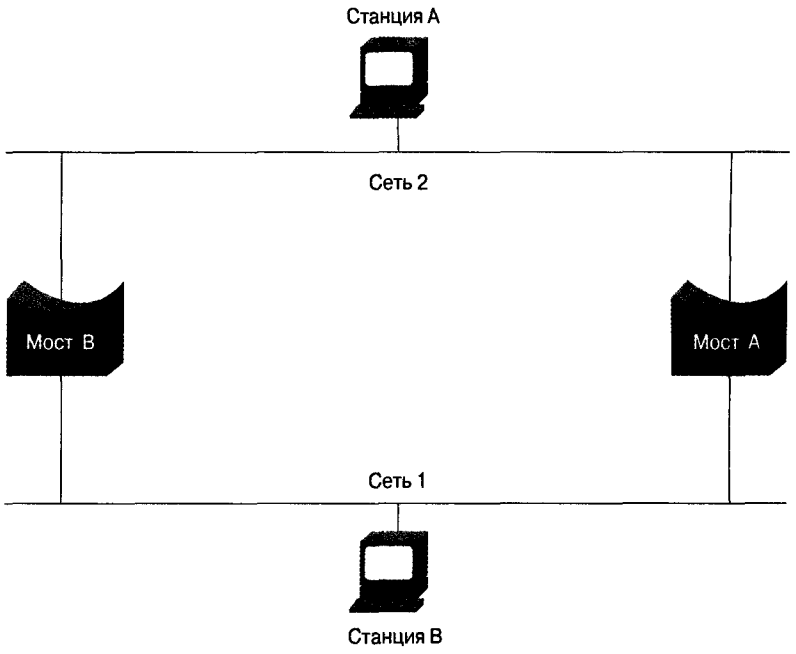


Рис. 27.2. Мостовые петли в среде прозрачных мостовых соединений могут стать причиной неточной пересылки и ошибок при построении адресных таблиц

Алгоритм STA выбирает в топологии сети подмножество без петель путем расположения мостовых портов таким образом, что если порт активен, то в режиме ожидания (блокировки) он создает петли. При обрыве первичного соединения заблокированные мостовые порты могут быть активизированы, создавая новый маршрут по сети.

В основе построения подмножества сетевой топологии без петель при помощи алгоритма STA, лежит теория графов, согласно которой для любого связного графа, состоящего из узлов и ребер, соединяющих пары узлов, связующее дерево из ребер поддерживает связность графа, но не содержит петель.

На рис. 27.3 показано, как с помощью алгоритма STA удаляются петли. Для работы алгоритма STA требуется, чтобы каждому мосту был присвоен идентификатор. Как правило, этим идентификатором является один из MAC-адресов моста (Media Access Control — MAC) и приоритет, назначенный администратором. Каждому порту также назначается уникальный идентификатор (в пределах моста), которым обычно является его собственный MAC-адрес. Кроме того, каждому порту моста сопоставляется стоимость маршрута, соответствующая затратам на передачу фрейма по локальной сети через данный порт. На рис. 27.3 стоимость маршрута отмечена на линиях, исходящих из каждого моста. Эта стоимость обычно определяется по умолчанию, но может быть и задана вручную сетевым администратором.

Прежде всего при вычислении связующего дерева производится выбор *корневого моста (root bridge)*,. Которым является мост с наименьшим значением идентификатора. На рис. 27.3 корневым является мост 1. Затем для всех остальных мостов определяется *корневой порт (root port)*. Под корневым портом моста понимается порт, через который может быть достигнут корневой мост с наименьшими суммарными затратами, которые называются *стоимостью корневого маршрута (root path cost)*.

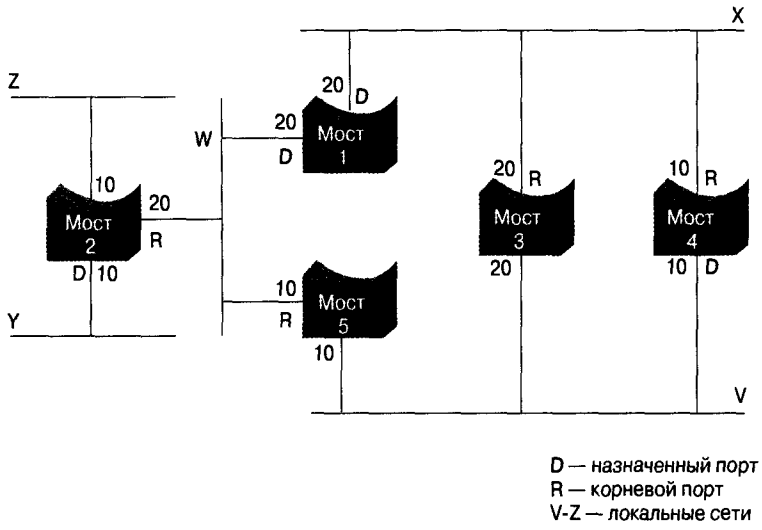


Рис. 27.3. Для того, чтобы избежать петель, мосты, расположенные с использованием алгоритма STA, используют назначенные и корневые порты

После этого определяются назначенные мосты и их назначенные порты. Под назначенным мостом понимается мост каждой локальной сети, обеспечивающий минимальную стоимость корневого маршрута. *Назначенный мост (deignated bridge)* локальной сети представляет собой единственный мост, которому разрешено пересылать обмениваться с другими сегментами фреймами локальной сети, для которой он является назначенным. Под *назначенным портом (designated port)* локальной сети понимается порт, соединяющий ее с назначенным мостом.

Иногда у двух и более мостов могут оказаться равными стоимости корневых маршрутов. Например, на рис. 27.3 мосты 4 и 5 позволяют достичь моста 1 (корневого) с затратами, равными 10. В таком случае снова используются идентификаторы мостов, но на этот раз, чтобы определить назначенные мосты. Порту локальной сети V моста 4 отдается предпочтение по сравнению с портом локальной сети V моста 5.

При продолжении этого процесса для каждой локальной сети исключаются все мосты, кроме одного, который непосредственно соединен с ней. Таким путем удаляются все петли между парами локальных сетей. Кроме того, алгоритм STA исключает петли, охватывающие более двух локальных сетей, сохраняя при этом связность. На рис. 27.4 показан результат применения алгоритма STA к сети, изображенной на рис. 27.3. На рис. 27.4 более ясно видна топология дерева. На нем также показано, что согласно алгоритму STA порты моста 3 и моста 5 к локальной сети V переведены в режим ожидания.

Вычисление связующего дерева происходит при включении моста и при каждом изменении топологии сети. Эти вычисления требуют обмена информацией между мостами связующего дерева, что осуществляется при помощи *конфигурационных сообщений,* иногда называемых *модулями данных мостового протокола* (Bridge Protocol Data Units — BPDU). Конфигурационные сообщения содержат информацию, идентифицирующую мост, который, как предполагается, должен стать корневым (идентификатор корня), и расстояние от моста-источника до корневого моста (стоимость корневого маршрута). Кроме того, в конфигурационных сообщениях содержатся идентификаторы моста-источника и его порта, а также давность этой информации.

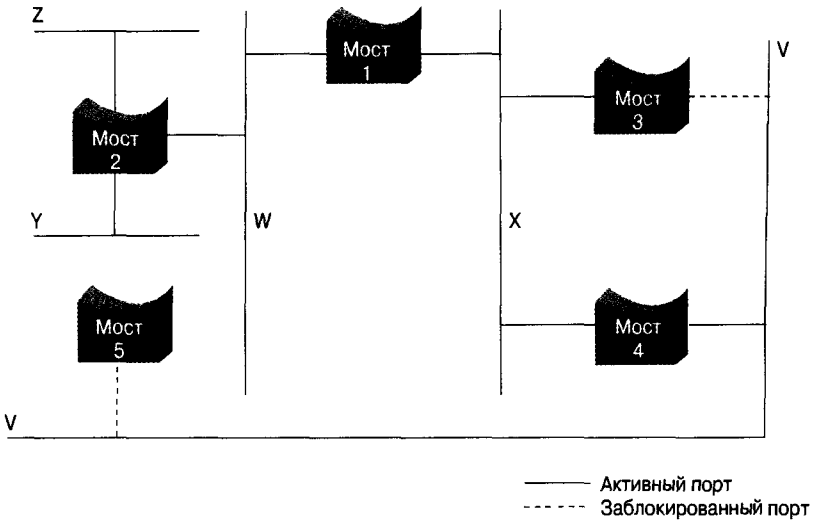


Рис. 27.4. Топология дерева без петель в сети с прозрачными мостами, построенная с использованием алгоритма STA

Мосты обмениваются конфигурационными сообщениями через равные интервалы (обычно от 1 до 4 секунд). В случае отказа моста (что приводит к изменению топологии) соседние мосты, не получив конфигурационные сообщения, начинают пересчет связующего дерева.

Все решения при выборе топологии прозрачных мостов принимаются локально, на уровне каждого отдельного моста. Мосты обмениваются конфигурационными сообщениями с соседними мостами. Центрального управления для определения сетевой топологии или администрирования не существует.

Формат фреймов

Прозрачные мосты обмениваются *конфигурационными сообщениями* и *сообщениями об изменении топологии*. Конфигурационные сообщения передаются между мостами для установления сетевой топологии. Сообщения об изменении топологии посылаются после того, как было обнаружено изменение топологии, для чтобы сообщить о необходимости пересчета связующего дерева. Получив такое сообщение, мосты заново исследуют расположение узлов, так как узел, прежде доступный из порта 1, после изменения топологии может стать доступным через порт 2.

На рис. 27.5 показан формат конфигурационного сообщения IEEE 802.1d.

Конфигурационное сообщение для прозрачного моста состоит из описанных ниже полей.

- **Идентификатор протокола.** Содержит ноль.
- **Версия.** Содержит ноль.
- **Тип сообщения.** Содержит ноль.

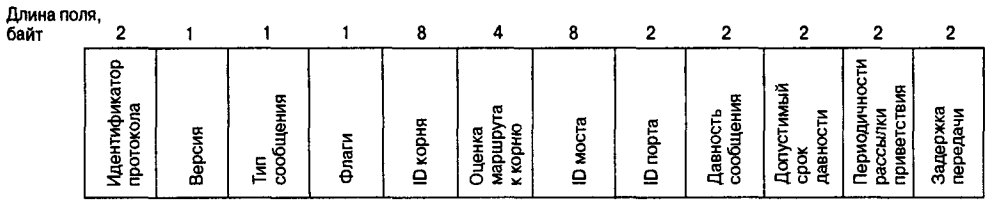


Рис. 27.5. Конфигурационное сообщение прозрачного моста состоит из 12 полей

- **Флаг.** Содержит 1 байт, в котором используются только 2 бита. Младший из них называется битом изменения топологии (topology-change — TC) и сообщает об изменении топологии. Старший называется битом подтверждения изменения топологии (topology-change acknowledgment — TCA) и устанавливается для подтверждения получения конфигурационного сообщения с установленным битом TC.
- **ID корневого моста.** Идентифицирует корневой мост и состоит из его 2-байтового приоритета и 6-байтового идентификатора.
- **Стоимость маршрута к корню.** Стоимость маршрута от моста, отправляющего конфигурационное сообщение, к корневому мосту.
- **ID моста.** Идентифицирует приоритет и ID моста, отправляющего сообщение.
- **ID порта.** Идентифицирует порт, из которого было отправлено конфигурационное сообщение. Это поле позволяет обнаруживать и обрабатывать петли, образованные несколькими связанными мостами.
- **Давность сообщения.** Время, прошедшее с момента отправки корневым маршрутизатором конфигурационного сообщения, на котором основано данное конфигурационное сообщение.
- **Допустимый срок давности.** Указывает, когда данное конфигурационное сообщение должно быть удалено.
- **Время приветствия (Hello Time).** Промежуток времени между конфигурационными сообщениями корневого порта.
- **Задержка передачи.** Период ожидания, который должен пройти, прежде чем мост перейдет в новое состояние после изменения топологии. Если переход происходит слишком быстро, то не все сетевые соединения могут быть готовы изменить свое состояние и могут образоваться петли.

Сообщения об изменении топологии состоят лишь из четырех байтов. Они включают в себя поля идентификатора протокола (Protocol Identifier) и версии (Version) с нулевыми значениями, а также поле типа сообщения (Message-Type) со значением 128.

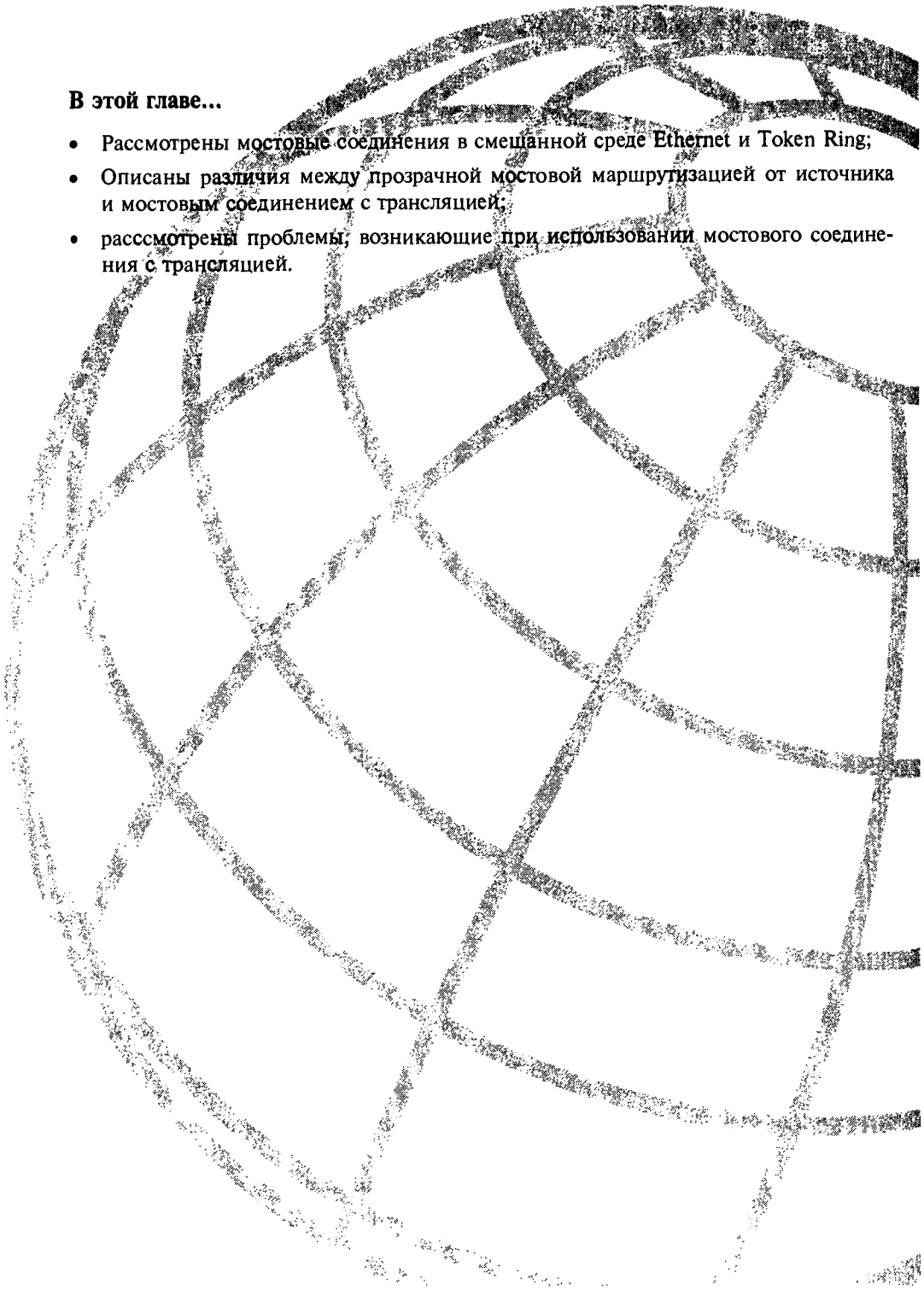
Контрольные вопросы

1. Какие три типа фреймов распространяет прозрачный мост методом лавинной маршрутизации?
2. Как мост узнает относительное расположение рабочей станции?
3. Какие два модуля PDU генерирует прозрачный мост и для чего они используются?

4. В чем состоит разница между пересылкой и лавинной маршрутизацией?
5. После того как топология связующего дерева определена, мосты делятся на две категории: корневые и назначенные мосты, а их порты настраиваются на различные режимы — корневых и назначенных портов. Если в сети есть 10 мостов и 11 сегментов, сколько из них будет принадлежать широковещательному домену?

Дополнительные источники

- Clark, Kennedy, and Kevin Hamilton, *CCIE Professional Development: Cisco LAN Switching*, Indianapolis: Cisco Press, 1999. (*Принципы коммутации в локальных сетях Cisco.* ИД "Вильямс", 2003.)
- Perlman R. *Interconnections*, Second Edition: *Bridges, Routers, Switches, and Internetworking Protocols.* Boston: Addison Wesley, 1999.



В этой главе...

- Рассмотрены мостовые соединения в смешанной среде Ethernet и Token Ring;
- Описаны различия между прозрачной мостовой маршрутизацией от источника и мостовым соединением с трансляцией;
- рассмотрены проблемы, возникающие при использовании мостового соединения с трансляцией.

Глава 28

Мостовое соединение разнородных сетей

Введение

Прозрачные мостовые соединения используются в основном в сетях Ethernet, а мостовая маршрутизация от источника (Source-Route Bridges — SRB) — главным образом в сетях Token Ring. И прозрачные мостовые соединения, и SRB широко распространены, поэтому возникает вопрос: существует ли способ непосредственного мостового соединения между такими сетями. Такие способы существуют и их несколько.

Мостовое соединение с трансляцией является относительно недорогим решением некоторых проблем из тех, которые вызываются мостовыми соединениями между доменами с прозрачными мостовыми соединениями и с SRB. Впервые мостовые соединения с трансляцией стали применяться в середине 80-х годов, но тогда они не получили поддержки ни одной организации по стандартизации. Вследствие этого многие аспекты таких соединений определяются разработчиком.

В 1990 г. компания IBM устранила некоторые слабые места мостового соединения с трансляцией, введя прозрачную мостовую маршрутизацию от источника (Source-Route Transparent — SRT). SRT-мосты могут передавать потоки данных от прозрачных и маршрутизируемых от источника конечных узлов и образовывать обычное разветвленное дерево с прозрачными мостами, тем самым позволяя однотипным конечным станциям обмениваться данными друг с другом в сети с произвольной топологией. Маршрутизация SRT описана в Приложении С стандарта IEEE 802.1d.

В конечном счете целью соединения доменов с прозрачными мостами и с SRB является обеспечение связи между конечными станциями доменов обоих типов. В настоящей главе описываются технические проблемы, решаемые алгоритмическим путем: мостовое соединение с трансляцией и мостовое SRT-соединение.

Проблемы трансляции

Перечисленные ниже проблемы связаны с обеспечением связи между конечными станциями принадлежащими доменам Ethernet и доменам с прозрачным мостовым соединением и конечными станциями из доменов SRB/Token Ring.

- **Несовместимый порядок битов.** Несмотря на то, что и Ethernet, и Token Ring поддерживают 48-разрядные MAC-адреса, внутреннее аппаратное представление этих адресов различно. Первый бит последовательного битового потока, представляющего адрес, Token Ring рассматривает как старший бит в байте, а Ethernet — как младший бит. Формат Ethernet называют каноническим, а Token Ring — неканоническим. Для преобразования между каноническим и неканоническим форматами трансляционный мост изменяет порядок битов в каждом байте адреса на обратный. Например, адрес Ethernet 0C-00-01-38-73-0B транслируется в адрес Token Ring 30-00-80-1C-CE-D0.
- **Встроенные MAC-адреса.** Иногда MAC-адреса передаются в области данных фрейма. Например, протокол протокол преобразования адресов (Address Resolution Protocol — ARP), распространенный в сетях TCP/IP, размещает аппаратные адреса в области данных фрейма канального уровня. Преобразование адресов, расположенных в области данных, требуется только в определенных случаях, поэтому это довольно сложная операция. Протокол IPX также встраивает адреса 2-го уровня в область данных некоторых фреймов. Трансляционные мосты должны изменять порядок битов также и в таких встроенных адресах. Многие протоколы реагируют на MAC-адреса, встроенные в протокол, а не в заголовки 2-го уровня. Поэтому трансляционный мост должен изменять порядок и в этих байтах, иначе устройства не будут реагировать на корректные MAC-адреса.
- **Несовместимые размеры максимальных модулей передачи** (Maximum Transfer Unit — MTU). В сетях Token Ring и Ethernet максимальные размеры фреймов различны. В Ethernet размер модуля MTU составляет около 1500 байтов; в то время как фреймы Token Ring могут быть намного больше. Поскольку мосты не позволяют фрагментировать и компоновать фреймы, пакеты, длина которых превышает MTU данной сети, должны отбрасываться.
- **Обработка битов состояния фреймов.** Фреймы Token Ring содержат три бита состояния: A, C и E. Назначение этих битов заключается в том, чтобы сообщить источнику фрейма, был ли данный фрейм получен получателем (бит A), скопирован (бит C) или в фрейме при приеме были обнаружены ошибки (бит E). Поскольку Ethernet не поддерживает эти биты, перед производителями мостов Ethernet-Token Ring стоит проблема их обработки.
- **Обработка особых функций Token Ring.** Некоторые биты Token Ring не имеют логических соответствий в Ethernet. Например, в Ethernet нет механизма приоритетности, который присутствует в Token Ring, а также битов маркировки, мониторинга и резервирования. При преобразовании во фрейм Ethernet эти биты фрейма Token Ring должны отбрасываться.
- **Обработка фреймов анализатора.** Прозрачные мосты не обрабатывают фреймы SRB-анализатора. Они узнают о топологии сети путем анализа адреса источника входящих фреймов и не поддерживают процесс определения маршрута SRB.
- **Обработка поля маршрута (Routing Information Field — RIF) в фрейме Token Ring.** SRB-алгоритм размещает информацию о маршрутизации в поле RIF. В алгоритме прозрачного мостового соединения нет эквивалента полю RIF и в нем вообще не используется принцип размещения информации о маршрутизации в фрейме.

- **Несовместимые алгоритмы ветвления.** Как прозрачное мостовое соединение, так и SRB во избежание петель используют алгоритмы связующего дерева деревьев. Однако эти алгоритмы несовместимы.
- **Обработка фреймов без информации о маршруте.** В SRB ожидается, что все фреймы локальной сети содержат информацию о маршруте. Фреймы без поля RIF (включая конфигурацию прозрачного мостового соединения и сообщения об изменении топологии, а также MAC-фреймы, отправленные из домена с прозрачными мостовыми соединениями), поступающий на SRB-мост, игнорируются.

Мостовое соединение с трансляцией

Поскольку способ обмена данными между двумя типами сетей так и не был стандартизирован, ни одно мостовое соединение с трансляцией нельзя назвать корректным. В этом разделе описываются несколько распространенных вариантов мостового соединения с трансляцией.

Трансляционные мосты при преобразовании форматов фрейма Ethernet и Token Ring переупорядочивают биты адресов источника и получателя. Проблема встроенных MAC-адресов решается путем программной проверки мостом различных типов MAC-адресов, однако это решение приходится адаптировать к каждому новому типу встроенных MAC-адресов. Некоторые мостовые соединения с трансляцией просто сверяются с наиболее распространенными встроенными адресами. Если программное обеспечение мостового соединения с трансляцией работает в мультипротокольном маршрутизаторе, то такое устройство может успешно маршрутизировать эти протоколы без каких-либо проблем.

В поле RIF есть подполе, где указывается максимальный размер фрейма, который может быть принят конкретной реализацией SRB. Трансляционные мосты, передающие фреймы из домена, где используются мостовые соединения с трансляцией, в SRB-домен, обычно записывают в поле MTU значение 1500 байтов. Это делается для ограничения размера фреймов Token Ring, передаваемых в домен мостовых соединений с трансляцией. Некоторые узлы не могут корректно обработать это поле. В таких случаях трансляционные мосты вынуждены отбрасывать фреймы, превосходящие MTU Ethernet.

Биты, соответствующие функциям Token Ring и не имеющие аналогов в Ethernet, чаще всего отбрасываются трансляционными мостами. Например, отбрасываются биты приоритетности, резервации и мониторинга Token Ring, содержащиеся в байте управления доступом. Биты состояния фрейма Token Ring, которые содержатся в байте, следующим за признаком конца поля данных, обрабатываются по-разному, в зависимости от производителя моста. Некоторые производители мостов просто игнорируют эти биты. Мосты других производителей устанавливают C-бит (указывающий, что фрейм был скопирован), но не A-бит (указывающий, что получатель распознал адрес). В первом случае узел источника Token Ring определяет, не был ли потерян отправленный им фрейм. Сторонники этого подхода считают, что механизмы повышения надежности, такие как контроль потерянных фреймов, лучше реализовать на 4-м уровне модели OSI. Сторонники установки C-бита считают, что такой бит должен быть установлен, чтобы следить за потерянными фреймами, а A-бит устанавливать не следует, поскольку мост не является получателем.

Трансляционные мосты могут создать программный шлюз между двумя доменами. Для конечных SRB-станций у трансляционного моста есть номер кольца и связанный с ним номер моста, поэтому он выглядит как стандартное SRB-устройство. В этом случае номер кольца на самом деле отражает весь домен мостовых соединений с трансляцией. Для домена прозрачных соединений трансляционный мост является прозрачным мостом.

При передаче данных из SRB-домена в домен прозрачных соединений SRB-информация удаляется. RIF-поля обычно кэшируются для использования обратным потоком данных. При передаче данных из домена прозрачных соединений в SRB-домен трансляционный мост может проверить фрейм на наличие одиночного адреса получателя. Если адрес получателя фрейма групповой или широковещательный, то он направляется в SRB-домен как анализатор связующего дерева. Если адрес получателя фрейма одиночный, то трансляционный мост ищет получателя в RIF-кэше. В случае нахождения пути он используется, а RIF-информация добавляется к фрейму; в противном случае фрейм отправляется как анализатор связующего дерева.

На рис. 28.1 показана смешанная сеть с трансляционным мостом, соединяющим сегменты Token Ring и Ethernet. Одноадресатная передача данных со станции 1 в сегменте Token Ring на станцию 2 в сегменте Ethernet проходит через два моста. Станция 1 генерирует фрейм с полем RIF, где содержится маршрут: Кольцо 1 — Мост 1 — Кольцо 2 — Мост 2 — Кольцо 3. Следует обратить внимание на то, что Кольцо 3 является сегментом Ethernet. На Станции 1 неизвестно, что Станция 2 принадлежит сегменту Ethernet. Отвечая Станции 1, Станция 2 генерирует фрейм без RIF-поля. Трансляционный мост, Мост 2, обнаруживает MAC-адрес получателя (Станция 1) и вставляет во фрейм RIF-поле, после чего отправляет его в направлении Станции 1.

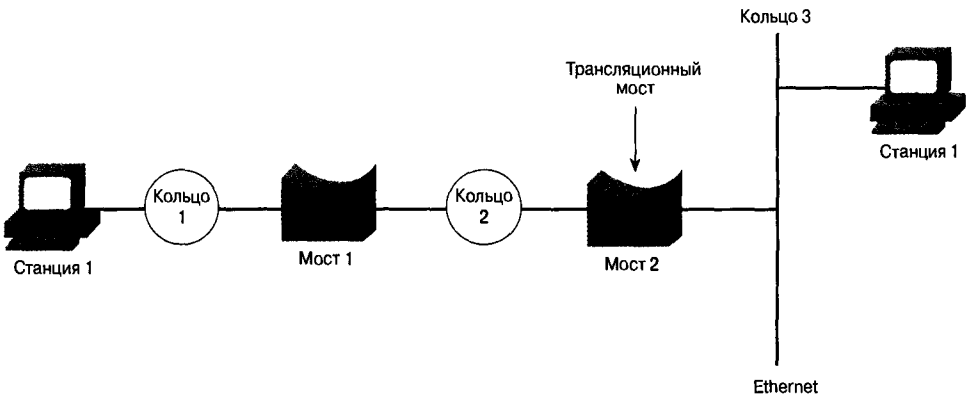


Рис. 28.1. Пример одноадресатной передачи данных между станциями в сегментах Token Ring и Ethernet

Поскольку реализации связующих деревьев в сегментах несовместимы, множественные маршруты между SRB-доменами и доменами прозрачных мостовых соединений обычно не допускаются. На рис. 28.2–28.4 представлены варианты преобразований фрейма мостовым соединением с трансляцией.

На рис. 28.2 показана схема преобразования фрейма при передаче между сетями IEEE 802.3 и Token Ring. Адреса получателя и источника (Destination And

Source Addresses — DASA), точки доступа к службе (Service-Access Point — SAP), информация управления логическим каналом (Logical Link Control — LLC) и данные заносятся в соответствующие поля фрейма получателя. Изменяется порядок битов в адресах получателя и источника. При передаче данных от IEEE 802.3 к Token Ring удаляется поле длины фрейма IEEE 802.3. При передаче данных от Token Ring к IEEE 802.3 удаляются байт управления доступом и поле RIF. Поле RIF может быть кэшировано в трансляционном мосту для использования обратным трафиком.

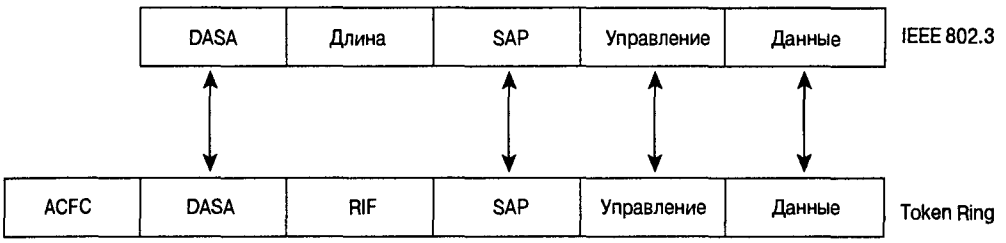


Рис. 28.2. При передаче данных между IEEE 802.3 и Token Ring без изменений остаются четыре поля

На рис. 28.3 показана схема преобразования фрейма при передаче между сетями Ethernet II и Token Ring с помощью протокола доступа к подсети (Subnetwork Access Protocol — SNAP). SNAP добавляет к полю данных фрейма Token Ring коды производителя и типа. Адреса получателя и источника, информация о типе и данные передаются соответствующим полям фрейма получателя, а биты DASA повторно упорядочиваются. При передаче данных по протоколу SNAP от Token Ring к Ethernet II удаляются поля RIF, SAP, LLC и код производителя. Данные RIF могут быть кэшированы в трансляционном мосту для использования обратным потоком данных. При передаче данных от Ethernet II к Token Ring SNAP-информация не удаляется.

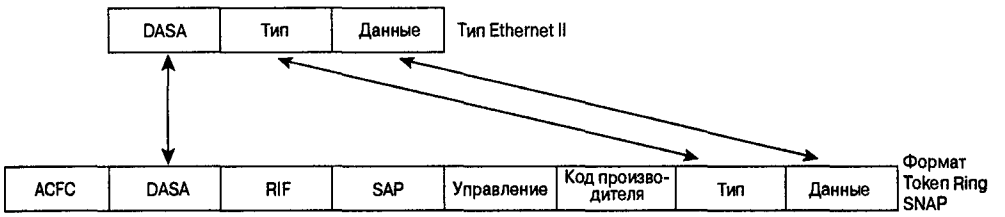


Рис. 28.3. При передаче данных по протоколу SNAP между Ethernet II и Token Ring без изменений остаются три поля

На рис. 28.4 показана схема преобразования фрейма из формата 0x80D5 Ethernet II в формат Token Ring. (Во фреймах Ethernet II 0x80D5 содержатся данные IBM SNA.) Информация DASA, SAP, LLC и данные передаются соответствующим полям фрейма получателя, а биты адресов получателя и источника повторно упорядочиваются. При передаче данных от Ethernet II 0x80D5 к Token Ring удаляются поля типа и заголовка 80D5. При передаче данных от Token Ring к Ethernet II 0x80D5 удаляется поле RIF. Информация RIF может быть кэширована в трансляционном мосту для использования обратным потоком данных.

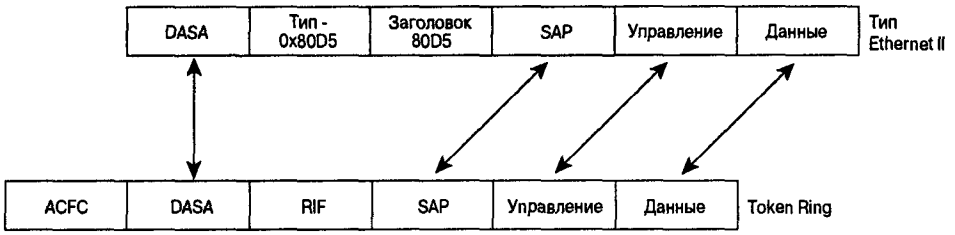


Рис. 28.4. При передаче данных между Ethernet II формата 0x80D5 и Token Ring без изменений остаются четыре поля

Прозрачная мостовая маршрутизация от источника

SRT-мосты объединяют системы с прозрачными мостовыми соединениями и системы с SRB-алгоритмами. В SRT-мостах для различения SRB-фреймов и фреймов прозрачного мостового соединения используется бит индикатора маршрутной информации (Routing Information Indicator — RII). Если бит RII равен 1, то во фрейме есть RIF-поле и мост использует SRB-алгоритм. Если бит RII равен 0, то во фрейме нет RIF-поля и мост использует прозрачное мостовое соединение.

Как и в случае трансляционных мостов, SRT-мосты не являются идеальным решением проблемы соединения разнородных сетей, так как сохраняется описанная ранее несовместимость Ethernet/Token Ring. Скорее всего, для мостового SRT-соединения потребуется усовершенствование оборудования до SRB, чтобы оно выдерживало возросшую нагрузку, возникающую за счет анализа каждого пакета. Может понадобиться и модернизация программного обеспечения до уровня SRB. Более того, в средах со смешанными SRT-мостами, прозрачными мостами и SRB выбранные маршруты от источника должны проходить по всем доступным SRT- и SRB-мостам. Такие маршруты потенциально могут в значительной степени зависеть от связующих деревьев, созданных прозрачными мостами. Наконец, смешанные сети с мостовыми SRB/SRT-соединениями теряют преимущества SRT-соединений, поэтому пользователи вынуждены обходить мостовые SRT-соединения, что влечет за собой значительные затраты. Тем не менее, мостовое SRT-соединение допускает сосуществование двух несовместимых сред и делает возможной связь между конечными узлами в SRB-доменах и доменах с прозрачными мостовыми соединениями.

Контрольные вопросы

1. При соединении между собой различных передающих сред, таких как Ethernet и Token Ring, возникают различные проблемы, для решения которых используются мостовые соединения с трансляцией. Перечислите и опишите четыре метода решения вышеупомянутых проблем.
2. Одна из проблем мостового соединения с трансляцией состоит в необходимости переупорядочивать биты каждого фрейма, передаваемого между сегментами Ethernet и Token Ring. Если станция Ethernet передает данные станции Token

Ring с MAC-адресом 00-00-0C-11-22-33 (канонический формат), то как будет выглядеть MAC-адрес Token Ring (неканонический формат)?

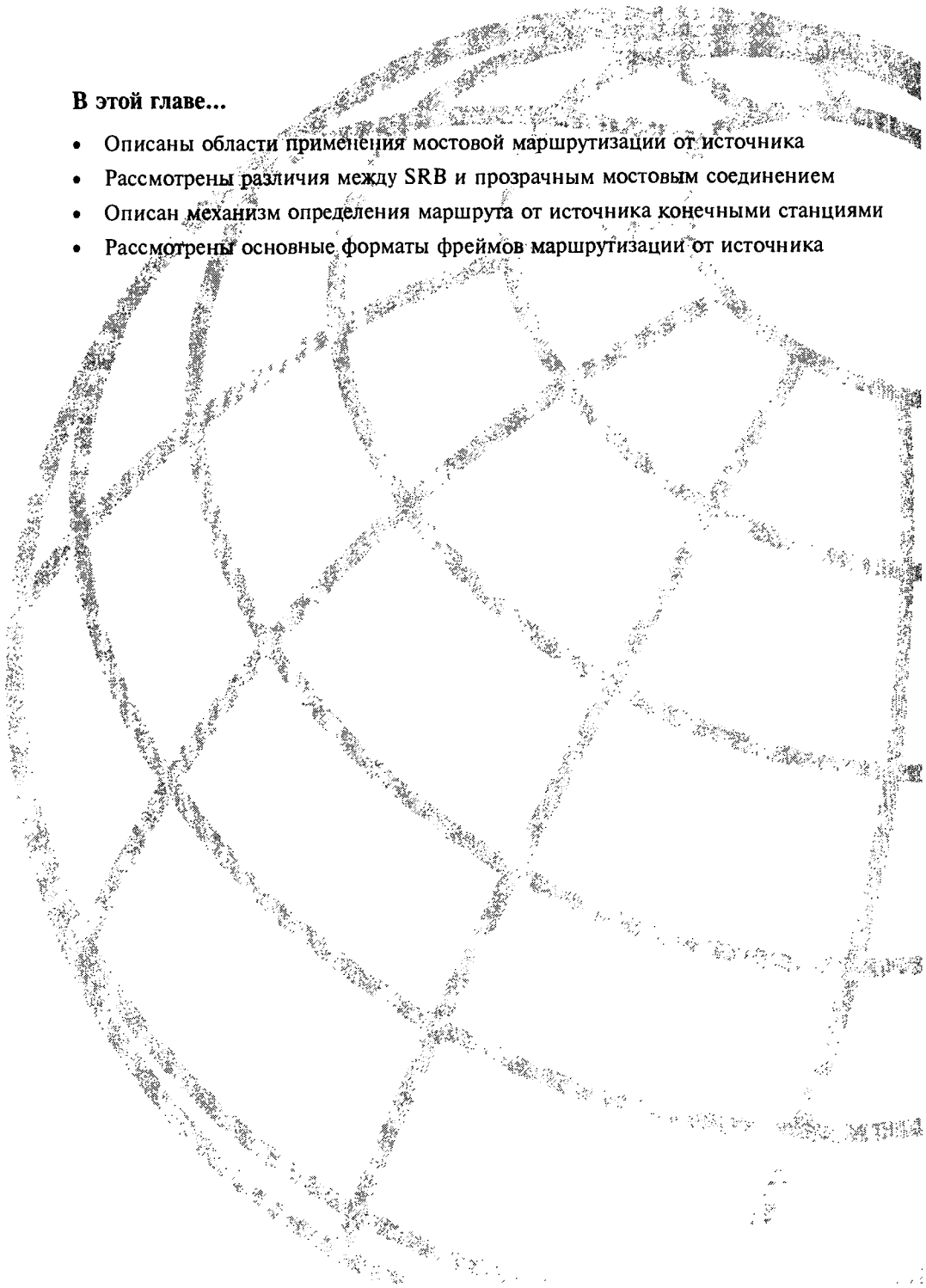
3. Может ли трансляционный мост работать с любыми сетями и протоколами Ethernet и Token Ring?
4. В чем состоит отличие между мостовой маршрутизацией от источника и прозрачной мостовой маршрутизацией от источника?

Дополнительные источники

- Kennedy C. and Hamilton K. *CCIE Professional Development: Cisco LAN Switching.* Cisco Press, 1999. (*Принципы коммутации в локальных сетях Cisco.* ИД "Вильямс", 2003.)
- Perlman R. *Interconnections, Second Edition: Bridges, Routers, Switches, and Internetworking Protocols.* Addison Wesley, 1999.

В этой главе...

- Описаны области применения мостовой маршрутизации от источника
- Рассмотрены различия между SRB и прозрачным мостовым соединением
- Описан механизм определения маршрута от источника конечными станциями
- Рассмотрены основные форматы фреймов маршрутизации от источника



Глава 29

Мостовая маршрутизация от источника

Введение

Алгоритм мостовой маршрутизации от источника (Source-Route Bridging — SRB) был разработан компанией IBM и предложен на рассмотрение комитета IEEE 802.5 как способ мостового соединения между локальными сетями. Затем IBM предложила комитету IEEE 802 новый стандарт мостового соединения — прозрачный мост с маршрутизацией от источника (Source-Route Transparent — SRT). Мост SRT не требует "чистых" SRB, оставляя два типа мостов локальных сетей: прозрачные мосты и мосты SRT. Хотя мостовые соединения SRT (см. главу 28 "Мостовое соединение разнородных сетей") получили распространение, соединения SRB также по-прежнему широко используются. В настоящей главе описывается основной SRB-алгоритм передачи фреймов и поля фреймов SRB.

SRB-алгоритм

Мосты SRB получили свое название по той причине, что их функционирование основано на предположении, что во всех фреймах, передаваемых от источника между локальными сетями, размещается полный маршрут от источника к получателю. SRB-мосты хранят и пересылают фреймы согласно маршруту, находящемуся в соответствующем поле фрейма. Пример SRB-сети показан на рис. 29.1.

Предположим, что узлу X на рис. 29.1 требуется послать фрейм узлу Y. Вначале узлу X неизвестно, принадлежит ли узел Y той же локальной сети, что и узел X. Для решения этого вопроса узел X посылает тестовый фрейм. Если этот фрейм возвращается узлу X без подтверждения о том, что узел Y его получил, то узел X считает, что узел Y принадлежит удаленному сегменту.

Для того чтобы определить точное местоположение узла Y, узел X посылает фрейм-анализатор. Каждый мост, получающий этот фрейм (мосты 1 и 2), копирует фрейм во все выходные порты. По мере прохода по сетям во фреймы-анализаторы заносится информация о маршруте. Когда фреймы-анализаторы узла X достигают узла Y, узел Y отвечает на каждый из них, используя собранную информацию о маршруте. После полу-

чения всех ответных фреймов узел X выбирает маршрут, исходя из заранее определенных критериев.

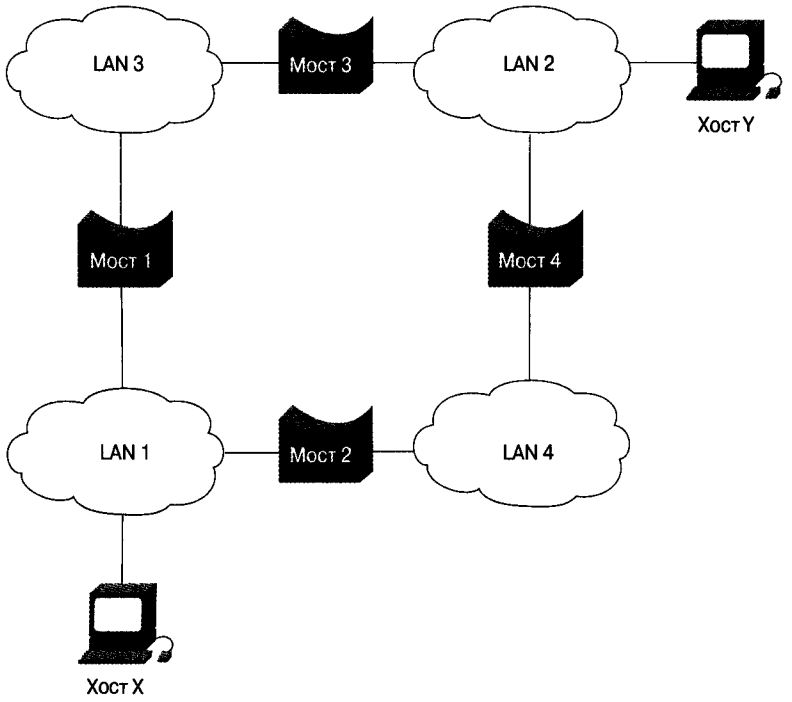


Рис. 29.1. SRB-сеть, содержащая локальные сети и мосты

В примере на рис. 29.1 образуются два маршрута:

- локальная сеть 1 — мост 1 — локальная сеть 3 — мост 3 — локальная сеть 2;
- локальная сеть 1 — мост 2 — локальная сеть 4 — мост 4 — локальная сеть 2.

Узел X должен выбрать один из этих двух маршрутов. В спецификации IEEE 802.5 не указано, какой критерий он должен при этом использовать, но есть несколько рекомендаций, в том числе следующие:

- первый полученный фрейм;
- ответ с наименьшим количеством узлов;
- ответ с наибольшим допустимым размером фрейма;
- различные комбинации предыдущих критериев.

Обычно выбирается маршрут, содержащийся в первом пришедшем фрейме.

Выбранный маршрут вставляется в *поле маршрутной информации* (Routing Information Field — RIF) фреймов, предназначенных для узла Y. Поле RIF включается только в те фреймы, которые предназначены для других локальных сетей. О том, что в фрейме присутствует информация о маршруте, свидетельствует старший бит поля адреса источника, называемый *индикатором маршрутной информации* (Routing Information Indicator — RII).

Формат фрейма

Структура поля RIF спецификации IEEE 802.5 показана на рис. 29.2.

Поле RIF, изображенное на рис. 29.2, состоит из двух частей: области управления маршрутом и области маршрута. Более подробно они будут рассмотрены далее.

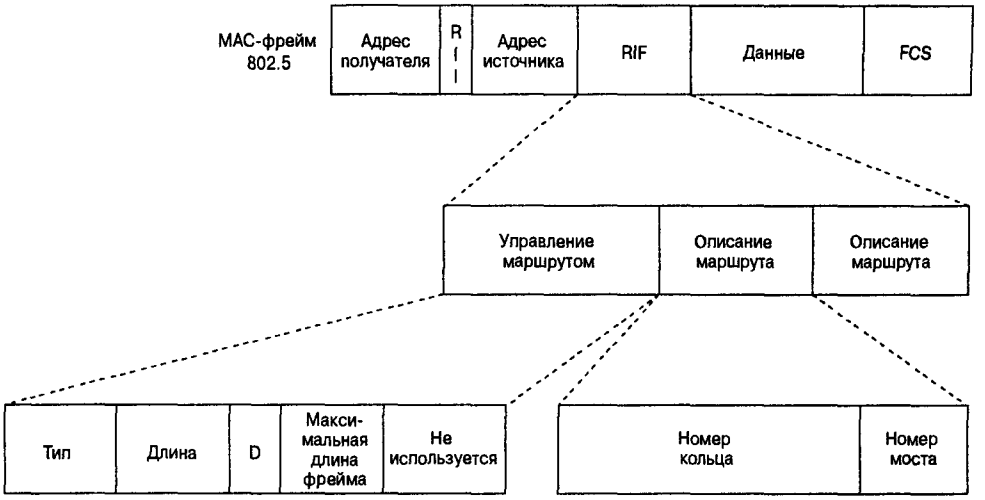


Рис. 29.2. Поле RIF IEEE 802.5 присутствует во фреймах, предназначенных для других локальных сетей

Поле управления маршрутом

Поле управления маршрутом состоит из четырех подполей: поля типа, длины, D-бита и поля максимального размера фрейма. Эти поля описаны ниже.

- **Тип.** Существуют следующие три типа управления маршрутом:
  - — **Специальный маршрут.** Узел источника предоставляет маршрут в заголовке RIF. Мосты передают фрейм согласно информации в поле маршрута.
  - — **Анализатор всех маршрутов.** Используется для обнаружения удаленного узла. Маршрут формируется по мере прохождения пакета по сети. Мосты добавляют к фрейму свои номера и номера колец, в которые передается фрейм. (Первый мост добавляет номер первого кольца.) Получатель получит столько фреймов, сколько к нему ведет маршрутов.
  - — **Анализатор связующего дерева.** Используется для обнаружения удаленного узла. Фрейм передается только мостами связующего дерева, которые при передаче добавляют в них свои номера и номера присоединенных колец. При использовании этого метода в процессе анализа передается меньше фреймов.
- **Длина.** Общая длина поля RIF в байтах — от 2 до 30 байтов.
- **D-бит.** Направление передачи фрейма — прямое или обратное. D-бит влияет на порядок прочтения мостом комбинаций номера кольца и номера моста в указателе маршрута — справа налево (в прямом направлении) или слева направо (в обратном).

- **Максимальная длина фрейма.** Наибольший размер фрейма, который может быть обработан на указанном маршруте. Начальный наибольший размер фрейма устанавливает источник, но мосты могут уменьшить его, если не могут обработать фрейм такого размера.

Поле описания маршрута

Каждое поле описания маршрута состоит из описанных ниже двух подполей.

- **Номер кольца** (12 битов). Значение, которое в сети с мостами должно быть уникальным.
- **Номер моста** (4 бита). Значение после номера кольца. Этот номер не обязательно должен быть уникальным, кроме случая, когда имеется два или более моста, соединяющих одни и те же два кольца.

Мост добавляет к фрейму свой номер и номер кольца, на которое пересылается фрейм. (Первый мост также добавляет номер первого кольца.)

Маршрут представляет собой последовательность номеров колец и мостов, причем первый и последний номера принадлежат кольцам. Одно поле RIF может содержать несколько полей описания маршрута. Согласно спецификации IEEE, максимальное количество полей описания маршрута равно 14 (до 13 мостов или узлов, поскольку номер последнего моста всегда равен нулю).

До недавних пор согласно спецификации IBM максимальное количество полей описания маршрута равнялось 8 (максимум семь мостов или узлов), и большинство производителей мостов придерживались этой спецификации IBM. Новое программное обеспечение мостов IBM и новые сетевые адаптеры позволяют составлять маршруты из 13 узлов.

Контрольные вопросы

1. В чем заключается основное различие в процессе передачи между прозрачными мостами и мостами с маршрутизацией от источника?
2. В стандартах SRB не определен способ, с помощью которого источник выбирает маршрут к получателю из нескольких вариантов. В настоящей главе перечислены четыре метода принятия такого решения и сказано, что чаще всего выбирается маршрут первого полученного фрейма. Какие предположения о сети может сделать источник при использовании этого метода?
3. Каким образом станции и мосты узнают, существует ли определенный во фрейме маршрут от источника?
4. Какие проблемы возможны в большой SRB-сети с несколькими альтернативными маршрутами?
5. Для номера моста отводится всего 4 бита. Означает ли это, что мостов может быть не более 16 (2^4=16)? Обоснуйте свой ответ.
6. Можно ли подключить к центральному кольцу несколько мостов с одинаковым номером?
7. Для номера кольца отводится 12 битов. Может ли сеть состоять из более чем 4096 колец (2^{12}=4096)? Обоснуйте свой ответ.

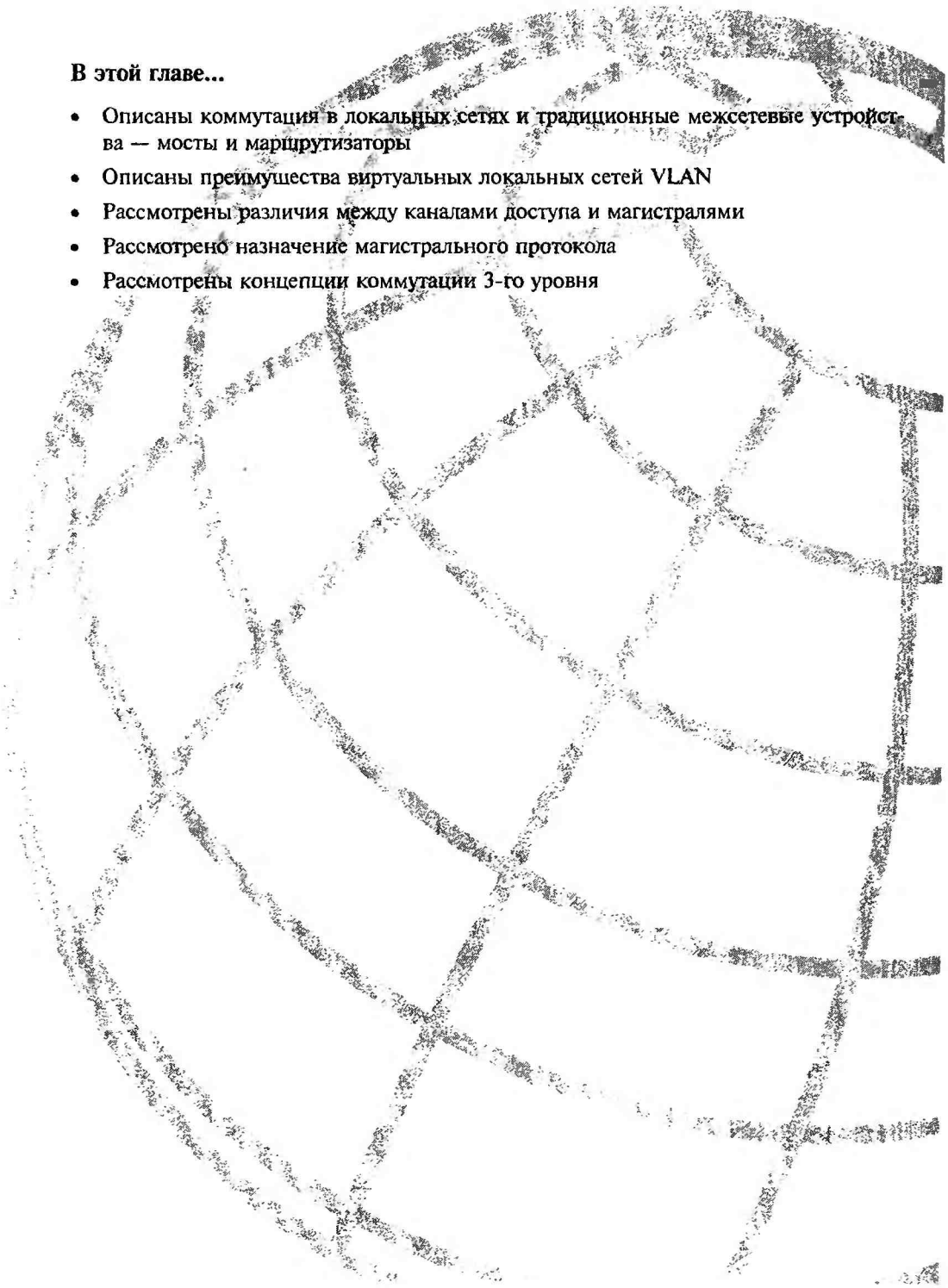
Дополнительные источники

- Computer Technology Research Corporation. *The IBM Token Ring Network.* New York: Prentice Hall, 1990.
- IEEE. "IEEE Standard for Local Area Networks: Token ring Physical Layer Specifications". June 1989.

  В настоящее время разрабатывается стандарт высокоскоростной сети Token Ring. Хотя он не связан непосредственно с маршрутизацией от источника, желающие узнать о нем более подробно могут сделать это по адресу http://www.hstra.com/.

В этой главе...

- Описаны коммутация в локальных сетях и традиционные межсетевые устройства — мосты и маршрутизаторы
- Описаны преимущества виртуальных локальных сетей VLAN
- Рассмотрены различия между каналами доступа и магистралями
- Рассмотрено назначение магистрального протокола
- Рассмотрены концепции коммутации 3-го уровня



Глава 30

Коммутируемые локальные сети и сети VLAN

Коммутатор локальной сети представляет собой устройство, обеспечивающее более высокую плотность портов по сравнению с традиционными мостами при меньших затратах. Коммутаторы локальных сетей позволяют создавать сети с меньшим количеством пользователей в сегменте, увеличивая таким образом среднюю доступную пропускную способность для каждого пользователя. В настоящей главе описывается работа коммутаторов локальных сетей и проводится сравнение коммутируемых локальных сетей с эталонной моделью OSI.

Сокращение количества пользователей в сегменте называется *микросегментацией*. Микросегментация позволяет создавать частные или выделенные сегменты, в которых на каждый сегмент приходится по одному пользователю. В этом случае каждый пользователь получает доступ сразу ко всей полосе пропускания и ему не приходится конкурировать с другими пользователями. Исключаются коллизии (нормальное явление в сетях с общим доступом к среде передачи, использующих концентраторы), в случае, если оборудование работает в дуплексном режиме. Коммутатор локальной сети передает фреймы на основе адреса фрейма 2-го уровня (коммутатор локальной сети 2-го уровня) или, в некоторых случаях, на основе адреса фрейма 3-го уровня (многоуровневый коммутатор локальной сети). Коммутатор локальной сети также называют коммутатором фреймов, так как он передает фреймы 2-го уровня, в то время как ATM-коммутатор передает ячейки.

На рис. 30.1 показан коммутатор локальной сети, предоставляющий устройствам выделенную полосу пропускания, а также соответствие коммутации 2-го уровня в локальной сети канальному уровню OSI.

История коммутаторов

Первые коммутаторы локальных сетей появились в 1990 году. Это были устройства 2-го уровня (мосты), предназначенные для решения проблем пропускной способности для настольных PC. Последние модели коммутаторов локальных сетей представляют собой многоуровневые устройства, способные обрабатывать протоколы приложений, требующих большой полосы пропускания — то, что раньше делали маршрутизаторы. Современные коммутаторы локальных сетей заменяют концентраторы, поскольку пользовательские приложения требуют большей пропускной способности.

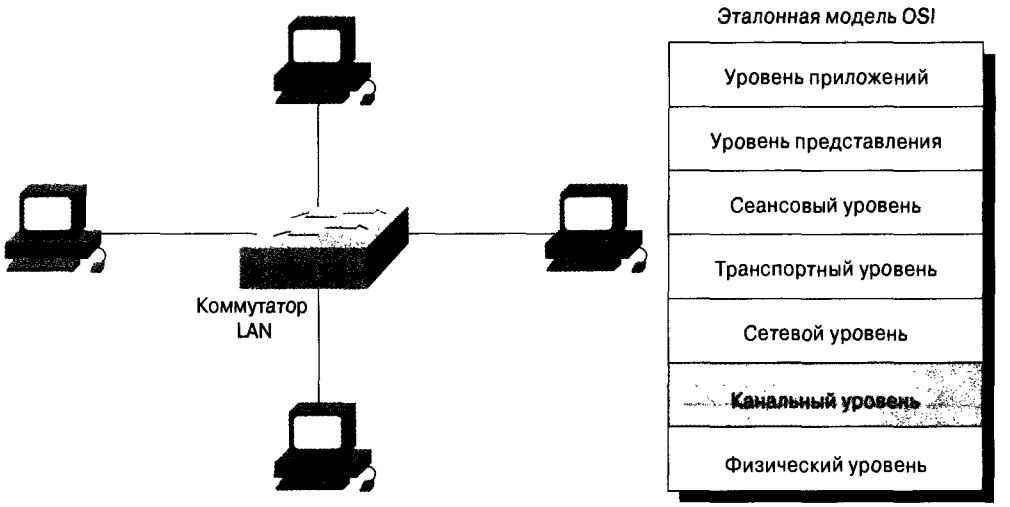


Рис. 30.1. Коммутатор локальной сети является устройством канального уровня

Функционирование коммутатора LAN

Коммутаторы локальных сетей подобны прозрачным мостам — они тоже анализируют топологию, выполняют фильтрацию и передачу. Эти коммутаторы также поддерживают несколько новых, уникальных функций, таких как выделенная коммуникация между устройствами в дуплексном режиме, несколько параллельных обменов данными и адаптация к скорости среды передачи.

В дуплексном режиме обмена данными между сетевыми устройствами повышается количество передаваемой информации. Несколько параллельных обменов данными возможны благодаря одновременной передаче, или коммутации, нескольких пакетов, что повышает пропускную способность сети. Дуплексный обмен данными фактически удваивает пропускную способность, а благодаря адаптации к скорости среды передачи коммутатор локальной сети может передавать данные со скоростью от 10 до 100 Мбит/с, распределяя полосу пропускания по мере необходимости.

Внедрение коммутаторов в локальные сети не требует изменения существующих концентраторов, сетевых адаптеров или кабелей.

Сети VLAN

Виртуальная локальная сеть (virtual LAN — VLAN) представляет собой *широковещательный домен* коммутируемой сети. Широковещательные домены определяют степень распространения по сети широковещательного фрейма, сгенерированного станцией. Некоторые коммутаторы можно настроить на поддержку одиночных сетей VLAN и их групп. Если коммутатор поддерживает несколько сетей VLAN, то широковещательная рассылка внутри одной VLAN никогда не распространяется в другую VLAN-сеть. Порты коммутатора, настроенные на одну VLAN-сеть, принадлежащую нескольким широковещательным доменам, эквивалентны портам коммутатора, принадлежащим нескольким VLAN.

VLAN-сеть позволяет администраторам строить широковещательные домены с меньшим количеством пользователей в каждом из доменов. Это увеличивает полосу пропускания, доступную для пользователей, поскольку конкурировать за нее приходится меньшему количеству пользователей.

Маршрутизаторы также обеспечивают изоляцию широковещательных доменов путем блокирования широковещательных фреймов. Поэтому потоки данных могут проходить от одной VLAN-сети к другой только через маршрутизатор.

Обычно различные подсети принадлежат к разным VLAN-сетям. Поэтому сеть, состоящая из нескольких подсетей, как правило, содержит несколько VLAN. Использование коммутаторов и VLAN-сетей позволяют сетевому администратору распределять пользователей по широковещательным доменам в зависимости от потребностей пользователей. Это предоставляет администратору дополнительную гибкость при размещении рабочих станций.

Сети VLAN обладают следующими преимуществами:

- сегментация широковещательных доменов для увеличения полосы пропускания;
- дополнительная безопасность за счет изоляции пользователей с помощью мостов;
- гибкость внедрения, основанная на рабочих функциях, а не на физическом расположении.

Режимы портов коммутаторов

Порты коммутатора работают либо в режиме доступа, либо в магистральном режиме. В режиме доступа интерфейс полностью принадлежит одной сети VLAN. Обычно порт коммутатора в режиме доступа подключается к устройству конечного пользователя или к серверу. Фреймы, передаваемые в режиме доступа, выглядят как обычные фреймы Ethernet.

В отличие от режима доступа, при использовании магистрали потоки нескольких VLAN мультиплексируются для передачи по одному физическому каналу. Магистральные каналы обычно соединяют между собой коммутаторы (рис. 30.2). Однако они могут подключаться и к конечным устройствам, таким как серверы со специальными сетевыми адаптерами, участвующими в протоколе мультиплексирования.

Следует обратить внимание на то, что некоторые устройства подключены к своим коммутаторам через каналы доступа, а для соединения между коммутаторами используются магистральные каналы.

Для того чтобы мультиплексировать потоки данных от различных VLAN-сетей, существуют специальные протоколы, которые инкапсулируют фреймы или снабжают их тегами, для того, чтобы принимающему устройству было известно, какой сети VLAN принадлежит данный фрейм. Магистральные протоколы являются либо фирменными разработками, либо основаны на стандарте IEEE 802.1Q. Например, протокол Cisco Inter-Switch Link (ISL) является частным магистральным протоколом, позволяющим устройствам Cisco мультиплексировать данные VLAN-сетей специальным способом, оптимизированным для сетевых компонентов Cisco. Можно также воспользоваться открытым протоколом, таким как 802.1Q, который позволяет оборудованию нескольких производителей мультиплексировать данные VLAN-сетей в магистральном канале.

Без магистральных каналов для поддержки нескольких VLAN между коммутаторами пришлось бы устанавливать несколько каналов доступа. Такая система не очень

экономична и ее трудно масштабировать. Поэтому в большинстве случае для соединения коммутаторов между собой предпочтительнее использовать магистрали.

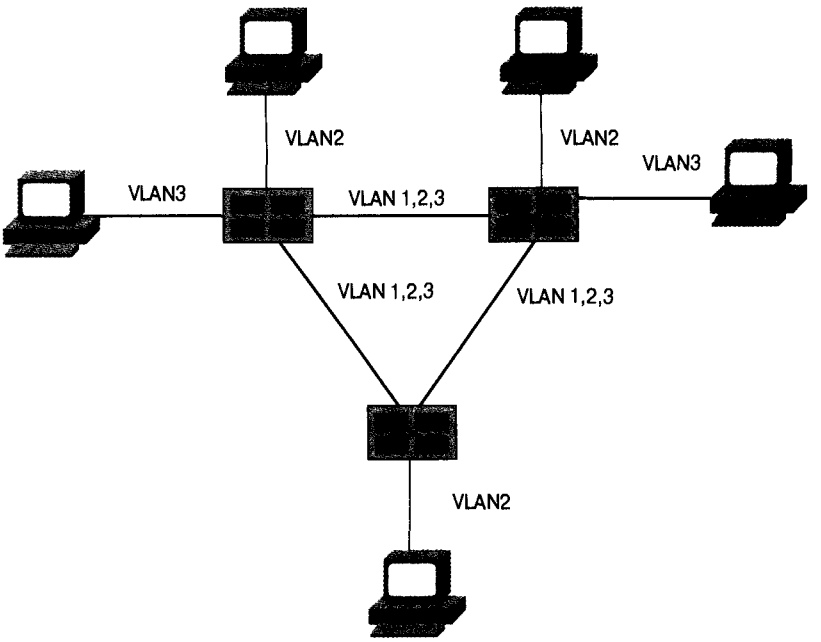


Рис. 30.2. Коммутаторы, объединенные магистральными каналами

Передача данных в коммутируемой локальной сети

Коммутаторы локальных сетей можно классифицировать по методам передачи. При коммутации с промежуточным хранением (store-and-forward) выполняется проверка ошибок и удаление фреймов с ошибками. При использовании сквозной коммутации или коммутации без буферизации пакетов (cut-through) проверка на наличие ошибок не выполняется, что сокращает задержку.

При коммутации с промежуточным хранением коммутатор локальной сети копирует весь фрейм во встроенные буферы и производит проверку контрольной суммы (CRC). Фрейм отбрасывается, если в CRC будет обнаружена ошибка, или если он является *"карликом" (runt)* (менее 64 байтов, включая CRC) либо *"гигантом" (giant)* (более 1518 байтов, включая CRC). Если фрейм не содержит ошибок, то коммутатор локальной сети находит адрес получателя в своей таблице пересылки (коммутации) и определяет исходящий интерфейс. После этого фрейм пересылается в пункт назначения.

При коммутации без буферизации пакетов коммутатор локальной сети копирует во внутренние буферы только адрес получателя (первые 6 байтов после префикса). Затем он находит адрес получателя в своей таблице коммутации, определяет выходной интерфейс и пересылает фрейм получателю. При коммутации без буферизации пакетов задержки меньше, так как передача фрейма начинается сразу после прочтения адреса получателя и определения выходного интерфейса.

Некоторые коммутаторы можно настроить на коммутацию пакетов без буферизации по конкретным портам. Такой метод коммутации используется до тех пор,

пока не будет достигнуто предельное значение ошибки, определяемое пользователем. Если этот порог достигается, то порт автоматически переходит в режим коммутации с промежуточным хранением. Если количество ошибок падает ниже этого порога, то порт автоматически выполняет обратное переключение в режим коммутации с промежуточным хранением.

Для поддержки многоуровневой коммутации в коммутаторах локальных сетей необходимо использовать методику с промежуточным хранением, поскольку коммутатор должен получить весь фрейм до того, как он начнет выполнять какие-либо операции на уровне протокола. Соответственно, более сложные коммутаторы, осуществляющие коммутацию 3-го уровня, относятся к устройствам с промежуточным хранением.

Пропускная способность коммутируемой локальной сети

Коммутаторы локальных сетей можно классифицировать и по относительной полосе пропускания, выделяемой каждому порту. Симметричная коммутация обеспечивает равномерное распределение полосы пропускания, а асимметричная предоставляет неодинаковую полосу пропускания для разных портов.

Асимметричный коммутатор локальной сети обеспечивает коммутируемые соединения между портами с неодинаковой полосой пропускания, например 10BaseT и 100BaseT. Этот тип коммутации еще называют *коммутацией 10/100.* Асимметричная коммутация предназначена для потоков данных приложений "клиент/сервер", в которых несколько клиентов одновременно связываются с сервером. Сервер требует большей полосы пропускания, иначе этот порт станет "узким местом" в сети.

Симметричный коммутатор обеспечивает соединение между портами с одинаковой полосой пропускания — либо 10BaseT, либо 100BaseT. Симметричная коммутация предназначена для более или менее равномерного распределения потоков данных, которое обычно имеет место в одноранговой сети.

Выбирая между симметричной и асимметричной коммутацией, менеджер сети должен оценить требуемую величину полосы пропускания для соединений между устройствами, с тем, чтобы оптимизировать потоки данных сетевых приложений.

Коммутируемые локальные сети и эталонная модель OSI

Коммутаторы локальных сетей можно классифицировать в соответствии с уровнями OSI, на которых они фильтруют и коммутируют фреймы. Это могут быть коммутаторы 2-го уровня, 2-го уровня с некоторыми свойствами 3-го уровня или многоуровневые коммутаторы.

Коммутаторы локальной сети 2-го уровня подобны многопортовым мостам, но они гораздо мощнее и поддерживают много новых функций, таких, в частности, как дуплексный режим. Коммутаторы локальной сети 2-го уровня выполняют коммутацию и фильтрацию на основании MAC-адресов канального уровня OSI (2-го уровня). Как и мосты, они абсолютно прозрачны для сетевых протоколов и пользовательских приложений.

Коммутаторы локальной сети 2-го уровня с функциями 3-го уровня принимают решения о коммутации на основании большего объема информации, чем просто MAC-адрес.

Такие коммутаторы обладают некоторыми функциями управления потоками данных на 3-м уровне, такими как управление широковещательной и многоадресатной рассылкой, обеспечение безопасности благодаря спискам доступа и IP-фрагментации.

Многоуровневые коммутаторы осуществляют коммутацию и фильтрацию на основании адресов канального (2-го) и сетевого (3-го) уровней OSI. Такие коммутаторы динамически решают, коммутировать (2-й уровень) или маршрутизировать (3-й уровень) поступающие потоки данных. Многоуровневые коммутаторы локальных сетей выполняют коммутацию в пределах рабочей группы и маршрутизацию между рабочими группами.

Коммутация на 3-м уровне позволяет потокам данных обходить маршрутизаторы. Первый фрейм проходит через маршрутизатор обычным образом, чтобы убедиться в соблюдении всех политик защиты. Коммутаторы следят за способом обработки маршрутизатором фрейма и затем воспроизводят этот процесс для остальных фреймов. Рассмотрим следующий пример. Предположим, что нужно передать несколько FTP-фреймов от источника 10.0.0.1 к получателю 192.168.1.1. Обычно такие фреймы проходят через маршрутизатор. Многоуровневый коммутатор наблюдает за тем, как маршрутизатор изменяет заголовки 2-го и 3-го уровней первого фрейма и имитирует действия маршрутизатора для остальных фреймов. Это уменьшает нагрузку на маршрутизатор и величину задержки в сети.

Контрольные вопросы

1. Многоуровневый коммутатор повторяет действия маршрутизатора после того, как маршрутизатор обработает первый фрейм. Что делает многоуровневый коммутатор с заголовками 2-го и 3-го уровней для того, чтобы точно выполнить имитацию работы маршрутизатора?
2. На какой тип межсетевых устройств больше всего похож коммутатор локальной сети?
3. В настоящей главе были описаны два магистральных протокола. В каких случаях применяется протокол IEEE 802.1Q?
4. Какой метод коммутации защищает полосу пропускания сетевых сегментов от фреймов с ошибками?
5. Каким образом коммутатор с промежуточным хранением определяет, что фрейм содержит ошибку?
6. Пересекают ли маршрутизаторы границы VLAN?
7. Чем отличается магистральный канал от канала доступа?
8. До появления коммутаторов и VLAN-сетей администраторы назначали пользователям сетевые ресурсы, исходя не из потребностей пользователей, а из других соображений. Из каких именно?

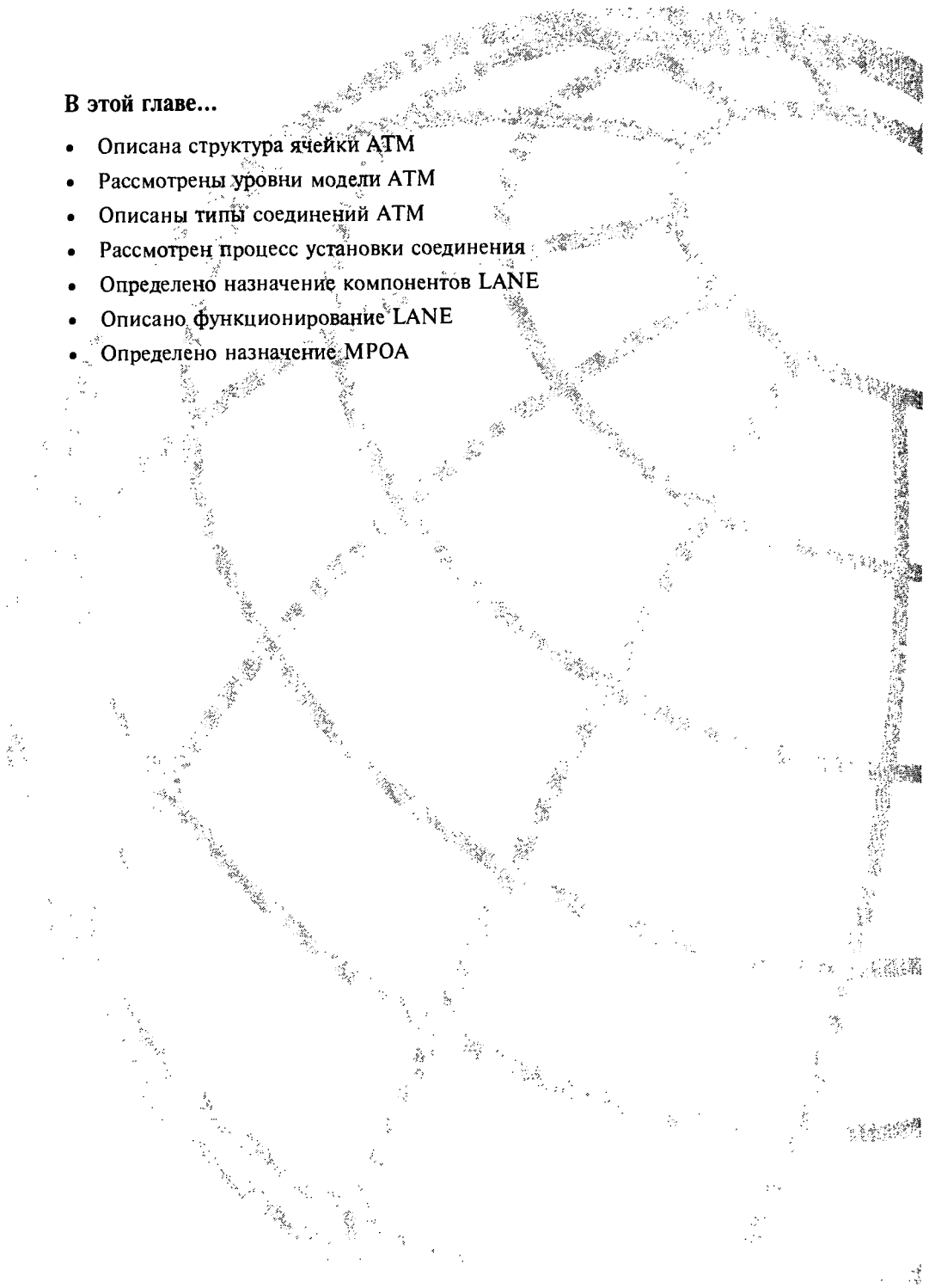
Дополнительные источники

- R. Breyer, Sean R. *Switched and Fast Ethernet.* Ziff-Davis Press, 1997.
- Kennedy C., Hamilton K. *CCIE Professional Development: Cisco LAN Switching.* Cisco Press, 1999. (*Принципы коммутации в локальных сетях Cisco.* ИД "Вильямс", 2003.)

- Mathias H., Griffiths D. *Switching Technology in the Local Network.* International Thomson Publishing, 1997.
- Perlman R. *Interconnections, Second Edition: Bridges, Routers, Switches, and Internetworking Protocols.* Addison Wesley, 1999.

В этой главе...

- Описана структура ячейки ATM
- Рассмотрены уровни модели ATM
- Описаны типы соединений ATM
- Рассмотрен процесс установки соединения
- Определено назначение компонентов LANE
- Описано функционирование LANE
- Определено назначение MPOA



Глава 31

Коммутация в режиме ATM

Асинхронный режим передачи (Asynchronous Transfer Mode — ATM) является стандартом ITU-T для поэлементной передачи, когда информация различного типа: речь, видео и т.д. передается в небольших ячейках фиксированной длины. Сети ATM представляют собой сети, ориентированные на соединение. В настоящей главе описываются протоколы, службы и функционирование ATM. На рис. 31.1 показана частная и общедоступная сети ATM, передающие речь, видео и данные.

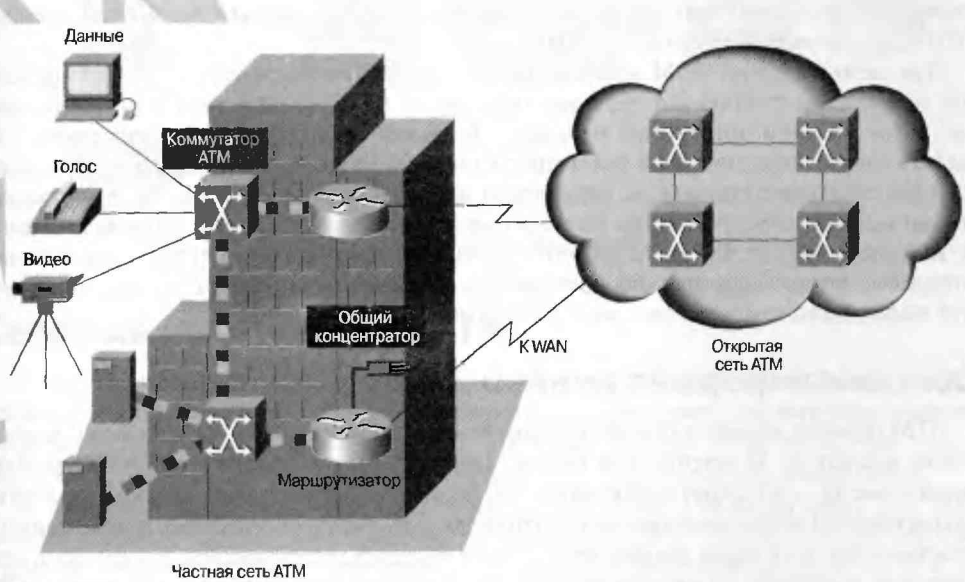


Рис. 31.1. Частная и открытая сети ATM передают речь, видео и данные

Стандарты

В основе ATM лежит стандарт широкополосной сети ISDN (Broadband ISDN — B-ISDN) Международного телекоммуникационного союза (ITU-T). Этот стандарт первоначально рассматривался как технология высокоскоростной передачи речи, видео и данных по сетям общего пользования. Форум ATM распространил его и на частные сети, разработав следующие спецификации:

- интерфейс "пользователь-сеть" (User-to-Network Interface — UNI) 2.0;
- UNI 3.0;
- UNI 3.1;
- UNI 4.0;
- интерфейс открытых сетей (Public-Network Node Interface — P-NNI);
- эмуляция LAN (LAN Emulation — LANE);
- многопротокольная схема в ATM.

Устройства ATM и сетевая среда

ATM представляет собой технологию коммутации ячеек и мультиплексирования, в которой объединены преимущества коммутации каналов (гарантированная пропускная способность и постоянная задержка передачи сигнала) и коммутации пакетов (гибкость и эффективность для пульсирующего потока данных). ATM обеспечивает масштабирование полосы пропускания от нескольких мегабитов до многих гигабитов в секунду. Асинхронный режим передачи ATM оказывается эффективнее, чем синхронные технологии, такие как мультиплексирование с *временным разделением каналов TDM (Time-Division Multiplexing — TDM).*

При использовании TDM каждому пользователю отводится определенный временной интервал, в течение которого никакая другая станция не может отправлять данные. Если станции потребуется отправить большой объем данных, то она может это сделать только тогда, когда ей будет предоставлен достаточный отрезок времени, даже если все остальные станции не используют для передачи свое время. Если у станции нет данных для передачи, когда подходит ее очередь, то временной интервал полезно не используется. Так как ATM является асинхронным режимом передачи, временные интервалы предоставляются по требованию с идентификацией источника передачи (эта информация содержится в заголовке ячейки ATM).

Основной формат ячейки ATM

ATM передает данные в пакетах фиксированной длины, называемых *ячейками.* Каждая ячейка состоит из 53 октетов, или байтов. Первые 5 байтов содержат заголовок ячейки, а остальные 48 — полезную информацию (информацию пользователя). Небольшие ячейки фиксированной длины особенно хорошо подходят для передачи голосовых и видеоданных, поскольку для этих типов данных недопустима задержка, возникающая, в частности, при ожидании окончания передачи большого пакета данных. Основной формат ячейки ATM показан на рис. 31.2.

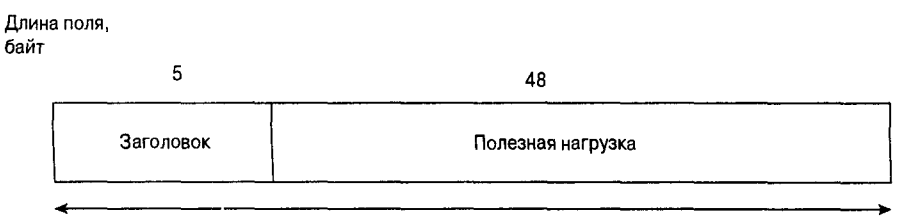


Рис. 31.2. Ячейка ATM

Устройства ATM

Сеть ATM состоит из *коммутатора* и *конечных точек*. Коммутатор отвечает за передачу ячеек по сети ATM. Перед ATM-коммутатором ставятся строго определенные задачи: принять входящую ячейку от конечной точки или другого ATM-коммутатора, прочесть и обновить заголовок, а также быстро переслать ячейку через выходной интерфейс в пункт назначения. Конечная точка (или конечная система) ATM имеет адаптер сетевого интерфейса ATM. Конечными точками ATM являются рабочие станции, маршрутизаторы, устройства DSU, коммутаторы LAN и видеокодеки. На рис. 31.3 показана сеть ATM, состоящая из ATM-коммутаторов и конечных точек.

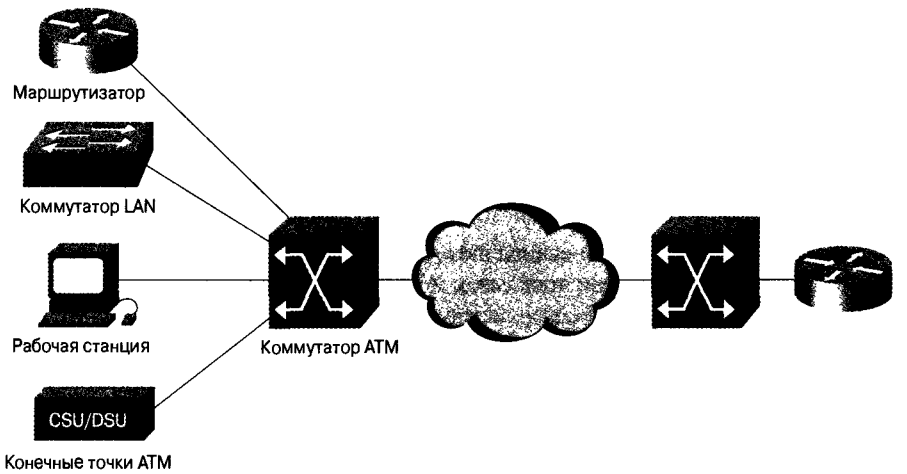


Рис. 31.3. Сеть ATM состоит из коммутаторов и конечных точек

Сетевые интерфейсы ATM

Сеть ATM состоит из ATM-коммутаторов, объединенных ATM-соединениями или интерфейсами типа "точка-точка". ATM-коммутаторы поддерживают два основных типа интерфейсов: UNI и NNI. Первый соединяет конечные системы ATM (такие, как узлы и маршрутизаторы) с ATM-коммутатором, а второй — ATM-коммутаторы между собой.

В зависимости от того, кому принадлежит коммутатор (частному лицу или телефонной компании), и кто им управляет, интерфейсы UNI и NNI делятся на общедоступные и частные. Частный интерфейс UNI соединяет конечную станцию ATM с частным ATM-коммутатором. Его общедоступным аналог соединяет конечную станцию или частный коммутатор с другим общедоступным коммутатором. Частный интерфейс NNI соединяет два ATM-коммутатора в пределах одной частной организации. Общедоступный NNI соединяет два ATM-коммутатора в открытой сети.

Соединение двух общедоступных коммутаторов разных провайдеров описывается дополнительной спецификацией широкополосного интерфейса между носителями (Broadband InterCarrier Interface — B-ICI). На рис. 31.4 показаны спецификации интерфейсов ATM для частных и открытых сетей.

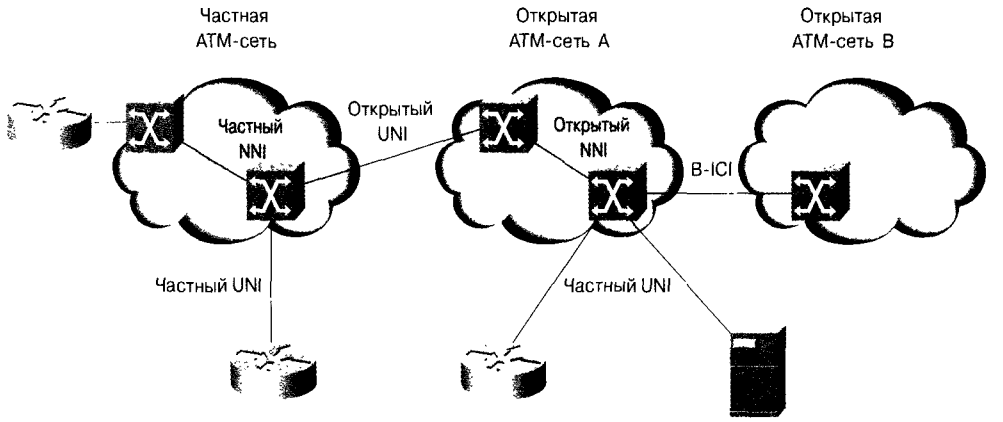


Рис. 31.4. Спецификации интерфейсов ATM для частных и открытых сетей

Формат заголовка ячейки ATM

Существует два формата заголовка ячейки ATM: UNI и NNI. Заголовок UNI используется для связи между конечными точками и ATM-коммутаторами в частных сетях ATM. Заголовок NNI используется для связи между ATM-коммутаторами. На рис. 31.5 показан основной формат ячейки ATM и форматы заголовков UNI и NNI.

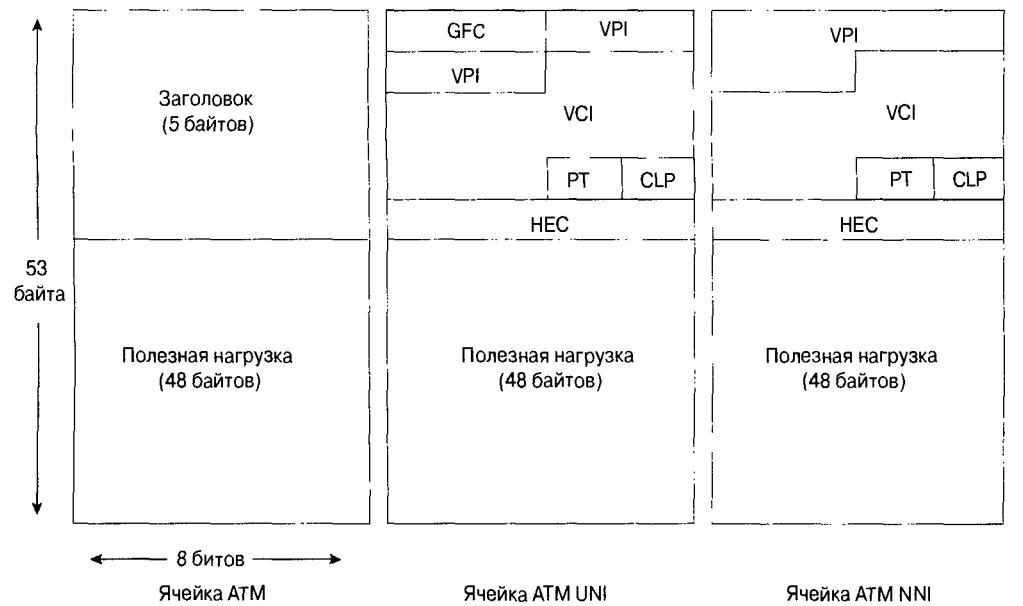


Рис. 31.5. Ячейка ATM, заголовок UNI ATM и заголовок ячейки NNI ATM содержат по 48 байтов полезной нагрузки

В отличие от UNI, заголовок NNI не содержит поля общего управления потоком (Generic Flow Control — GFC). Однако этот заголовок NNI содержит поле идентификатора виртуального маршрута (Virtual Path Identifier — VPI), которое занимает первые

12 битов, что позволяет использовать более длинные каналы связи между открытыми АТМ-коммутаторами.

Поля заголовка ячейки ATM

Кроме GFC и VPI, в заголовках ячейки АТМ имеется ряд других полей (см. рис. 31.5), описанных ниже.

- **GFC Общее управление потоком (Generic Flow Control).** Обеспечивает выполнение локальных функций, таких как определение нескольких станций, использующих общий интерфейс АТМ. Это поле, как правило, не используется и по умолчанию его значение равно 0 (двоичный код 0000).
- **VPI Идентификатор виртуального маршрута (Virtual Path Identifier).** Вместе с VCI определяет следующий промежуточный получатель ячейки по мере ее прохождения через несколько АТМ-коммутаторов на пути к конечному получателю.
- **VCI Идентификатор виртуального канала (Virtual Channel Identifier).** Вместе с VPI определяет следующего промежуточного получателя ячейки по мере ее прохождения через несколько АТМ-коммутаторов на пути к конечному получателю.
- **PT Тип полезной нагрузки (Payload Type).** Первый бит определяет, какой тип данных содержится в ячейке (пользовательские или управляющие). Если ячейка содержит пользовательские данные, то этот бит равен 0, если управляющие, то его значение равно 1. Второй бит указывает на перегрузку канала (0 — нет перегрузки, 1 — перегрузка), а третий показывает, является ли данная ячейка последней в последовательности ячеек, представляющих один фрейм AAL5 (если он равен 1, то это последняя ячейка фрейма).
- **CLP Приоритет ячейки при отбрасывании (Cell Loss Priority).** Показывает, следует ли отбрасывать ячейку, если она попадет в перегруженный канал. Если значение бита CLP равно 1, то ячейка должна быть удалена прежде, чем ячейки с битом CLP, равным 0.
- **HEC Контроль ошибок заголовка (Header Error Control).** Вычисляет контрольную сумму только по первым четырем байтам заголовка. При использовании контроля HEC можно исправить одну ошибку бита в этих байтах, таким образом сохраняя ячейку, а не удаляя ее.

Службы ATM

Существует три типа служб АТМ: постоянные виртуальные каналы, коммутируемые виртуальные каналы и служба без подтверждения соединения (аналогичная SMDS).

Постоянный виртуальный канал (Permanent Virtual Circuit — PVC) осуществляет прямое соединение между узлами, подобно выделенной линии. Преимущества канала PVC заключаются в том, что он гарантирует доступность соединения и не требует установки соединения между коммутаторами. Недостатками PVC являются статическое соединение и необходимость настройки вручную. Каждое устройство, находящееся между источником и получателем, должно быть настроено для PVC вручную. Кроме того, при использовании PVC уменьшается гибкость сети.

Коммутируемый виртуальный канал (Switched Virtual Circuit — SVC) создается и удаляется динамически и используется только до тех пор, пока передаются данные,

как при телефонном соединении. Динамический контроль вызова требует обмена управляющими сигналами между конечной точкой и ATM-коммутатором. Преимущества канала SVC заключаются в гибкости соединения и установки связи, которая может осуществляться автоматически сетевым устройством. Среди недостатков следует отметить то, что для установки соединения требуется больше времени и дополнительные управляющие сигналы.

Виртуальные соединения ATM

Сети ATM ориентированы на соединение. Это означает, что каждой передаче данных в сети ATM предшествует установка виртуального канала (Virtual Channel — VC).

Существует два типа соединений ATM: *виртуальные маршруты*, определяемые идентификаторами виртуального маршрута (Virtual Path Identifier — VPI) и *виртуальные каналы*, определяемые комбинацией VPI и идентификатора виртуального канала (Virtual Channel Identifier — VCI).

Виртуальный маршрут представляет собой ряд смежных виртуальных каналов, прозрачно коммутируемых через сеть ATM на основе общего для всех них идентификатора VPI. Однако все VPI и VCI имеют только локальное значение в отдельно взятом канале и перераспределяются на каждом коммутаторе.

Маршрут передачи представляет собой физическую среду, в которой создаются виртуальные каналы и виртуальные маршруты. На рис. 31.6 показано, как виртуальные каналы объединяются в виртуальные маршруты, которые, в свою очередь, проходят по каналу передачи.

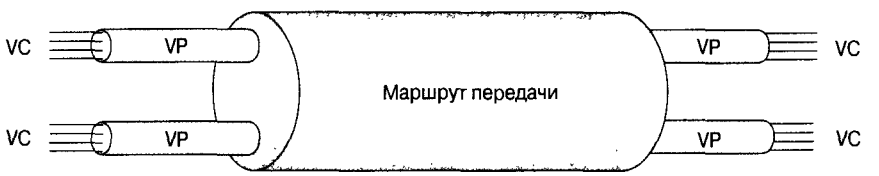


Рис. 31.6. Виртуальные каналы (VC) объединяются в виртуальные маршруты (VP)

ATM-коммутация

Основная задача ATM-коммутатора проста: ячейка, передаваемая по каналу, принимается при определенном значении поля VCI или VPI. По значению соединения в локальной таблице преобразований коммутатор определяет исходящий порт (или порты) соединения и новое значение полей VPI/VCI соединения этого канала. Затем коммутатор пересылает ячейку по исходящему каналу с соответствующими идентификаторами соединения. Так как все VCI и VPI имеют только локальное значение для данного канала, значения полей переопределяются на каждом коммутаторе.

Эталонная модель ATM

Для описания функциональных возможностей архитектуры ATM используется логическая модель. Функции ATM соответствуют физическому и частично канальному уровням эталонной модели OSI.

Эталонная модель ATM состоит из следующих плоскостей, охватывающих все уровни.

- **Контрольная плоскость.** Эта плоскость отвечает за генерирование и контроль сигнальных запросов.
- **Плоскость пользователя.** Данная плоскость отвечает за управление передачей данных.
- **Плоскость управления.** Эта плоскость состоит из описанных ниже двух компонентов.
  - **Управление уровнем.** Функции уровня, такие как обнаружение ошибок и разрешение проблем, связанных с протоколами.
  - **Управление плоскостью.** Функции, относящиеся ко всей системе.

Эталонная модель ATM состоит из приведенных ниже уровней.

- **Физический уровень.** Аналогичен физическому уровню эталонной модели OSI. Этот уровень ATM управляет передачей данных в физической среде.
- **Уровень ATM.** Вместе с адаптационным уровнем аналогичен канальному уровню эталонной модели OSI. Уровень ATM отвечает за одновременный совместный доступ к виртуальным каналам на физическом уровне (мультиплексирование ячеек) и передачу ячеек по сети ATM (ретрансляция ячеек). Для этого уровень ATM использует информацию VPI и VCI, содержащуюся в заголовке ячеек ATM.
- **Уровень адаптации ATM (ATM Adaptation Layer — AAL).** Определяет способ подготовки информации для передачи по сети ATM. Вместе с уровнем ATM AAL аналогичен канальному уровню модели OSI. Уровень AAL отвечает за отделение протоколов высшего уровня от особенностей процесса ATM. Адаптационный уровень подготавливает пользовательские данные для преобразования в ячейки и делит их на 48-байтовые блоки полезной нагрузки.

Наконец, на высших уровнях пользовательские данные принимаются, делятся на пакеты и передаются на уровень AAL. Эталонная модель ATM показана на рис. 31.7.

Физический уровень ATM

Физический уровень ATM выполняет четыре функции: преобразование ячеек в битовый поток, управление передачей и получением битов в физической среде, определение границ ячейки ATM и упаковка ячеек в соответствующие типы фреймов для передачи в физической среде. Например, для передачи в среде SONET и DS-3/E-3 ячейки преобразуются во фреймы разными способами.

Физический уровень ATM делится на две части: подуровень, зависящий от среды передачи данных (Physical Medium-Dependent — PMD), и подуровень сходимости передачи (Transmission Convergence — TC).

Подуровень PMD выполняет две основные функции. Во-первых, он синхронизирует передачу и прием путем отправки и получения постоянного битового потока с информацией о синхронизации. Во-вторых, он определяет физическую среду передачи, включая типы разъемов и кабеля: синхронная цифровая иерархия/синхронная оптическая сеть (Synchronous Digital Hierarchy/Synchronous Optical Network — SDH/SONET), DS-3/E-3, многомодовый оптоволоконный кабель

(MultiMode Fiber — MMF) со скоростью передачи 155 Мбит/с или экранированная витая пара (Shielded Twisted-Pair — STP) со схемой шифрования 8B/10B.

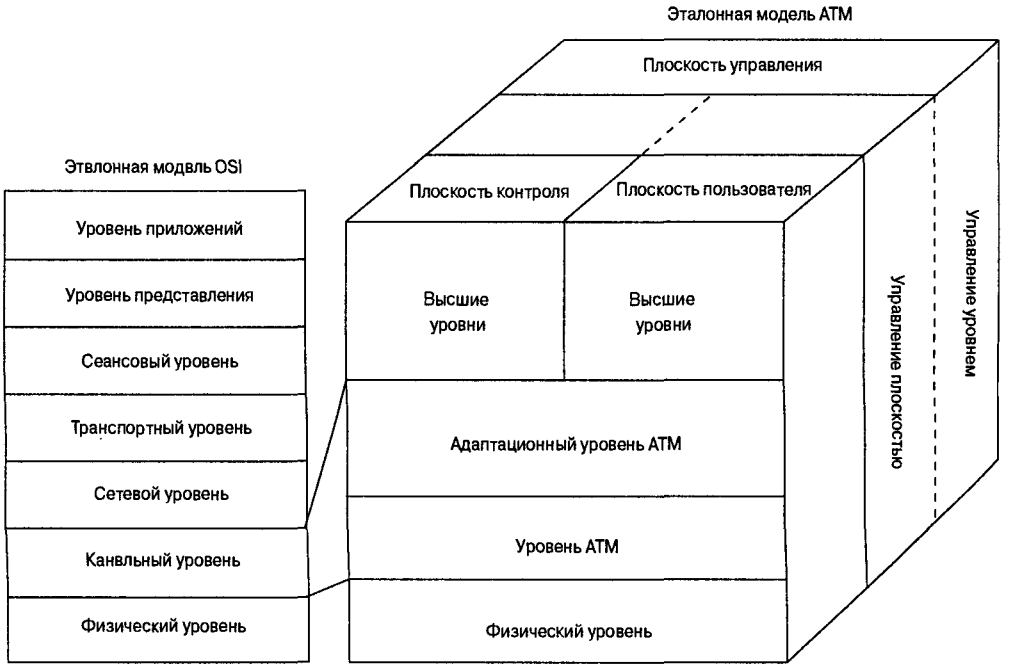


Рис. 31.7. Эталонная модель ATM соответствует двум нижним уровням эталонной модели OSI

Подуровень TC выполняет четыре функции: разграничение ячеек, генерирование и подтверждение последовательности контроля ошибок заголовка (Header Error Control — HEC), разделение ячеек по скорости передачи и адаптация фрейма передачи. Разграничение ячеек ATM позволяет устройствам выделять ячейки в битовом потоке. HEC генерирует и проверяет код контроля ошибок, подтверждающий корректность данных. Разделение ячеек по скорости передачи обеспечивает синхронизацию и добавляет или удаляет лишние (незанятые) ячейки ATM, для того, чтобы количество ячеек соответствовало пропускной способности системы передачи. Адаптация фрейма передачи пакетирует ATM-ячейки во фреймы, приемлемые для данной реализации физического уровня.

Адаптационные уровни ATM: AAL1

Уровень AAL1 представляет собой службу, ориентированную на соединение. Она удобна при работе с данными битовых потоков, передаваемых с постоянной битовой скоростью (Constant Bit Rate — CBR), такими как голосовые данные и видеоконференции. ATM передает потоки данных CBR, используя службы эмуляции каналов. Служба эмуляции каналов также обеспечивает подключение к магистрали ATM оборудования, которое до настоящего времени использовало выделенные линии. Уровень AAL1 требует синхронизации по времени между источником и получателем. Поэтому уровню AAL1 требуется среда передачи, поддерживающей синхронизацию, такой как SONET.

Подготовка ячейки к передаче осуществляется на уровне AAL1 в три этапа. Прежде всего в поле полезной нагрузки вставляются синхронные кванты данных (например, 1 байт данных за 125 мкс). Затем добавляются поля порядкового номера (Sequence Number — SN) и зашиты порядкового номера (Sequence Number Protection — SNP) с информацией, по которой получающий AAL1 определяет правильность последовательности получения ячеек. Наконец, остаток поля полезной нагрузки заполняется пустыми байтами, чтобы довести размер поля до 48 байтов. Процесс подготовки ячейки к передаче на уровне AAL1 показан на рис. 31.8.

Адаптационные уровни ATM: AAL2

Имеется еще один тип данных, который, как и данные CBR, требует синхронизации, но является пульсирующим по своей природе. Этот тип данных передается с переменной битовой скоростью (Variable Bit Rate — VBR). Обычно такой тип данных генерируется такими службами, как пакетированные речь или видео, которые не имеют постоянной скорости передачи данных, но предъявляют требования, подобные требованиям служб постоянной битовой скорости. Для потоков данных VBR удобен уровень AAL2. Процесс AAL2 использует поле полезной нагрузки ячейки длиной 44 байта и резервирует 4 байта для поддержки AAL2.

Потоки данных VBR делятся на два типа: данные реального времени (VBR-RT) и данные свободного времени (VBR-NRT). Уровень AAL2 поддерживает оба типа потоков данных VBR.

Уровни адаптации ATM: AAL3/4

Уровень AAL3/4 поддерживает передачу данных как с ориентацией на соединение, так и без подтверждения соединения. Он предназначен для провайдеров сетевых служб и тесно связан со скоростной технологией SMDS. AAL3/4 используется для передачи пакетов SMDS по сети ATM.

На уровнях AAL3/4 подготовка ячейки к передаче осуществляется в три этапа. Сначала подуровень сходимости (Convergence Sublayer — CS) создает модуль данных протокола (PDU) путем присоединения в начале или в конце фрейма заголовка-тега и добавления в конце поля длины. Затем подуровень сегментации и повторной сборки (Segmentation And Reassembly — SAR) фрагментирует модуль PDU, добавляет к каждому фрагменту PDU заголовок и трейлер CRC-10 для контроля ошибок. В конечном итоге готовый модуль SAR PDU становится информационным полем ячейки ATM, к которому уровень ATM присоединяет стандартный заголовок ATM.

Заголовок AAL3/4 SAR PDU состоит из полей типа, порядкового номера и идентификатора мультиплексирования. Поля типа определяют, является ли ячейка началом, продолжением или концом сообщения, поля порядкового номера определяют последовательность сборки ячеек, а поле идентификатора мультиплексирования определяет, какие ячейки из других источников попали в этот же виртуальный канал (VC), для того, чтобы собрать в источнике только нужные ячейки.

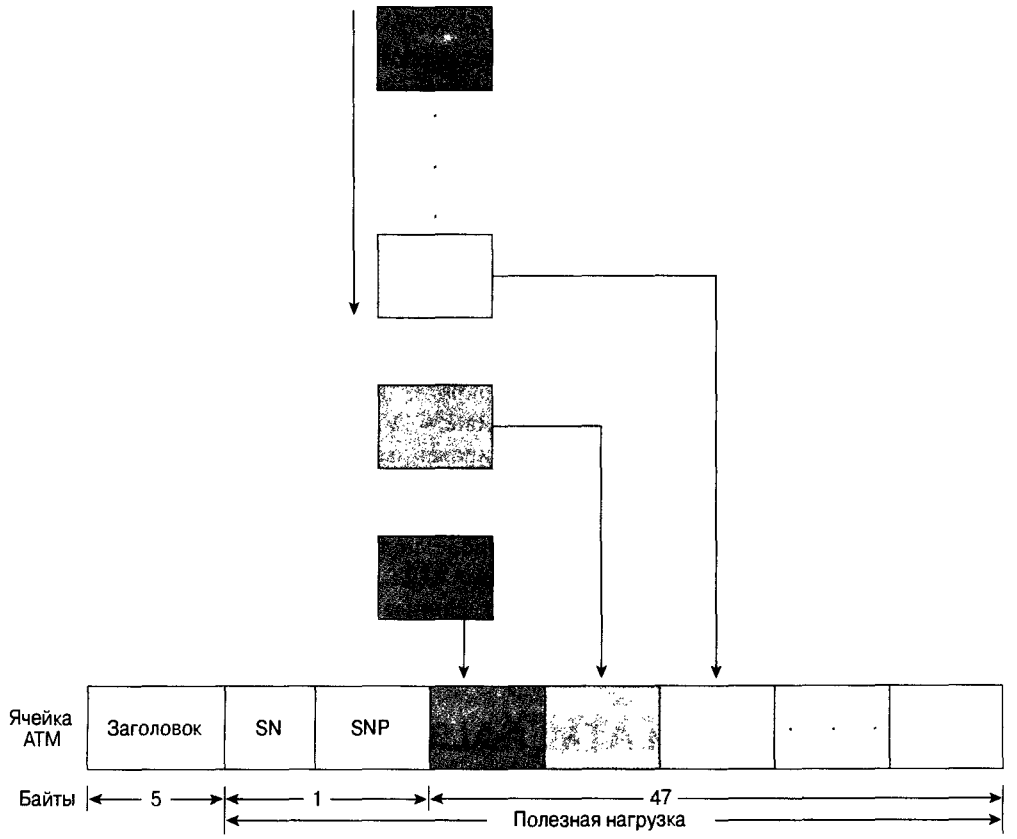


Рис. 31.8. AAL1 подготавливает ячейку к передаче таким образом, чтобы сохранить последовательность ячеек

Уровни адаптации ATM: AAL5

AAL5 является базовым уровнем ATM для данных и поддерживает передачу как с подтверждением соединения, так и без него. Чаще всего он используется для передачи данных, отличных от SMDS, таких как классическая схема IP в ATM и эмуляция LAN (LANE). AAL5 также является простым и эффективным уровнем адаптации, поскольку подуровень SAR просто принимает модуль CS-PDU и делит его на 48-октетные блоки SAR-PDU без резервирования байтов в каждой ячейке.

На уровне AAL5 подготовка ячейки к передаче осуществляется в три этапа. Сначала подуровень CS присоединяет к фрейму некоторое количество пустых байтов-заполнителей и 8-байтовый трейлер. Благодаря байтам-заполнителям образовавшийся модуль PDU всегда соответствует по размеру 48-байтовой ячейке ATM. Трейлер состоит из значения длины фрейма и 32-битового циклического избыточного кода (CRC), рассчитанного для всего модуля PDU. Это позволяет уровню AAL5 обнаруживать при приеме ошибки битов, потерянные ячейки и ячейки, не вошедшие в последовательность. Затем подуровень SAR делит CS-PDU на 48-байтовые блоки. В отличие от AAL3/4, заголовок и трейлер не добав-

ляются, так что сообщения могут чередоваться. В конечном итоге уровень ATM помещает каждый блок в поле полезной нагрузки ячейки ATM. Для всех ячеек, за исключением последней, бит в поле типа полезной нагрузки (Payload Type — PT) равен 0; это означает, что ячейка не является последней в группе, образующей один фрейм. Для последней ячейки бит в поле PT равен 1.

Адресация ATM

Для открытых сетей ATM стандарт ITU-T основан на использовании адресов типа E.164 (аналогичных телефонным номерам). Форум ATM расширил адресацию ATM, включив в нее частные сети. Она основана на подсетевой или оверлейной модели адресации, в которой уровень ATM отвечает за преобразование адресов сетевого уровня в адреса ATM. Эта подсетевая модель является альтернативой адресации протоколов сетевого уровня (таких, как IP и IPX) и существующих протоколов маршрутизации (таких, как IGRP и RIP). Форум ATM определил формат адреса, основанного на структуре адресов точки доступа к сетевой службе OSI (Network Service Access Point — NSAP).

Подсетевая модель адресации

Подсетевая модель адресации отделяет уровень ATM от любого из существующих протоколов высшего уровня, например IP или IPX. Поэтому она требует совершенно новой схемы адресации и нового протокола маршрутизации. Каждой ATM-системе должен быть назначен, кроме адреса протокола высшего уровня, ATM-адрес. Поэтому протокол преобразования адресов ATM (Address Resolution Protocol — ARP) должен преобразовать адреса протоколов высшего уровня в соответствующие адреса ATM.

Формат NSAP ATM-адресов

20-байтовые ATM-адреса формата NSAP предназначены для использования в частных сетях ATM. В открытых сетях применяются адреса E.164, формат которых определен ITU-T. Форум ATM определил для адресов E.164 кодировку NSAP, которая применяется в частных сетях для преобразования адресов E.164. Но эти адреса могут использоваться в некоторых частных сетях и без преобразования.

Такие частные сети могут создать собственную (формата NSAP) адресацию на адресах E.164 общедоступных интерфейсов UNI, к которым они подключены и у которых могут заимствовать префикс адреса, используя для идентификации локальных узлов младшие биты.

Все ATM-адреса формата NSAP состоят из трех компонентов: идентификатор полномочий и формата (Authority And Format Identifier — AFI), идентификатор исходного домена (Initial Domain Identifier — IDI) и адрес в пределах домена (Domain-Specific Part — DSP). AFI определяет тип и формат IDI, а та, в свою очередь, — способ выделения адреса и административные полномочия. Действительная маршрутная информация содержится в DSP.

Примечание

Подводя итог сказанному выше, можно сказать что первые 13 байтов *префикса* NSAP отвечают на вопрос "Какой коммутатор?". У каждого коммутатора должен быть уникальный префикс, идентифицирующий его. Устройства, подключенные к коммутатору, наследуют его префикс как часть своего адреса NSAP. Этот префикс используется коммутаторами для поддержки ATM-маршрутизации.

Следующие 6 байтов, называемые идентификатором конечной станции (End Station Identifier — *ESI*), определяют элемент сети ATM, подключенный к коммутатору. Каждое устройство, подключенное к коммутатору, должно иметь уникальный идентификатор ESI.

Последний байт, называемый байтом *селектора* (SEL), определяет процесс в устройстве, с которым осуществляется соединение.

Три формата адресации в частных сетях ATM различаются свойствами AFI и IDI. В кодированном NSAP-формате E.164 IDI является числом E.164. В формате DCC IDI представляет собой код страны-источника данных (Data Country Code — DCC), который определяет страну согласно ISO 3166. Такие адреса контролируются государственными отделениями ISO. В формате ICD IDI представляет собой международный код (International Code Designator — ICD), назначаемый регистрирующим органом ISO 6523. Коды ICD определяются соответствующими международными организациями.

Форум ATM рекомендует организациям и частным провайдерам сетевых услуг использовать для формирования собственной схемы нумерации формат DCC или ICD.

На рис. 31.9 показаны три формата адресов ATM, используемые для частных сетей.

Поля адреса ATM

Ниже описаны поля, показанные на рис. 31.9.

- **AFI.** Определяет тип и формат адреса (E.164, ICD или DCC).
- **DCC.** Определяет страну.
- **HO-DSP** Часть адреса, относящаяся к домену высшего порядка (High-Order Domain-Specific Part). Объединяет маршрутизирующий домен (RD) и идентификатор региона (AREA) адресов NSAP. Форум ATM объединил эти поля для обеспечения гибкой многоуровневой иерархии адресов для протоколов маршрутизации, основанных на префиксах.
- **ESI** Идентификатор конечной системы (End System Identifier). 48-разрядный MAC-адрес IEEE.
- **SEL** (селектор). Используется для локального мультиплексирования в пределах конечных станций и не имеет значения для сети.
- **ICD.** Определяет международную организацию.
- **E.164.** Адрес BISDN E.164.

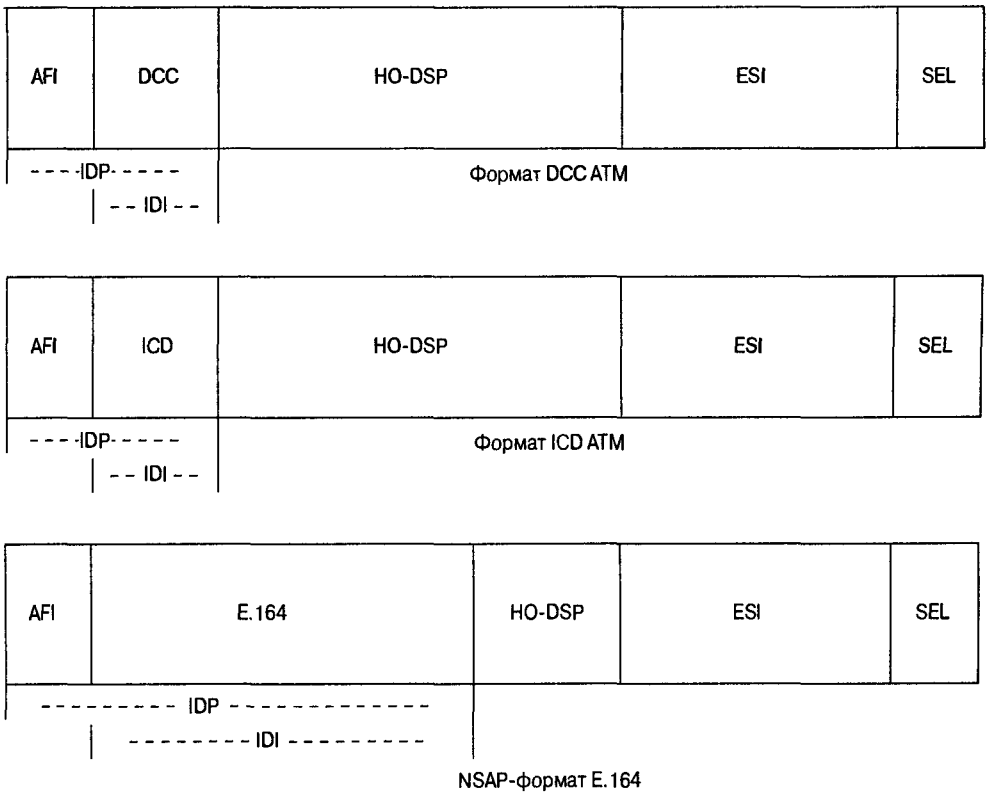


Рис. 31.9. В частных сетях используются три формата адресов ATM

ATM-соединения

ATM поддерживает два типа соединений: "точка-точка" и многоточечное.

Соединение типа "точка-точка" соединяет две конечные системы ATM и может быть однонаправленным (одностороннее соединение) или двунаправленным (двустороннее соединение). Многоточечное соединение представляет собой соединение между одной конечной системой-источником (называемой корневым узлом) и несколькими конечными системами-получателями (называемыми листьями). Такие соединения могут быть только однонаправленными. Корневые узлы могут передавать данные листьям, но листья не могут передавать данные корневому узлу или друг другу в пределах данного соединения. Дублирование ячеек в сети ATM производится коммутаторами в том случае, когда соединение делится на две и более ветвей.

В сетях ATM желательно иметь двунаправленные многоточечные соединения. Подобные соединения аналогичны широковещательной и многоадресатной передаче в локальной сети с общими каналами передачи, такой как Ethernet или Token Ring. Возможность широковещательной рассылки легко использовать в LAN с общим каналом передачи, где все узлы одного сегмента локальной сети должны обрабатывать все пакеты, отправленные в этот сегмент.

К сожалению, двунаправленное многоточечное соединение на уровне AAL5, который является наиболее часто применяемым уровнем AAL для передачи данных по сети ATM, невозможно. В отличие от AAL3/4, который содержит поле идентификации сообщений, формат ячейки AAL5 не предусматривает чередования ячеек разных пакетов AAL5 в одном соединении. Это означает, что все пакеты AAL5, отправленные данному адресату через данное соединение, должны быть получены в определенной последовательности. В противном случае полученные пакеты не удастся восстановить при сборке.

Поэтому многоточечное соединение AAL5 может быть только однонаправленным. Если бы конечный узел-лист, например, отправлял пакет AAL5 по соединению, его бы получили и корневой узел, и все остальные узлы-листья. В этих узлах пакет, отправленный упомянутым выше листом, мог бы смешаться с пакетами, отправленными корневым узлом и, возможно, другими листьями, что воспрепятствовало бы сборке любого из перемешавшихся пакетов.

ATM и многоадресатная передача

Использование коммутации ATM требует некоторых форм многоадресатной передачи. Уровень AAL5 (наиболее часто применяемый уровень адаптации для передачи данных) не поддерживает чередующиеся пакеты, а следовательно, и многоадресатную передачу.

Если бы узел-лист послал пакет по соединению AAL5, то этот пакет смешался бы с другими пакетами и был бы неправильно собран. Были предложены три метода решения этой проблемы: многоадресатная передача по виртуальному маршруту, многоадресатный сервер и многослойное многоточечное соединение.

Многоадресатная передача по виртуальному маршруту подразумевает, что многоточечный виртуальный маршрут связывает все узлы в многоадресатную группу, каждому узлу которой присваивается уникальное значение VCI в пределах этого виртуального канала. Таким образом, перемежающиеся пакеты могут быть идентифицированы по уникальному значению VCI-источника. К сожалению, этот механизм требует протокола, который бы назначал узлам уникальные значения VCI, а такого механизма протоколирования в настоящее время не существует. Также остается неясным, смогут ли подключенные в данный момент устройства SAR поддерживать такой режим работы.

Другое потенциальное решение проблемы многоадресатной передачи по сети ATM состоит в использовании многоадресатного сервера. В этом случае все узлы, которым требуется передать данные многоадресатной группе, создают соединение "точка-точка" с внешним устройством, называемым многоадресатным сервером (хотя лучше было бы назвать его ресеквенсером или параллельно-последовательным преобразователем). Многоадресатный сервер, в свою очередь, соединен со всеми узлами, получающими многоадресатные пакеты по многоточечному соединению. Сервер получает пакеты по соединению "точка-точка" и пересылает их по многоточечному соединению, но только после перевода в последовательный режим (то есть следующий пакет не передается, пока не будет полностью передан предыдущий пакет). Это исключает перемешивание ячеек.

Третье потенциальное решение проблемы многоадресатной передачи по сети ATM предполагает использование многослойного многоточечного соединения. В этом случае все узлы многоадресатной группы устанавливают многоточечное соединение с каждым узлом этой группы, играя роль листьев в соединениях остальных узлов. Таким образом, все узлы могут и передавать, и получать информацию от других узлов. Данный способ требует, чтобы каждый узел поддерживал соединение

с каждым передающим членом группы, тогда как механизм многоадресатного сервера требует всего два соединения. Этот тип соединения также нуждается в процессе регистрации для информирования узлов, которые присоединяются к группе других узлов, чтобы новые узлы смогли установить многоточечное соединение. Остальные узлы должны знать о новом узле, чтобы включить его в свои многоточечные соединения. Механизм многоадресатного сервера обладает более широкими возможностями расширения соединений, но его проблема заключается в том, что он нуждается в централизованном ресиквенсере, который является потенциальным ограничителем производительности сети и единственной точкой возможного сбоя.

Качество обслуживания ATM

ATM гарантирует качество обслуживания QoS, включающее в себя контракт потока данных, формирование потока и управление потоком.

В контракте потока данных оговариваются параметры предполагаемого потока данных, такие как максимальная полоса пропускания, средняя непрерывная полоса пропускания и размер пакета. Когда конечная ATM-система подключается к сети ATM, она заключает с сетью контракт, основанный на параметрах QoS.

Формирование потока данных представляет собой способ использования очередей для ограничения всплесков потока данных, максимальной скорости передачи и обеспечения равномерного дребезга, с тем чтобы передача потока данных соответствовала контракту. Устройства ATM отвечают за соответствие контракту путем перераспределения потоков.

Коммутаторы ATM могут обеспечить принудительное соблюдение контракта посредством *управления потоком*. Коммутатор может измерять действительный поток данных и сравнивать его с параметрами контракта. Если коммутатор обнаружит, что параметры потока данных вышли за заданные пределы, то он может установить для соответствующих ячеек бит приоритета отбрасывания (CLP). Установка бита CLP делает ячейку *потенциально отбрасываемой (или допускающей отбрасывание)*. Это означает, что любой коммутатор, обрабатывающий эту ячейку, в случае перегрузки может ее отбросить.

Сигнализация и установка соединения ATM

Когда устройству ATM требуется установить соединение с другим устройством ATM, оно посылает непосредственно подключенному к нему коммутатору пакет запроса. Этот запрос содержит ATM-адрес получателя и параметры QoS соединения.

Протоколы обмена сигналами ATM различаются по типу ATM-соединения, которое может основываться либо на сигналах интерфейса UNI, либо на сигналах интерфейса NNI. UNI используется при связи между конечной системой и ATM-коммутатором по каналам UNI, а NNI — при связи по каналам NNI.

В настоящее время стандартом передачи сигналов UNI в сети ATM является спецификация UNI 3.1 форума ATM. В основе спецификации UNI 3.1 лежит разработанный ITU-T протокол обмена сигналами для открытых сетей Q.2931. Запросы о передаче UNI передаются по общеизвестному стандартному соединению — VPI = 0, VCI = 5.

Установка ATM-соединения

Для передачи сигналов в сети ATM применяется тот же однопроходный метод настройки соединения, что и во всех современных телекоммуникационных сетях, например, телефонных. Настройка соединения ATM происходит следующим образом. Сначала конечная система-источник посылает сигнальный запрос на соединение. Этот запрос распространяется по сети. В результате по всей сети устанавливаются соединения. Запрос достигает получателя, который либо принимает, либо отклоняет его.

Маршрутизация и согласование запросов на соединение

Маршрутизация запросов на соединение регулируется протоколом маршрутизации ATM (интерфейс частных сетей [PNNI], который маршрутизирует соединения на основе адресов источника и получателя) и параметров QoS, запрашиваемых источником. Возможности согласования запроса о соединении, отклоненного получателем, ограничены, так как маршрутизация вызова основана на параметрах исходящего соединения; изменение параметров может повлиять на маршрутизацию соединения. Однопроходный метод установки соединения ATM показан на рис. 31.10.

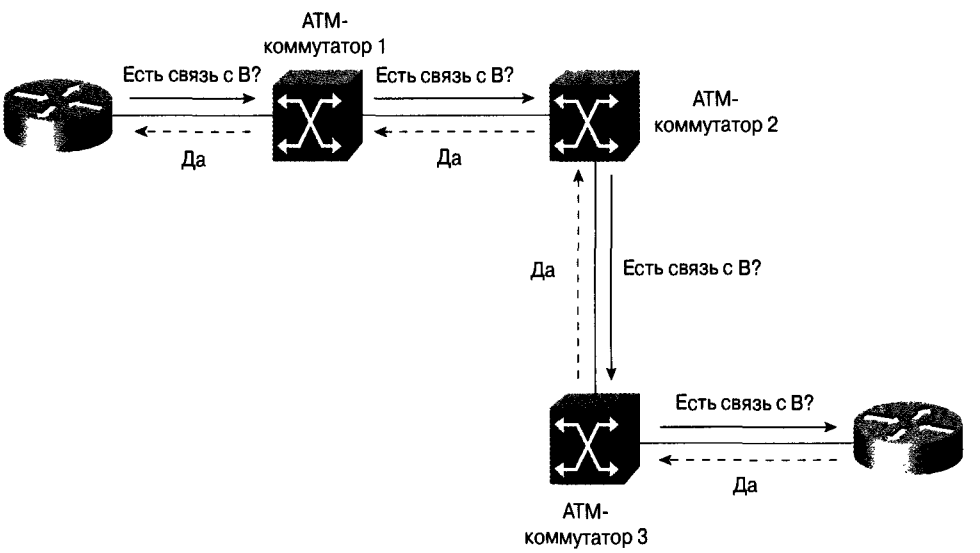


Рис. 31.10. Однопроходный метод установки соединения между ATM-устройствами

Сообщения управления соединением ATM

Для установки и разрыва ATM-соединения используется ряд управляющих сообщений, включая настройку, анализ вызова, подключение и разъединение. При установке соединения конечная система-источник посылает сообщение о настройке, куда входит адрес конечной системы-получателя и параметры QoS. В ответ на сообщение о

настройке входной коммутатор возвращает источнику сообщение об обработке вызова. Затем, если соединение установлено, конечная система-получатель посылает сообщение о подключении.

Если в подключении отказано, конечная система-получатель посылает системе-источнику сообщение о разъединении, тем самым прерывая соединение.

Управляющие сообщения используются для установки ATM-соединения следующим образом. Сначала система-источник посылает сообщение о настройке, которое направляется первому (входному) ATM-коммутатору в сети. Этот коммутатор, в свою очередь, отправляет сообщение об обработке вызова и активизирует протокол маршрутизации ATM. По сети распространяется сигнальный запрос. Выходной коммутатор, подключенный к системе-получателю, получает сообщение о настройке. Затем выходной коммутатор направляет сообщение о настройке по интерфейсу UNI конечной системе и эта ATM-система, если соединение принято, посылает сообщение о подключении. Сообщение о подключении проходит обратно через сеть по тому же маршруту к системе-источнику, которая посылает получателю сообщение о подтверждении соединения. После этого может начинаться передача данных.

Интерфейс PNNI

Интерфейс между частными сетями (Private Network-Network Interface — PNNI) предоставляет две важные службы: определение топологии сети ATM и установку вызова. Для того чтобы коммутаторы устанавливали соединения между конечными точками, они должны знать топологию сети ATM. PNNI является протоколом маршрутизации ATM, который позволяет коммутаторам автоматически определить топологию и параметры соединений, связывающих коммутаторы. Будучи протоколом маршрутизации по состоянию канала, во многом подобным OSPF, PNNI регистрирует такой параметр, как пропускная способность канала. Если происходит значимое событие, изменяющее параметры соединения, то PNNI сообщает об этом изменении другим коммутаторам.

Когда станция посылает локальному коммутатору запрос о настройке вызова, входной коммутатор определяет маршрут от источника к предполагаемому получателю, соответствующий требованиям QoS, установленным источником, по таблице маршрутизации PNNI. Затем коммутатор, соединенный с источником, составляет список коммутаторов, которые должны будут обеспечивать соединение с получателем — *назначенный транзитный список (Designated Transit List — DTL).*

Для PNNI резервируется значение VCI = 18.

Интерфейс ILMI

Интегрированный интерфейс локального управления (Integrated Local Management Interface — ILMI) позволяет устройствам определять состояние компонентов на другом конце физического канала и согласовывать общие рабочие параметры для обеспечения функциональной совместимости. ILMI работает с зарезервированным VCC со значениями VPI = X, VCI = 16.

Администраторы могут включать или отключать ILMI. Настоятельно рекомендуется его включать. Это позволяет устройствам определять наивысший уровень интерфейса UNI (3.0, 3.1, 4.0), UNI или NNI и многие другие параметры. Кроме того, ILMI дает возможность устройствам совместно использовать такую информацию, как

адреса NSAP, имена одноранговых интерфейсов и IP-адреса. Без ILMI многие из этих параметров пришлось бы настраивать вручную для того, чтобы обеспечить нормальную работу подключенных к сети ATM-устройств.

Примечание

Значения VCI от 0 до 31 являются зарезервированными и не должны использоваться для пользовательских потоков данных. В табл. 31.1 указаны три часто используемых значения VCI.

Таблица 31.1. Часто используемые значения VCI

VCI	Функция
5	Передача сигналов от конечного устройства к его коммутатору (входному коммутатору)
16	ILMI для обмена параметрами канала связи
18	PNNI для маршрутизации ATM

Эмуляция LAN

Эмуляция локальной сети (LAN Emulation — LANE) представляет собой стандарт, определенный форумом ATM, который предоставляет станциям, соединенным сетью ATM, те же возможности, что и традиционные локальные сети, такие как Ethernet и Token Ring. Как следует из названия, назначение протокола LANE заключается в эмуляции локальной сети в сети ATM, а именно — стандартов IEEE 802.3 Ethernet или IEEE 802.5 Token Ring. Существующий протокол LANE не определяет отдельной инкапсуляции для FDDI (пакеты FDDI должны преобразовываться в эмулированную LAN Ethernet или Token Ring с применением существующих мостовых преобразований). Fast Ethernet (100BaseT) и IEEE 802.12 (100VG-AnyLAN) не требуют изменений, так как используют такие же форматы фреймов. На рис. 31.11 приведено сравнение физической и эмулированной LAN.

Протокол LANE определяет служебный интерфейс для протоколов высшего (сетевого) уровня, идентичный протоколу сетевого уровня настоящей LAN. Данные, отправленные по сети ATM, инкапсулируются в соответствующий формат пакета LAN MAC. Проще говоря, протоколы LANE заставляют сеть ATM выглядеть и действовать как Ethernet или Token Ring, но работает она гораздо быстрее, чем настоящая локальная сеть Ethernet или Token Ring.

Следует отметить, что LANE не пытается эмулировать настоящий протокол MAC, используемый в локальной сети (CSMA/CD для Ethernet или передача маркера для IEEE 802.5). LANE не требует изменения протоколов высшего уровня для работы в сети ATM. Поскольку служба LANE предоставляет тот же служебный интерфейс существующих протоколов MAC для драйверов сетевого уровня (таких, как NDIS- или ODI-подобный интерфейс драйверов), изменения этих драйверов не нужны.

Архитектура протокола LANE

Основное назначение протокола LANE заключается в преобразовании MAC-адресов в адреса ATM. Нужно преобразовать адрес так, чтобы конечные системы LANE могли устанавливать между собой прямые соединения и передавать по ним

данные. Протокол LANE используется в двух типах оборудования в сети ATM: в сетевых адаптерах и коммутационном оборудовании для объединенных сетей и LAN.

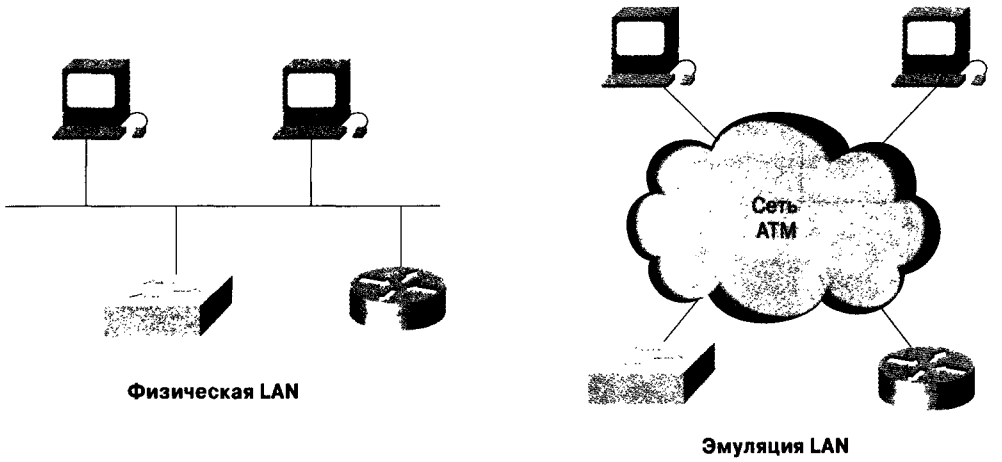


Рис. 31.11. В сети ATM можно эмулировать физическую LAN

В сетевых адаптерах ATM используется интерфейс и протокол LANE для ATM, но драйверам протоколов высшего уровня в пределах подключенной конечной системы предоставляется служебный интерфейс данной LAN. Протоколы сетевого уровня на конечной системе продолжают обмениваться информацией так же и используют те же процедуры, как если бы они были установлены в обычной LAN. Но им предоставляется гораздо большая пропускная способность сетей ATM.

Ко второму классу сетевого оборудования, входящему в состав LANE, относятся подключенные к сети ATM коммутаторы и маршрутизаторы LAN. Эти устройства, а также непосредственно подключенные ATM-узлы с сетевыми адаптерами (NIC) ATM образуют виртуальную LAN (VLAN), в которой порты коммутаторов LAN назначены конкретным VLAN, независимо от их физического местонахождения. На рис. 31.12 показана архитектура протокола LANE, применяемая в сетевых устройствах ATM.

Примечание

Протокол LANE не взаимодействует с ATM-коммутаторами непосредственно. Подобно другим протоколам ATM, LANE построен на оверлейной модели. Поэтому протоколы LANE работают прозрачно с ATM-коммутаторами, используя только стандартные процедуры передачи сигналов ATM.

Компоненты LANE

Протокол LANE определяет действие только одной ELAN или VLAN. Хотя несколько ELAN могут одновременно существовать в одной сети ATM, ELAN эмулирует либо Ethernet, либо Token Ring и состоит из описанных ниже компонентов.

- **LEC** Клиент эмуляции LAN (LAN Emulation Client). Объект в конечной системе, осуществляющий пересылку данных, преобразование адресов и регистрацию MAC-адресов на сервере эмуляции LAN (LES). LEC также обеспечивает стандартный интерфейс LAN для протоколов высшего уровня в традиционных

LAN. У конечной системы ATM, которая соединяется с несколькими ELAN, существует по одному LEC на каждую ELAN.

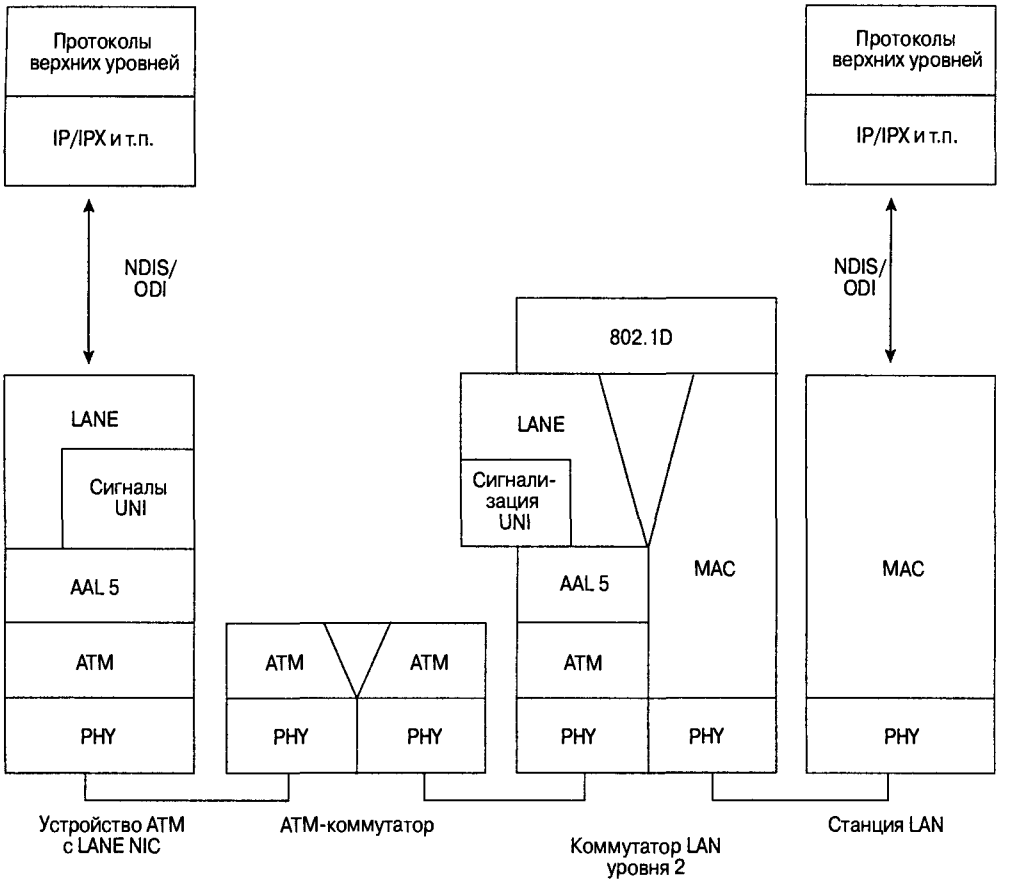


Рис. 31.12. Архитектура протокола LANE может применяться в сетевых устройствах ATM

- **LES** Сервер эмуляции LAN (LAN Emulation Server). Центральный пункт управления, через который LEC передают регистрационную и управляющую информацию (в каждой ELAN существует только один LES). LES содержит список MAC-адресов данной ELAN и соответствующие адреса NSAP.
- **BUS** Сервер широковещательных сообщений и сообщений для неизвестных адресатов (Broadcast and Unknown Server). Многоадресатный сервер, используемый для направления потока данных с неизвестным адресом получателя и пересылки многоадресатных и широковещательных данных клиентам в пределах данной ELAN. Каждый LEC связан с одним BUS в каждой ELAN.
- **LECS** Сервер конфигурации эмуляции LAN (LAN Emulation Configuration Server). Содержит базу данных всех LEC и ELAN, к которым они принадлежат. Принимает запросы от LEC и сообщает в ответ идентификатор ELAN, а именно — ATM-адрес LES, который обслуживает соответствующую ELAN. В каждом административном домене должен быть один LECS, обслуживающий все ELAN этого домена.

Поскольку серверные компоненты требуют избыточности, корпорация Cisco разработала собственную систему — простой серверный протокол с избыточностью (Simple Server Redundancy Protocol — SSRP). Протокол SSRP работает с LEC любых производителей, но требует использования серверных компонентов Cisco. Он позволяет использовать 16 LEC в сети LANE ATM и неограниченное количество пар LES/BUS в ELAN. Форум ATM также разработал независимый метод обеспечения избыточности серверных ресурсов — межсетевой интерфейс эмуляции LANE (LANE Emulation Network-Network Interface — LNNI). Благодаря ему серверы различных производителей обеспечивают избыточность с сохранением функциональной совместимости.

Компоненты ELAN показаны на рис. 31.13.

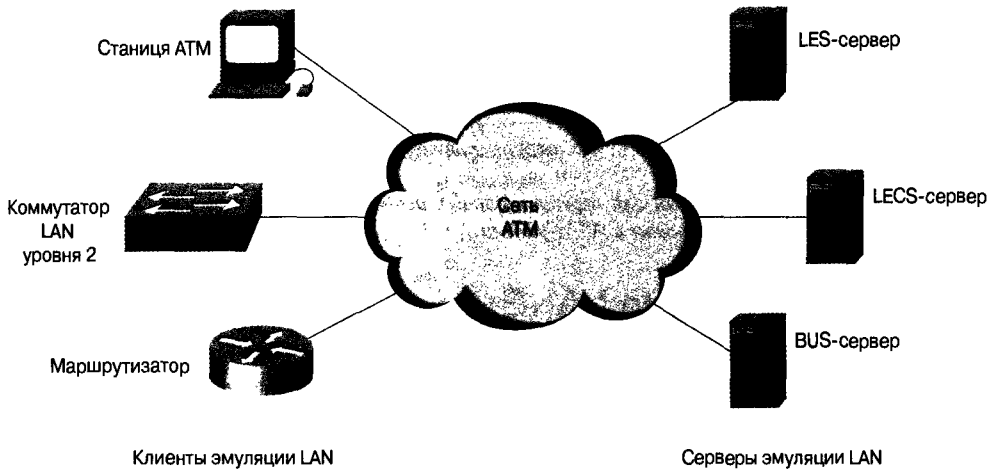


Рис. 31.13. ELAN состоит из клиентов, серверов и различных промежуточных узлов

Типы соединений в эмулированной LAN

Объекты первой фазы LANE обмениваются данными между собой, используя ряд ATM VCC. LEC поддерживают отдельные соединения для передачи данных и управляющих данных. Соединения в LANE представляют собой каналы VCC передачи данных, VCC многоадресатной передачи и VCC многоадресатной пересылки.

VCC передачи данных представляет собой двунаправленный канал VCC типа "точка-точка" между двумя LEC, которым требуется произвести обмен данными. Два LEC используют, как правило, один и тот же VCC для передачи всех пакетов. Они не открывают новый VCC для каждой пары MAC-адресов. Такой подход экономит ресурсы соединения и уменьшает задержку на настройку соединения.

VCC многоадресатной передачи представляет собой двунаправленный VCC типа "точка-точка", устанавливаемый между LEC и BUS.

VCC многоадресатной пересылки представляет собой однонаправленный VCC от BUS к LEC. Как правило, это многоточечное соединение с LEC в роли листьев.

LANE-соединения для передачи данных показаны на рис. 31.14.

Управляющие соединения включают VCC передачи конфигурации, VCC управления и VCC распределения (рис. 31.15). VCC передачи конфигурации представляет собой двунаправленный VCC типа "точка-точка", устанавливаемый между LEC и LECS. VCC управления представляет собой двунаправленный VCC, устанавливаемый между

LEC и LES. VCC распределения представляет собой однонаправленный VCC от LES к LEC (как правило, это многоточечное соединение).

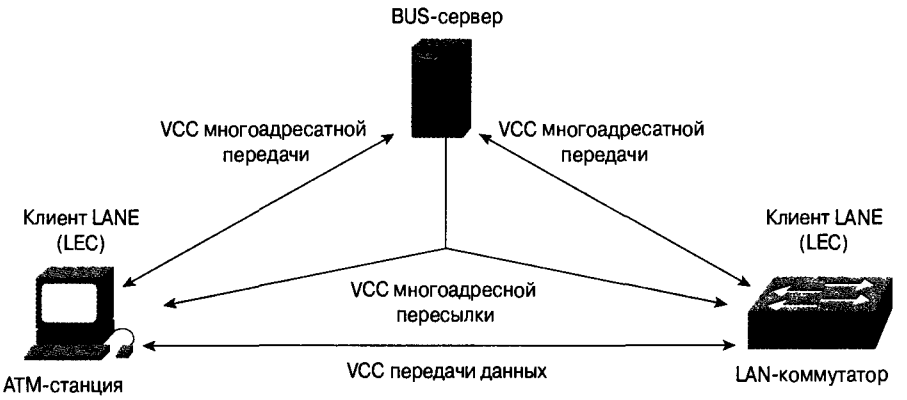


Рис. 31.14. LANE-соединения для передачи данных используют несколько VCC для связи между LAN-коммутатором и ATM-узлами

Функционирование LANE

Для того чтобы лучше понять принцип работы системы LANE и ее компонентов, исследуем этапы работы LEC: инициализация и настройка, подключение к LES с регистрацией, поиск и подключение к BUS и передача данных.

Инициализация и настройка

При инициализации LEC находит LECS и получает от него нужную информацию о конфигурации. LEC начинает этот процесс, когда получает собственный ATM-адрес, что, как правило, происходит при регистрации адреса.

Затем LEC должен определить местонахождение LECS. Для этого LEC должен обнаружить LECS одним из следующих способов: по предопределенной процедуре ILMI определения адреса LECS, по общеизвестному адресу LECS или по общеизвестному постоянному соединению с LECS (VPI = 0, VCI = 17). Последнее используется довольно редко.

После того как LEC узнает NSAP-адрес LECS, он устанавливает с ним VCC настройки и отправляет сообщение LE_CONFIGURE_REQUEST. Если нужные данные найдены, LECS возвращает сообщение LE_CONFIGURE_RESPONSE с параметрами конфигурации, которая требуется для подключения к ELAN, в том числе следующими: ATM-адрес LES, тип эмулируемой LAN, максимальный размер пакета в ELAN и имя ELAN (текстовая строка для отображения на экране).

Подключение к LES и регистрация

Подключение LEC к LES и регистрация ATM- и MAC-адресов LEC происходит в три этапа.

1. Когда LEC получает адрес LES, он может разорвать соединение с LECS, установить VCC управления с LES и послать по этому VCC сообщение

LE_JOIN_REQUEST. Это позволяет LEC регистрировать на LES собственные MAC- и ATM-адреса а также, возможно, любые другие MAC-адреса, для которых он является посредником. Эта информация сохраняется, чтобы два разных LEC не могли зарегистрировать одинаковые MAC- или ATM-адреса.

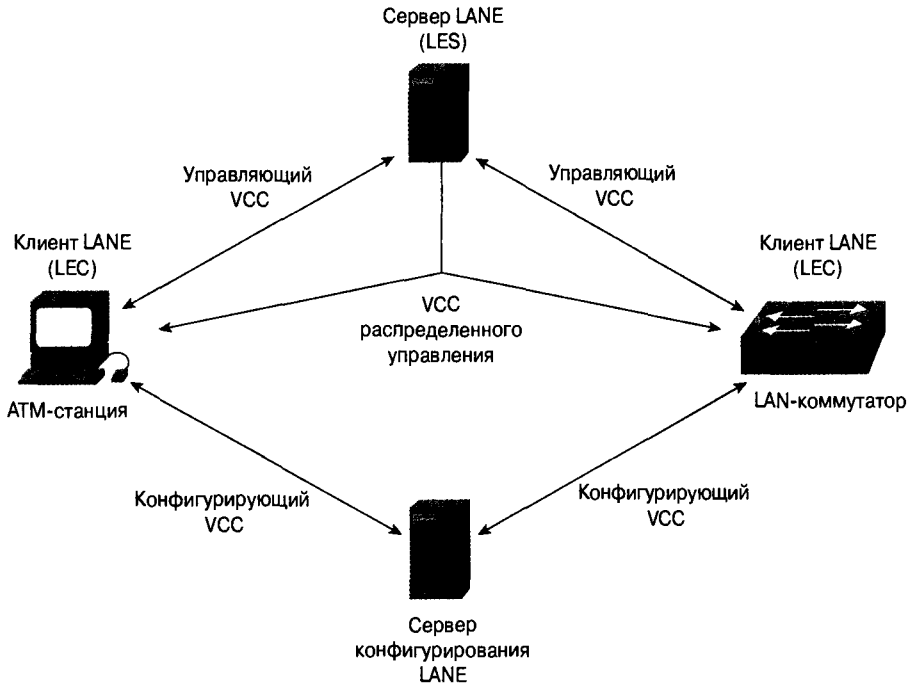


Рис. 31.15. Управляющие соединения эмуляции LAN связывают LES, LECS, LAN-коммутатор и ATM-узел

2. После получения сообщения LE_JOIN_REQUEST LES сверяется с LEC по открытому соединению, проверяет запрос и подтверждает принадлежность клиента сети.
3. После удачного подтверждения LES присоединяет LEC к сети в качестве листа своего многоточечного VCC распределения и посылает ему сообщение LE_JOIN_RESPONSE, содержащее уникальный идентификатор клиента эмуляции LAN (LECID). LEC использует LECID для отделения собственных широковещательных рассылок от BUS.

Поиск и подключение к BUS

После успешного подключения LEC к LECS следующей задачей становится поиск ATM-адреса BUS для включения в широковещательную группу и эмулируемую LAN.

Сначала LEC создает пакет LE_ARP_REQUEST с MAC-адресом 0xFFFFFFFF. Затем LEC посылает на LES специальный пакет LE_ARP по VCC управления. LES определяет, что LEC ищет BUS, и посылает по VCC распределения ответ с ATM-адресом BUS.

Получив ATM-адрес BUS, LEC соединяется с ним, создавая сначала сигнальный пакет с ATM-адресом BUS и устанавливая с ним многоадресатный VCC. Получив

сигнальный запрос, BUS добавляет этот LEC к VCC многоадресатной пересылки в качестве листа. Теперь LEC является членом ELAN и готов к передаче данных.

Передача данных

Последний этап, передача данных, включает в себя преобразование ATM-адреса конечного LEC и собственно передачу данных, которая может подразумевать и процедуру очистки канала.

Если у LEC есть пакет данных для передачи получателю с неизвестным MAC-адресом, он должен узнать ATM-адрес LEC-получателя, через который можно достичь конкретного адреса. Для этого LEC сначала посылает фрейм данных на BUS (через VCC многоадресатной передачи) для распространения по всем LEC в данной ELAN по VCC многоадресатной пересылки. Это делается потому, что на преобразование ATM-адреса может уйти некоторое время, а многие сетевые протоколы не терпят задержек.

Затем LEC посылает серверу LES через VCC управления управляющий фрейм запроса (LE_ARP_Request).

Если LES знает ATM-адрес LEC, который имеет MAC-адрес, указанный в запросе, он посылает его в ответ. Если LES не знает такого адреса, он рассылает LE_ARP_REQUEST нескольким или всем LEC (по правилам рассылки действительного фрейма данных с BUS, но по VCC управления и распределения, а не многоадресатной передачи или многоадресатной пересылки, которую использует BUS). Если в ELAN существует мост или коммутатор с программным обеспечением LEC и если они обслуживают устройство LAN с запрашиваемым MAC-адресом, то они отвечают на LE_ARP_REQUEST. Эта функция называется *прокси-службой*.

В случае передачи действительных данных, если получено сообщение LE_ARP, LEC создает VCC передачи данных с LEC-получателем и использует для передачи его, а не маршрут BUS. Но прежде чем сделать это, LEC, возможно, потребуется выполнить очистку канала, чтобы все пакеты, отправленные на BUS, были доставлены получателю до того, как был использован VCC передачи данных. При очистке по первому маршруту передачи за последним пакетом посылается контрольный фрейм. LEC ждет, пока получатель не подтвердит получение пакета очистки, прежде чем использовать для передачи пакетов второй маршрут.

Многопротокольная схема в ATM

Многопротокольная схема в ATM (MultiProtocol Over ATM — MPOA) обеспечивает передачу данных между сетями ELAN, минуя маршрутизатор. Обычно для того, чтобы попасть из одной ELAN в другую, данные проходят по крайней мере через один маршрутизатор. Это нормальный режим поузловой маршрутизации, используемый в среде LAN. Но MPOA позволяет устройствам из разных ELAN обмениваться данными, минуя маршрутизаторы.

На рис. 31.16 показан процесс без MPOA часть (а) и с MPOA часть (б). При обмене информацией с использованием MPOA только первые несколько фреймов проходят через маршрутизаторы. Это называется *основным маршрутом*. Фреймы передаются из одной ELAN в другую через соответствующие маршрутизаторы. После того как несколько фреймов проследуют по основному маршруту, устройства MPOA определяют NSAP-адрес устройства, с которым они связываются, и создают для всех последующих фреймов потока прямое соединение, называемое *кратчайшим маршрутом*.

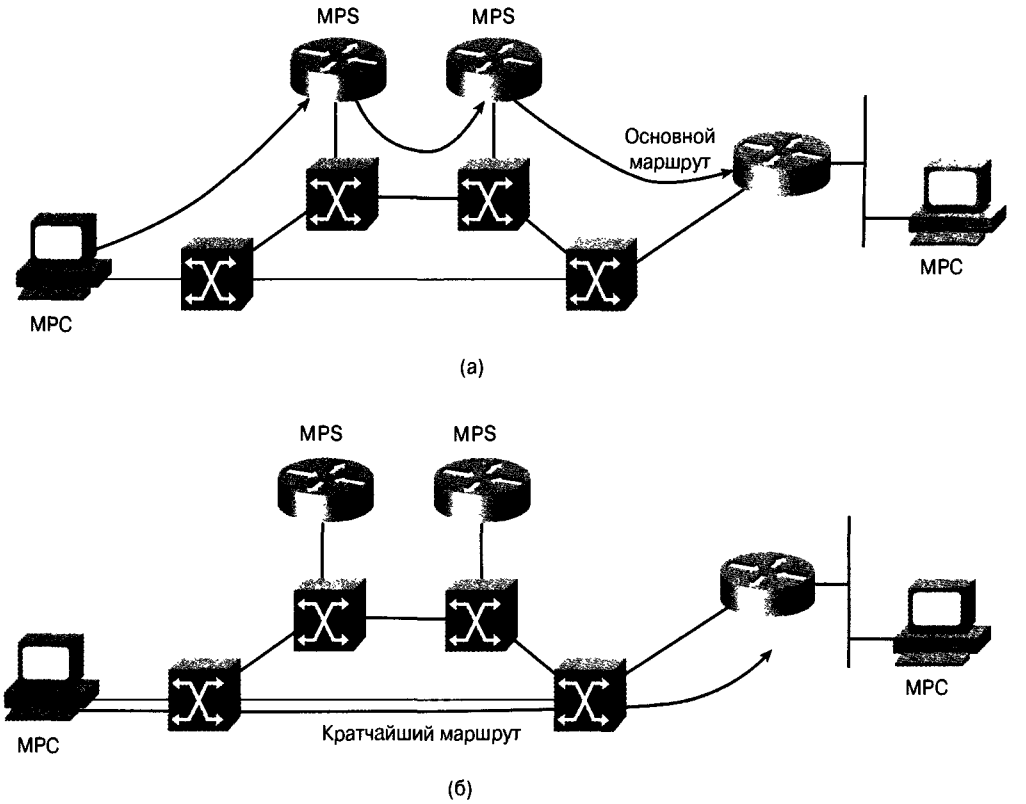


Рис. 31.16. Соединение между ELAN с MPOA (а) и без него (б)

Конечные устройства, генерирующие поток данных ATM, называются многопротокольными клиентами (MultiProtocol Client — MPC). Ими могут быть рабочие станции или маршрутизаторы, подключенные к сети ATM. Маршрутизаторы, расположенные между ELAN, называются многопротокольными серверами (MultiProtocol Servers — MPS) и помогают клиентам в построении кратчайшего маршрута. В роли MPS может выступать только маршрутизатор.

MPOA снижает нагрузку на маршрутизаторы, так как последним не требуется обрабатывать весь поток данных, проходящих между устройствами. Кроме того, MPOA иногда позволяет сократить количество ATM-коммутаторов, обслуживающих соединение, освобождая виртуальные каналы и коммутационные ресурсы в сети ATM. На рис. 31.16 показано соединение до и после создания кратчайшего маршрута.

Следует обратить внимание на то, что MPOA не заменяет LANE. Более того, MPOA требует использования LANE 2.

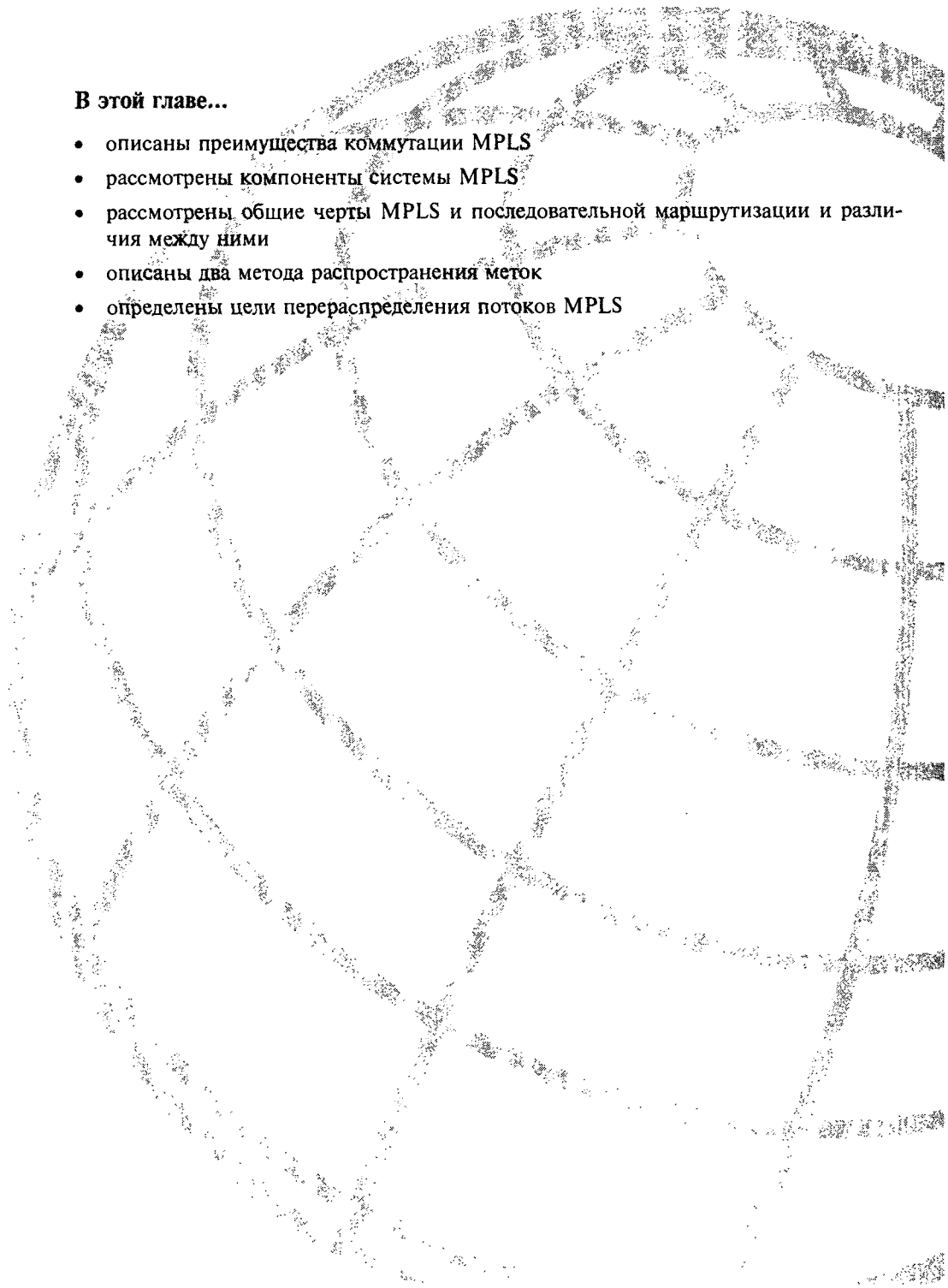
Контрольные вопросы

1. Назовите четыре компонента LANE.
2. Какой компонент LANE содержит таблицу ARP сети ATM?
3. Какой компонент LANE управляет компонентами ELAN?

4. Назовите две функции интерфейса частных сетей (PNNI).
5. По какому полю заголовка ATM проверяется целостность заголовка?
6. В чем заключается основное отличие между заголовками UNI и NNI?
7. Какой режим адаптации наиболее подходит для обмена сигналами T1 между мини-АТС в сети ATM?
8. Какой режим адаптации наиболее часто применяется для передачи данных по сети ATM?
9. Какое значение VCI резервируется для запросов установки соединения от конечных ATM-устройств?
10. Какой протокол ATM облегчает работу администратора, автоматически обеспечивая совместимость определенных параметров двух устройств, подключенных к одному и тому же каналу?
11. Какой протокол ATM используется исключительно при соединении ATM-коммутаторов?
12. Чем отличается PVC от SVC?
13. Какова цель адаптационного уровня?
14. Каковы преимущества MPOA?

Дополнительные источники

- Clark, Kennedy, and Kevin Hamilton. *CCIE Professional Development: Cisco LAN Switching.* Indianapolis: Cisco Press, 1999.
- Ginsburg D. *ATM: Solutions for Enterprise Internetworking.* Boston: Addison-Wesley Publishing Co, 1996.
- McDysan, David E., and Darren L. Spohn. *ATM Theory and Application.* New York: McGraw-Hill, 1998
- http://www.atmforum.com (стандарты ATM)



В этой главе...

- описаны преимущества коммутации MPLS
- рассмотрены компоненты системы MPLS
- рассмотрены общие черты MPLS и последовательной маршрутизации и различия между ними
- описаны два метода распространения меток
- определены цели перераспределения потоков MPLS

Глава 32

Коммутация MPLS

Введение

В среде с обычной маршрутизацией дейтаграммы 3-го уровня направляются от источника к получателю последовательно (отдельными переходами). Промежуточные маршрутизаторы анализируют заголовок 3-го уровня каждого фрейма и ищут в таблице маршрутизации адрес следующего узла в направлении получателя. Хотя в некоторых маршрутизаторах для ускоренного определения адреса используются методы аппаратной и программной коммутации (например, скоростная пересылка Cisco [Cisco Express Forwarding — CEF]), создающие для определении пути к получателю высокоскоростные кэш-элементы, в целом эти методы основываются на протоколе маршрутизации 3-го уровня.

К сожалению, протоколы маршрутизации практически не могут просматривать характеристики сети на 2-м уровне, в частности, учитывать требования качества обслуживания (QoS) и загрузку сети. Быстрые изменения типа и объема потоков данных, обрабатываемых в сети Internet, и взрывной рост числа пользователей вызывают беспрецедентные нагрузки на инфраструктуру Internet. Это требует использования новых систем управления потоками. Целью использования коммутации MPLS и ее предшественницы, коммутации по тегам, является решение многих проблем, вызванных общим развитием глобальной сети Internet и высокоскоростных каналов передачи данных.

Для удовлетворения этих новых требований была разработана многопротокольная коммутация по метке (MultiProtocol Label Switching — MPLS), изменяющая сам принцип последовательной маршрутизации При использовании коммутации MPLS граничные маршрутизаторы определяют маршруты в сети на основании определяемых пользователем требований с учетом требуемого качества обслуживания QoS и необходимой приложению полосы пропускания. Иными словами, при выборе маршрута в сети, которая использует только маршрутизаторы, теперь можно учитывать атрибуты 2-го уровня. Такое решение позволяет Internet-провайдерам (Internet service provider — ISP) и крупным промышленным сетям реализовать объединенную инфраструктуру 3-го уровня, которая может удовлетворять требования, которые ранее могли выполняться только в магистрали 2-го уровня (такой как магистраль Frame Relay или ATM).

По существу технология MPLS объединяет богатство функций IP-маршрутизации и простоту последовательной коммутации технологий Frame Relay и ATM, осуществляя

гармоничное слияние ориентированной на соединение пересылки 2-го уровня со средой протокола IP, для которого характерна связь без установки соединения. В силу своей двойственной природы (действуя как на уровне протокола IP, так и на уровне коммутации по меткам), устройства MPLS часто называются маршрутизаторами, осуществляющими коммутацию по метке (Label Switch Router — LSR) или LSR-устройствами.

Основываясь на фирменном протоколе коммутации тегов Cisco, группа IETF определяет MPLS как протокол, не зависящий от производителя. У этих двух протоколов много общего. Единственным серьезным различием являются детали протокола, используемого смежными устройствами MPLS, который дает возможность сетевым администраторам осуществлять постепенный переход от сетей с коммутацией по тегам к основанным на стандартах сетям MPLS.

Терминология MPLS

Коммутация MPLS использует ряд новых терминов. Ниже описаны наиболее важные из них.

- **Заголовок метки (Label header).** Заголовок, создаваемый граничным LSR-устройством и используемый другими LSR-устройствами для пересылки пакетов. Формат заголовка меняется в зависимости от типа используемой в сети передающей среды. В сетях ATM метка располагается в полях VPI/VCI заголовка каждой ATM-ячейки. Во всех остальных средах (например, в LAN-сетях или в каналах типа "точка-точка") этот заголовок является "промежуточным" (shim) и располагается между заголовками 2-го и 3-го уровней, как показано на рис. 32.1. Заголовок метки может содержать одну метку или стек меток.
- **Информационная база пересылки по меткам (Label Forwarding Information Base — LFIB).** Таблица, созданная устройством коммутации по метке (Label Switch-Capable Device — LSR), которая указывает, куда и как следует пересылать фреймы с определенными значениями меток.
- **Маршрутизатор коммутации по метке или LSR-устройство (Label Switch Router — LSR).** Коммутатор или маршрутизатор, который передает элементы с метками согласно значению этих меток.
- **Граничный маршрутизатор коммутации по метке или граничное LSR-устройство (edge LSR).** Устройство, первым добавляющее или последним удаляющее метку из пакета. Граничное LSR-устройство имеет интерфейсы, соединенные с другими LSR-устройствами и интерфейсы, соединенные с устройствами, не обладающими функциями MPLS (например, с узлами протокола IP).
- **Базовое LSR-устройство (Core LSR).** Устройство, выполняющее коммутацию на основе значения метки, содержащегося в заголовке пакета. Все интерфейсы такого устройства соединены с другими LSR-устройствами.
- **Пересылка с использованием коммутации по метке (label switched).** Решение о передаче, принятое LSR-устройством на основании метки, содержащейся во фрейме/ячейке.
- **Маршрут с коммутацией по меткам (Label-switched path — LSP).** Определяемый метками маршрут между двумя граничными LSR-устройствами, проходящий через базовые LSR.

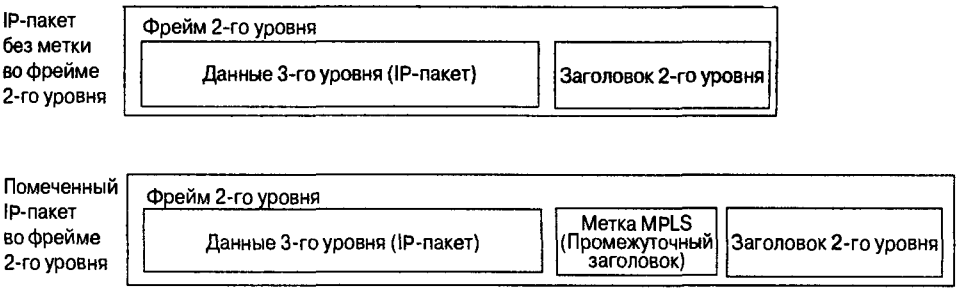


Рис. 32.1. Положение заголовка метки MPLS во фрейме 2-го уровня

Для описания работы MPLS в среде ATM определены несколько новых терминов, приведенных ниже.

- **Виртуальный канал с коммутацией по метке (Label virtual circuit — LVC).** Маршрут LSP в системе IP+ATM (сеть ATM с функциями коммутации по меткам).
- **Контроллер коммутации по меткам (Label switch controller — LSC).** Соединенное с ATM-коммутатором или встроенное в него LSR-устройство, которое обменивается данными с этим ATM-коммутатором для инициализации и поддержки кросс-соединений LVC в коммутаторе ATM.
- **Протокол распространения меток (Label distribution protocol — LDP).** Протокол рассылки сообщений, предназначенных для распространения информации о метках между LSR-устройствами.
- **XmplsATM.** Виртуальный интерфейс между ATM-коммутатором и контроллером LSC.

Функционирование коммутации MPLS

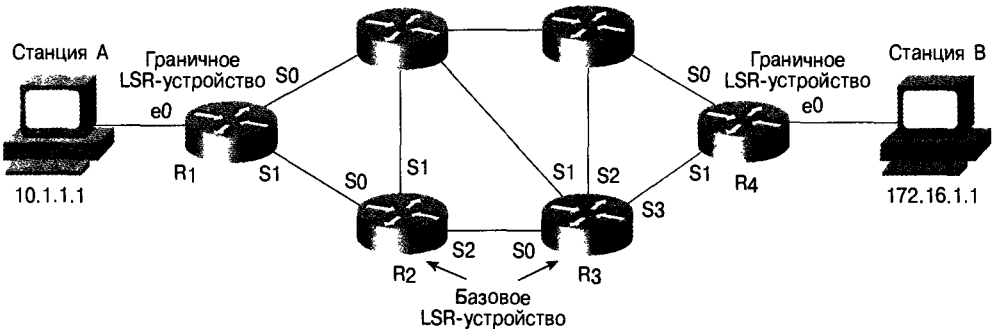
В настоящем разделе описываются процесс передачи фреймов в системе MPLS и функции некоторых основных компонентов MPLS. В частности, в нем описано функционирование коммутации MPLS в инфраструктуре, основанной на передаче фреймов, в сравнении с системой, основанной на передаче ячеек (ATM).

На рис. 32.2 показано соединение нескольких LSR-устройств (граничных и базовых), образующих физический путь между двумя элементами — станцией A и станцией B.

Ethernet-фрейм, созданный станцией A, переносит IP-дейтаграмму и соответствует стандартному формату Ethernet с обычным заголовком 2-го уровня, за которым следует заголовок 3-го уровня. Поскольку адрес получателя указывает на другую сеть, станция A направляет фрейм с заголовком 2-го уровня на свой стандартный шлюз (R1). В данном случае стандартный шлюз одновременно играет роль граничного LSR-устройства (входного). Это LSR-устройство по своей внутренней таблице IP-коммутации (Forwaring Information Base — FIB) определяет, что эту IP-дейтаграмму следует отправить в направлении следующего LSR-устройства через интерфейс S1.

Позиция базы FIB для сети 172.16.1.0/24 на входном LSR-устройстве указывает на то, что между заголовками 2-го и 3-го уровней должна быть вставлена метка, чтобы указать, по какому маршруту должен направляться фрейм, адресованный станции B. Поэтому входное LSR вставляет заголовок MPLS между заголовком 2-го уровня протокола PPP (Point-to-Point) и IP-заголовком (этот процесс называется присвоением метки) и направляет этот помеченный пакет маршрутизатору R2. Маршрутизатор 2

анализирует фрейм, поступающий на порт 1, и обнаруживает между заголовками 2-го и 3-го уровней метку, значение которой основано на информации заголовка фрейма 2-го уровня (например, поля пакета PPP или поля Ethertype в пакетах LAN). Далее маршрутизатор обрабатывает фрейм согласно своей базе LFIB, в которой указано, что фрейм требуется отправить через порт 2, заменив входную метку 6 выходной меткой с новым значением, равным 11. Все последующие маршрутизаторы выполняют над фреймом такие же операции, пока фрейм не достигнет выходного LSR-устройства.



Маршрутизатор	Входная метка	Входной интерфейс	Сеть-получатель	Выходной интерфейс	Выходная метка
R1	C	e0	172.16.1	S1	6
R2	6	S0	172.16.1	S2	11
R3	11	S0	172.16.1	S3	7
R4	7	S1	172.16.1	e0	C

Рис. 32.2. Соединенные между собой LSR-устройства

Выходное граничное LSR-устройство таким же образом, как и предыдущие, просматривает свою таблицу и обнаруживает, что выходная метка для этого фрейма отсутствует. Поэтому оно стирает всю информацию о метках (этот процесс называется удалением меток) и передает стандартную IP-дейтаграмму, инкапсулированную во фрейм ethernet, станции B. Поскольку каждый из маршрутизаторов, расположенных между Станциями A и B, может коммутировать фрейм согласно информации своей базы LFIB и не должен совершать обычные операции маршрутизации, IP-дейтаграмма обрабатывается быстрее и эффективнее. Кроме того, для маршрута LSP от R1 к R4 в данном случае могут быть использованы каналы, отличные от тех, которые указываются таблицей маршрутизации протокола IP.

Структура коммутации MPLS и коммутации по тегам

В основе MPLS лежат два принципиально важных компонента: компонент передачи и компонент управления. Компонент управления отвечает за поддержку правильной информации о передаче по метке в группе связанных между собой LSR-устройств. Компонент

передачи использует для пересылки пакетов метки, переносимые пакетами, и информацию о пересылке по метке, поддерживаемую LSR-устройствами. Механизмы пересылки и управления MPLS будут подробно описаны ниже.

Компонент управления

Все устройства сети MPLS поддерживают на своей управляющей плоскости (contol plane) какой-либо IP-протокол маршрутизации для построения своих таблиц IP-маршрутизации. В устройствах MPLS, поддерживающих IP-пересылку (например, на граничных LSR-устройствах), для построения таблиц IP-пересылки (баз FIB) используются таблицы IP-маршрутизации. На устройствах MPLS, которые поддерживают только пересылку по меткам (таких, как ATM-коммутаторы с функциями MPLS), базы FIB IP-маршрутизации отсутствуют. На рис. 32.3 показано функционирование IP-маршрутизации на управляющей плоскости MPLS.

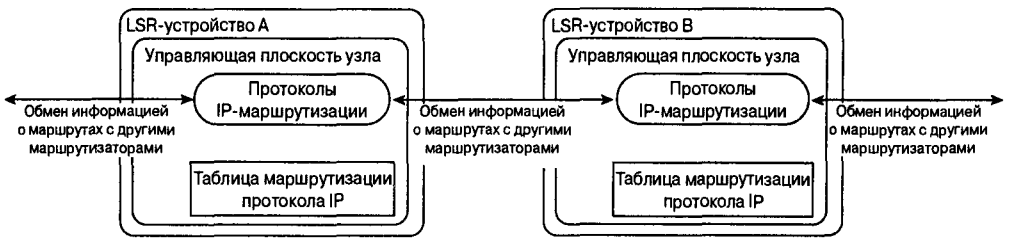


Рис. 32.3. LSR-устройства создают таблицы IP-маршрутизации

После того, как таблицы IP-маршрутизации построены, отдельным позициям этих таблиц назначаются метки (индивидуальные IP-префиксы), которые затем распространяются среди смежных устройств MPLS при помощи протокола LDP.

Внимание

При обычном функционировании коммутации MPLS пунктам назначения протокола граничного шлюза (Border Gateway Protocol — BGP) метки не назначаются, поскольку маршрутизаторы всегда получают доступ к этим пунктам путем рекурсивного просмотра на следующем BGP-переходе. Вследствие этого пункты назначения протокола BGP могут быть достигнуты с помощью метки, связанной со следующим BGP-переходом для этих пунктов, как описано в разделе "Иерархическая маршрутизация".

Каждое устройство MPLS использует свое собственное пространство меток. При этом отсутствует необходимость в глобально уникальных метках или в централизованном назначении меток, что обеспечивает коммутации MPLS высокую надежность и масштабируемость. Каждая метка, назначаемая MPLS-устройством, вводится как входная метка в его базу LFIB, т.е. в таблицу пересылки, используемую для коммутации по метке. На рис. 32.4 показано назначение и распространение меток для MPLS-устройства.

Большинство назначений меток, как локальных, так и сделанных смежными устройствами, заносятся в таблицу, называемую информационной базой меток (Label Information Base — LIB). Метка, назначенная следующим IP-переходом, для конкретного IP-префикса, заносится в качестве выходной метки в локальную базу LFIB для того, чтобы стала возможной простая пересылка по метке. В устройствах, которые поддерживают IP-пересылку, такая метка также заносится в базу FIB для поддержки пересылки по схеме "IP-адрес — метка".

Внимание!

База LIB содержит все метки, назначенные IP-префиксу локальными LSR-устройствами и соседними с ним устройствами. База LFIB содержит только преобразования входных меток в выходные, которые используются для пересылки помеченных пакетов. Поэтому информация базы LFIB всегда является частью информации, содержащейся в базе LIB.

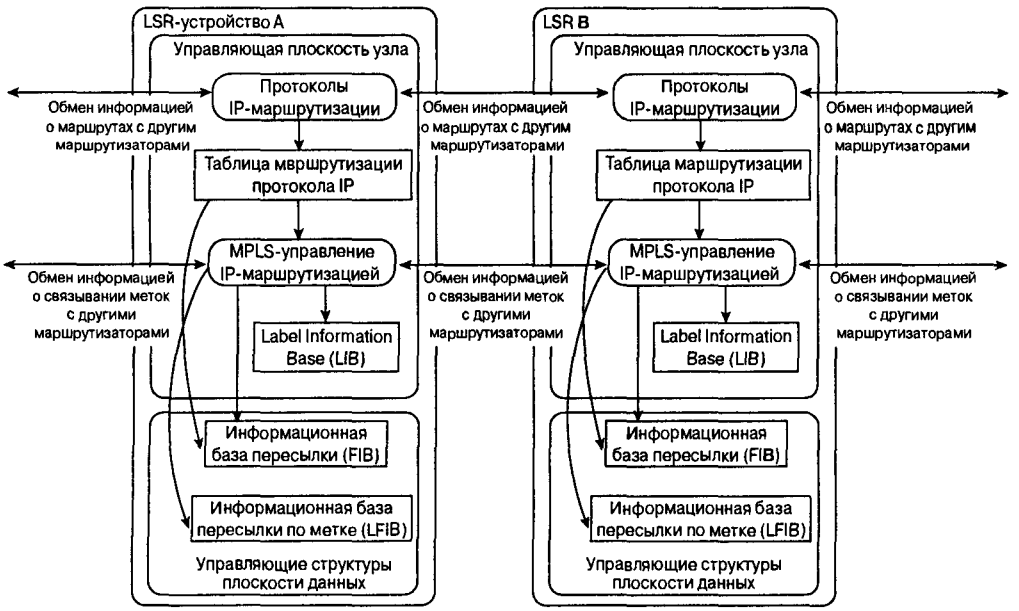


Рис. 32.4. Операции управляющей плоскости в LSR-устройстве

Протокол распространения меток

При использовании маршрутизации на основе адреса получателя маршрутизатор принимает решение о пересылке, основываясь на содержащемся в пакете адресе 3-го уровня получателя и на данных из информационной базы пересылки (FIB), которая поддерживается маршрутизатором. Маршрутизатор строит свою базу FIB на основе информации, получаемой в результате работы протоколов маршрутизации, таких как OSPF или BGP.

Для того чтобы обеспечить маршрутизацию по адресу получателя в системе MPLS, LSR-устройства принимают участие в работе протоколов маршрутизации и строят свои базы LFIB на основе информации, полученной из этих протоколов. В этом случае LSR-устройство функционирует как маршрутизатор.

Однако для правильной пересылки фрейма другими одноранговыми LSR-устройствами LSR-устройство должно распространять и использовать выделенные метки. Для распространения меток LSR-устройства используют протокол распространения меток (Label Distribution Protocol — LDP). При связывании меток локальной метке сопоставляется подсеть-получатель. (Метки называются локальными, поскольку они заменяются на каждом узле). Каждый раз, когда LSR-устройство обнаруживает соседнее LSR-устройство, между ними устанавливается TCP-соединение для передачи информации

о связывании меток. Протокол LDP осуществляет обмен информацией о связывании меток с подсетями одним из двух способов: нисходящее распределение без запроса или нисходящее распределение по запросу. Выбранный режим должен быть согласован между обоими LSR-устройствами.

Нисходящее распространение меток без запроса происходит в том случае, когда LSR-устройству, расположенному в нисходящем направлении необходимо создать новое связывание меток с соседним LSR-устройством, находящемся в восходящем направлении, например, в ситуации, когда на граничном LSR-устройстве появился новый интерфейс с другой подсетью. В этом случае граничное LSR-устройство сообщает маршрутизатору, находящемуся в восходящем направлении о появлении нового связывания, соответствующего маршруту в эту сеть.

Напротив, при нисходящем распространении меток по запросу находящееся в нисходящем направлении LSR-устройство сообщает о новом связывании меток в восходящем направлении только в том случае, если расположенное там LSR-устройство ее запрашивало. Для каждого маршрута своей таблицы это LSR-устройство определяет следующий переход на маршруте. После этого оно запрашивает (при помощи протокола LDP) у следующего узла связывание меток для этого маршрута. Когда узел следующего перехода получает этот запрос, он назначает метку, создает запись в своей базе LFIB с входной меткой, равной назначенной метке, а затем возвращает информацию о связывании (входной) метки и маршрута LSR-устройству, которое послало первоначальный запрос. Когда это последнее LSR-устройство получает информацию о связывании, оно создает в своей базе LFIB соответствующую запись и присваивает выходной метке в этой записи значение, полученное от узла следующего перехода. В сети, использующей нисходящее распространение меток по запросу, этот процесс рекурсивно повторяется до тех пор, пока на будет достигнут пункт назначения.

Компонент пересылки по метке

Применяемый в MPLS принцип пересылки основан на замене меток. Когда LSR-устройство получает пакет с меткой, коммутатор использует метку как индекс в своей информационной базе LFIB. Каждая запись в LFIB состоит из входной метки и одной или нескольких подзаписей (в виде выходной метки, выходного интерфейса и выходной информации канального уровня). Если коммутатор обнаруживает, что входная метка одной из записей совпадает с меткой, содержащейся в пакете, для каждой составляющей этой записи коммутатор заменяет метку пакета на выходную метку записи, информацию пакета канального уровня (такую как MAC-адрес) пакета на выходную информацию записи канального уровня и пересылает пакет через выходной интерфейс. Некоторые MPLS-устройства (например, граничные LSR) могут принимать IP-дейтаграммы, просматривать базу FIB, вставлять метку MPLS перед IP-дейтаграммой на основе информации базы FIB и пересылать помеченный пакет LSR-устройству следующего перехода. Маршруты коммутации, поддерживаемые граничным LSR-устройством показаны на рис. 32.5.

Из приведенного описания компонента передачи можно сделать следующие выводы. Во-первых, решение о передаче основано на алгоритме точного соответствия, использующем в качестве индексов короткие метки фиксированной длины. Благодаря этому процедура пересылки получается более простой по сравнению с пересылкой по максимальному совпадению меток, традиционно используемой на сетевом уровне.

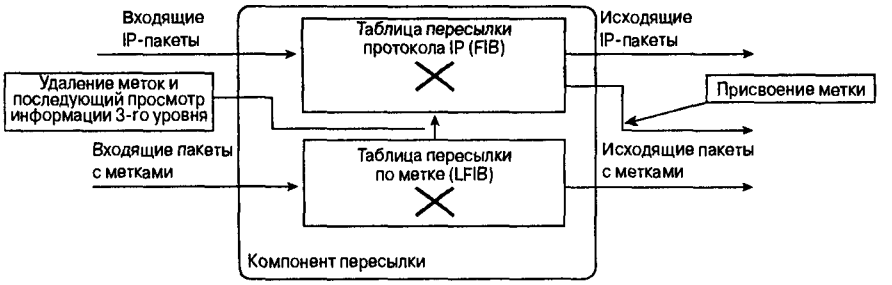


Рис. 32.5. Маршруты коммутации на граничном LSR-устройстве

Это, в свою очередь, обеспечивает более высокую производительность пересылки (передается больше пакетов в секунду). Процедура достаточно проста для того, чтобы ее можно было реализовать аппаратным способом. Второе наблюдение заключается в том, что решение о пересылке не зависит от способа дробления помеченных пакетов. При этом один и тот же алгоритм пересылки подходит как для одноадресатной, так и для многоадресатной рассылки. У одиночной записи будет единственная подзапись (выходная метка, выходной интерфейс и выходная информация канального уровня), а у групповой записи может быть несколько таких подзаписей. Это показывает, что при использовании коммутации по метке один и тот же способ передачи может использоваться для поддержки различных функций маршрутизации.

Таким образом, при коммутации по метке эта простая процедура пересылки оказывается практически отделена от компонента управления. Новые функции маршрутизации (управления) могут вводиться не затрагивая способ передачи. Это означает, что при добавлении (на уровне управляющей плоскости) новой функции маршрутизации нет необходимости заново оптимизировать процедуру пересылки (путем модернизации оборудования или программного обеспечения). Например, уже в настоящее время большое количество MPLS-приложений, совместно использующих базу LFIB, поддерживаются маршрутизаторами Cisco, как показано на рис. 32.6.

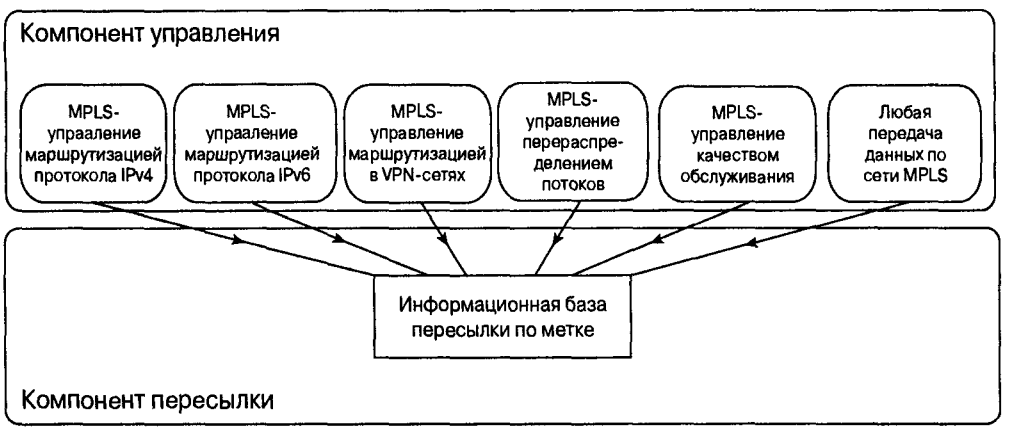


Рис.32.6. Несколько MPLS-приложений совместно используют общую базу LFIB

Инкапсуляция меток

Информация о метках может передаваться в пакетах следующими способами.

- В виде небольшого промежуточного заголовка-метки, вставляемого между заголовками 2-го и сетевого уровней (см. рис. 32.7).
- В составе заголовка 2-го уровня, при условии, что этот заголовок обеспечивает надлежащую семантику (например, заголовок ATM).

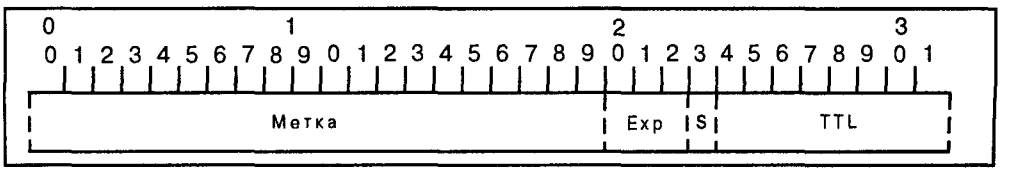


Рис. 32.7. Формат заголовка метки MPLS

Таким образом, MPLS может использоваться в любых сетях, в том числе для соединений "точка-точка", соединений множественного доступа и соединений ATM. Компонент пересылки по меткам не зависит от протокола сетевого уровня. Применение соответствующего компонента управления позволяет использовать коммутацию по метке с различными протоколами сетевого уровня.

Коммутация по метке в сетях ATM

Поскольку принцип передачи в сетях MPLS, как и в сетях ATM, основан на замещении меток, технология MPLS может быть применена к коммутаторам ATM путем использования компонента управления. Информация о метках, необходимая для MPLS-коммутации, передается в поле VPI и VCI каждой ячейки ATM.

Внимание!

Сочетание коммутации ATM, MPLS и IP-технологии в ATM-коммутаторах обычно обозначается как IP+ATM.

В большинстве сетей IP+ATM коммутаторы ATM поддерживают дополнительные механизмы назначения меток (например, сигнализацию Forum ATM), а поле VPI используется для выделения части доступного пространства метки различным механизмам установки метки. Для большинства сетей отдельное значение VPI, выделенное протоколу LDP MPLS является достаточным.

Использование коммутации MPLS в ATM-коммутаторах упрощает интеграцию ATM-коммутаторов и маршрутизаторов в сеть MPLS. ATM-коммутатор с функциями MPLS для смежного маршрутизатора, пересылающего пакеты, выглядит как маршрутизатор. Такой подход предоставляет масштабируемую альтернативу модели наложения и избавляет от необходимости использования адресации, маршрутизации и схем сигнализации ATM. Поскольку передача по адресу получателя основана скорее на топологии сети, а не на характере передаваемых потоков данных, применение такого подхода к ATM-коммутаторам не требует высокой скорости передачи при установке соединения, а также не зависит от долговечности потоков.

Применение коммутации MPLS в ATM-коммутаторе не препятствует поддержке на том же коммутаторе традиционной панели управления ATM (такой как PNNI).

Эти два компонента, MPLS и панель управления ATM, используют отдельные пространства VPI/VCI и другие ресурсы и не взаимодействуют друг с другом.

Иерархическая маршрутизация

Существенным для MPLS-коммутации является понятие связывания метки и маршрута сетевого уровня. Коммутация MPLS поддерживает широкий диапазон вариантов пересылки [UA23], что обеспечивает высокую степень масштабируемости, одновременно с разнообразием функций маршрутизации. Как крайний вариант метка может быть ассоциирована (связана) со всеми объявленными в IP-сети маршрутами граничного маршрутизатора при посредстве протокола BGP. Как показано в настоящем разделе, эта функция MPLS может быть успешно использована для построения высокомасштабируемых IP-сетей,

В архитектуре IP-маршрутизации сеть представляется в виде группы доменов маршрутизации. Внутри домена маршрутизация осуществляется по внутреннему протоколу (например, OSPF), а между доменами — по внешнему протоколу (к примеру, BGP). Однако все маршрутизаторы внутри доменов, через которые передаются транзитные потоки данных (в частности, внутри доменов, созданных провайдерами Internet), должны поддерживать не только внутреннюю, но и внешнюю маршрутную информацию.

MPLS отделяет внутреннюю и внешнюю маршрутизацию друг от друга, в результате чего обрабатывать внешнюю маршрутную информацию приходится только LSR-устройству, расположенному на границе домена. Остальные коммутаторы домена поддерживают только внутреннюю маршрутную информацию домена, объем которой обычно меньше, чем объем внешней маршрутной информации. Это, в свою очередь, уменьшает нагрузку по обработке маршрутов на базовых коммутаторах и сокращает время конвергенции протокола маршрутизации.

Для поддержки этих функций граничные LSR-устройства не назначают меток отдельным BGP-маршрутам, а повторно используют метки, назначенные BGP-узлам следующего перехода для всех BGP-пунктов назначения, к которым можно получить доступ через них, как показано на рис. 32.8.

На этом рисунке показана небольшая сеть ISP-провайдера, который имеет несколько маршрутизаторов, являющихся точками присутствия (Point-of-Presence — POP), подсоединенными к базовой сети, образованной тремя LSR-устройствами. Эта сеть также подсоединена к одноранговой точке (в данном примере MAE-East), через которую она получает маршрут к сети 192.168.3.0/24. Пересылка IP-пакетов от POP-маршрутизатора к внешнему пункту назначения по сети 192.168.3.0/24. (или по любому другому маршруту, объявленному точкой MAE-East с помощью протокола BGP) осуществляется как описано ниже.

Этап 1: маршрутизатор, выполняющий функции точки присутствия POP, получает IP-дейтаграмму для пункта назначения 192.168.3.0/24 в IP-сети.

Этап 2: POP-маршрутизатор выполняет просмотр информации 3-го уровня, вставляет перед IP-дейтаграммой заголовок метки MPLS и пересылает пакет маршрутизатору следующего перехода. Следует отметить, что метка в заголовке указывает на BGP-маршрутизатор, следующего перехода, а не на внешнюю IP-сеть.

Этап 3: базовое LSR-устройство Core-1 пересылает помеченный пакет в направлении пункта назначения, указанного в стеке меток MPLS, т.е. на BGP-маршрутизатор следующего перехода.

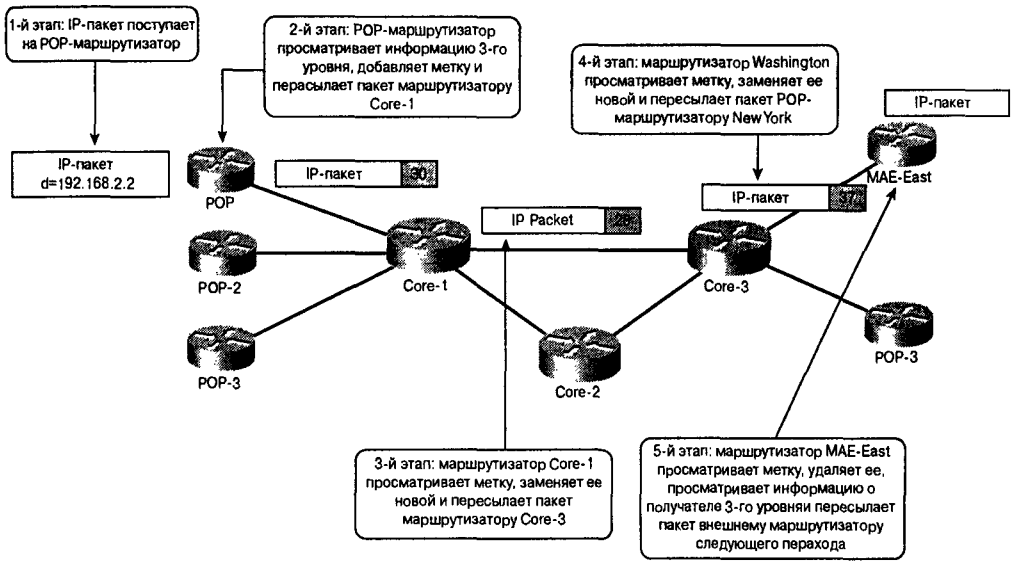


Рис. 32.8. MPLS-пересылка по IP-магистрали, работающей по протоколу BGP

Этап 4: этот же процесс повторяется на базовом LSR-устройстве Core-3.

Этап 5: выходное граничное LSR-устройство (MAE-East) удаляет заголовок метки MPLS, просматривает информацию 3-го уровня и пересылает IP-дейтаграмму в направлении внешнего пункта назначения.

Во время всего этого процесса базовое LSR-устройство вообще не просматривает информацию 3-го уровня об IP-адресе внешнего пункта назначения. Таким образом нет необходимости в работе протокола BGP на базовых LSR-устройствах, что уменьшает потребность в памяти и нагрузку на центральный процессор CPU, одновременно повышая устойчивость базовой сети.

Виртуальные частные сети на основе коммутации MPLS

Одним из наиболее популярных приложений коммутации MPLS является реализация на ее основе виртуальных частных сетей (Virtual Private Network — VPN). Для поддержки VPN-сетей на основе MPLS операционная система IOS Cisco была модифицирована в целях поддержки на одном маршрутизаторе большого количества независимых таблиц IP-маршрутизации, т.е. одной глобальной таблицы IP-маршрутизации и нескольких таблиц виртуальной маршрутизации и пересылки (Virtual Routing and Forwarding — VRF). Как показано на рис. 32.9, каждая VRF-таблица использует свой набор протоколов маршрутизации, и в отношении IP-маршрутизации функционирует как независимый маршрутизатор. Отметим, однако, что с точки зрения управления сетью весь маршрутизатор рассматривается как одно устройство. Такая полная независимость VRF-таблиц маршрутизации позволяет использовать в VPN-сетях перекрывающиеся пространства IP-адресов. Например, обе сети, VPN-A и VPN-B, могут использовать адрес 10.0.0.0/8.

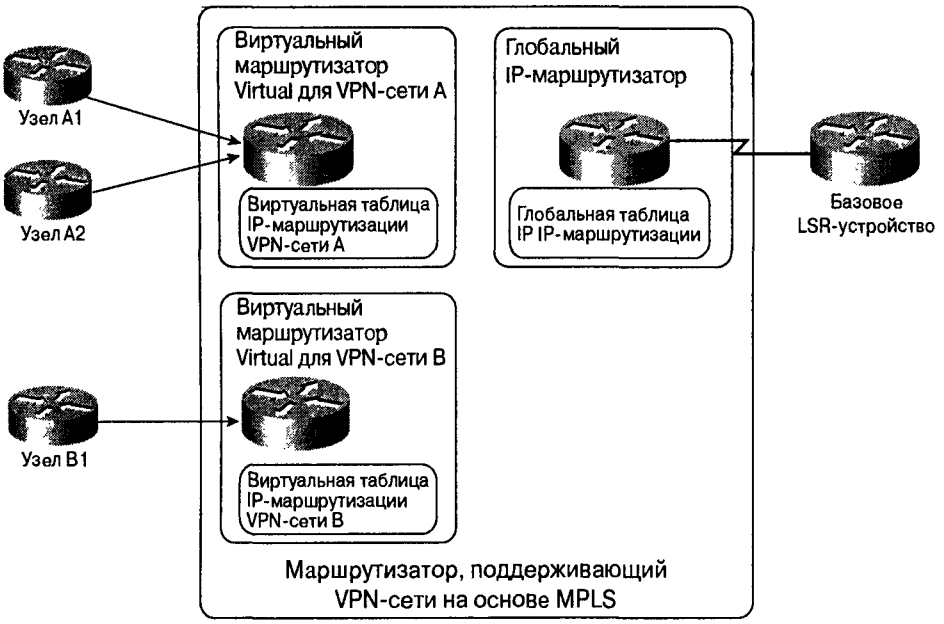


Рис.32.9. Архитектура VRF

Возможность наложения друг на друга адресных пространств пользователей VPN-сетей не позволяет использовать в архитектуре VPN MPLS обычный принцип пересылки используемый в иерархической IP-маршрутизации. В этой ситуации требуется более сложный подход с использованием стека меток (рис. 32.10). Этот стек состоит из двух меток:

- Верхняя метка (на рисунке обозначена как IL или IGP), указывающая на граничное LSR-устройство, назначается протоколом LDP.
- Нижняя метка (на рисунке обозначена как VL или VPN), указывающая на VPN-получателя, назначается выходным граничным LSR-устройством и непосредственно передается граничному LSR-устройству на другом конце сети по протоколу многопротокольного граничного шлюза (multiprotocol BGP).

Пакет, отправленный с узла A1 узлу A2, пересылается по MPLS-магистрали VPN-сети. Эта пересылка включает в себя несколько этапов, описанных ниже.

Этап 1: IP-дейтаграмма посылается с узла A1 на входной маршрутизатор.

Этап 2: входной маршрутизатор просматривает IP-адрес и вставляет в начале дейтаграммы заголовок MPLS, состоящий из двух меток — метки, назначенной протоколом LDP (метка протокола IGP [IL]), задающей маршрут к выходному маршрутизатору, и метку VPN-сети (VL), назначенную выходным маршрутизатором.

Этап 3: предпоследний базовый маршрутизатор (маршрутизатор Core на рис. 32.10) в сети провайдера службы удаляет метку IGP, оставляя в заголовке MPLS только метку VPN-сети.

Этап 4: выходной маршрутизатор просматривает метку VPN-сети, удаляет заголовок MPLS и пересылает IP-дейтаграмму в направлении узла A2.

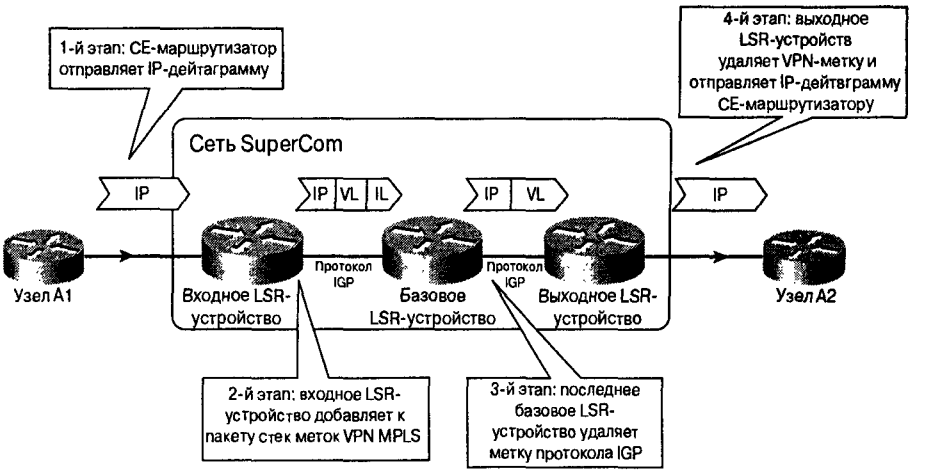


Рис. 32.10. Пересылка пакета в VPN-сети на базе MPLS

Качество обслуживания в сетях коммутации MPLS

Важной особенностью коммутации MPLS является возможность поддержки качества обслуживания QoS. Для этого на маршрутизаторе или коммутаторе, осуществляющем пересылку по тегам, используются два описанных ниже механизма.

- Классификация пакетов и отнесение их к различным классам.
- Обрабатывая пакеты в соответствии с их QoS-характеристиками (такими как полоса пропускания или возможность отбрасывания) коммутация MPLS предоставляет простой способ помечать пакеты, как принадлежащие к определенному классу, после того как они уже были однажды классифицированы. При первоначальной классификации используется информация, передаваемая в заголовках сетевого или более высокого уровня. Маркировка пакетов может быть выполнена двумя способами:
  - — В среде ATM метка, соответствующая результирующему классу, присваивается пакету. Помеченные пакеты могут эффективно обрабатываться LSR-устройствами на протяжении всего маршрута без повторной классификации.
  - — Во всех остальных средах приоритет пакета передается в 3-х битах заголовка метки MPLS.

Реальные очередность и расписание пакета как правило ортогональны. Ключевым фактором является то, что коммутация MPLS позволяет использовать простую логику для нахождения состояния, которое определяет способ установки пакета в очередь.

Перераспределение потоков в MPLS-сетях

Одним из фундаментальных свойств маршрутизации по адресу получателя является то, что для передачи пакетов в пункт назначения используется только информация об адресе получателя. Хотя это свойство обеспечивает высокую степень масштабируе-

мости, оно также ограничивает возможности влияния на действительный путь прохождения пакетов. Это уменьшает возможность равномерного распределения потоков между линиями связи, чтобы разгрузить одни каналы и передать часть потоков данных на другие, менее загруженные каналы.

Для провайдеров Internet, предоставляющих службы различных классов, маршрутизация по адресу получателя ограничивает возможности распределения различных классов между используемыми каналами. В настоящее время для того, чтобы обойти ограничения, налагаемые таким типом маршрутизации, некоторые Internet-провайдеры используют технологии Fame Relay или ATM. Благодаря возможности передачи различных групп пакетов с метками MPLS позволяет преодолеть эти ограничения без использования Fame Relay или ATM. Чтобы обеспечить передачу по маршрутам, отличным от тех, которое определяются маршрутизацией по адресу получателя, компонент управления MPLS позволяет устанавливать связывание меток в LSR-устройствах, не соответствующие маршрутам, определенным по адресу получателя.

Перераспределение потоков позволяет сетевому администратору создавать собственный маршрут, не совпадающий с обычными маршрутами, вычисленными по алгоритмам последовательной маршрутизации. Администратор может явно определить путь между станциями, чтобы обеспечить заданное QoS или уменьшить нагрузку на некоторые узлы. Иными словами, администратор может ликвидировать уменьшить степень переполнения, направив фреймы в обход перегруженных сегментов. Таким образом, перераспределение потоков позволяет администратору определить политику передачи фреймов, не зависящую от динамических протоколов маршрутизации.

Перераспределение потоков похоже на маршрутизацию по адресу источника тем, что позволяет определить явный маршрут прохождения фрейма. Однако, в отличие от маршрутизации по адресу источника, последовательное определение переходов не передается с каждым фреймом. Вместо этого узлы конфигурируются в LSR-устройстве заранее, с соответствующими значениями меток.

Несколько существующих протоколов были модифицированы для поддержки перераспределения потоков MPLS:

- Были определены расширения протоколов OSPF и IS-IS для того, чтобы эти протоколы состояния канала могли распространять по сети информацию о загруженности канала.
- В операционной системе IOS Cisco была реализована основанная на ограничениях маршрутизация, позволяющая высокопроизводительным маршрутизаторам находить в сети оптимальные маршруты на основе заданных оператором сети критериев.
- Протокол резервирования ресурсов (Resource Reservation Protocol — RSVP) был расширен для поддержания установки задаваемых явным образом LSP-маршрутов.

Резюме

Многопротокольная коммутация по меткам (Multiprotocol Label Switching — MPLS) представляет собой технологию, объединяющую преимущества ориентированной на соединение пересылки 2-го уровня с достоинствами протокола Internet (Internet Protocol — IP) 3-го уровня. В сетях с функциями MPLS все сетевые устройства оказываются способными выполнять функции протокола IP. На их управляющей

плоскости функционируют IP-протоколы маршрутизации, однако реальная пересылка пакетов происходит на основе меток, выделяемых IP-префиксам различными протоколами распространения меток. Возможность выполнять пересылку внутри базовой IP-сети не выполняя просмотр IP-адресов на каждом переходе позволяет реализовать ряд новых решений, описанных ниже.

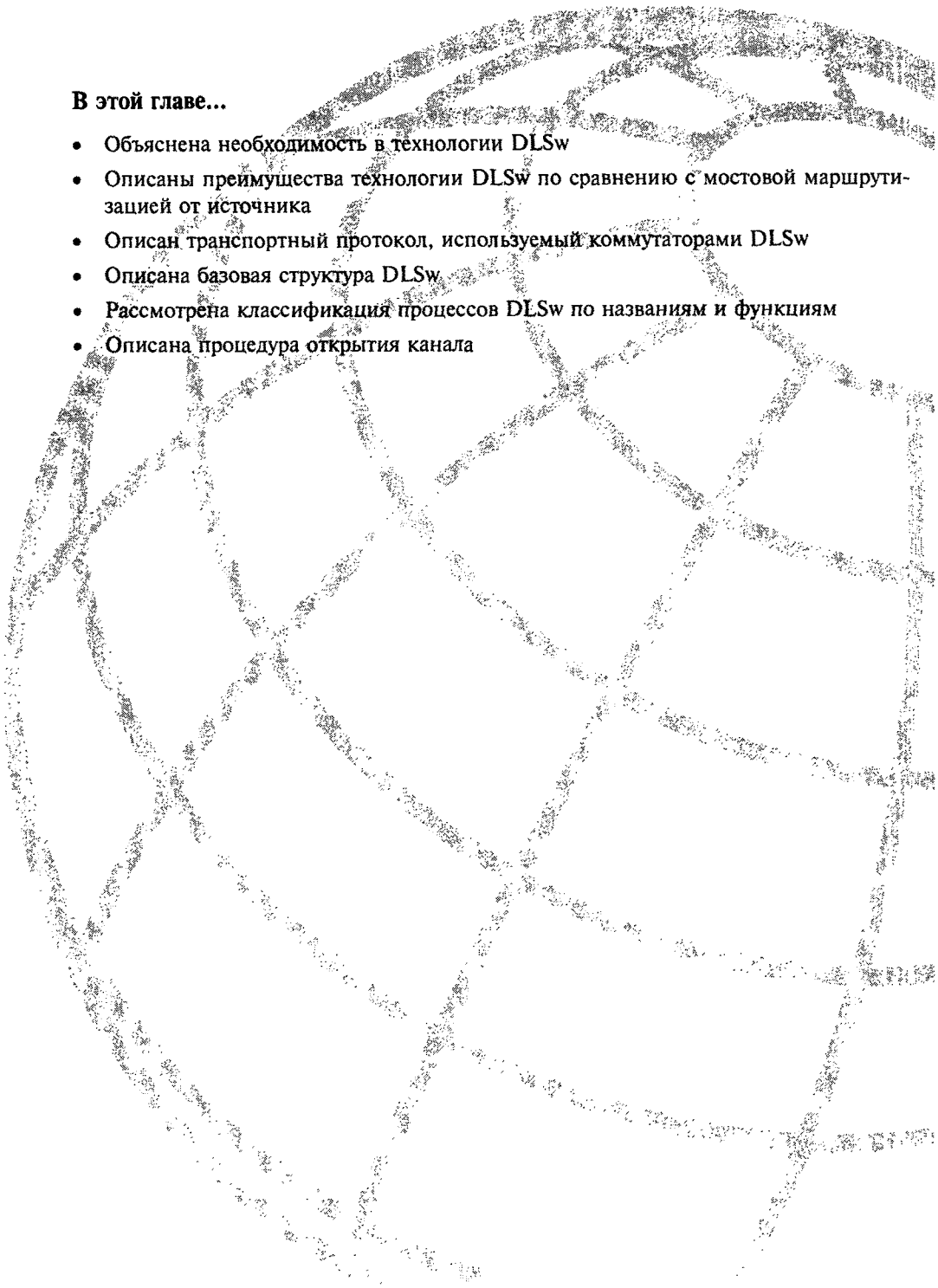
- Выполнение межсетевой маршрутизации (Internet routing) со значительно уменьшенным объемом таблиц IP-маршрутизации на базовых маршрутизаторах;
- Перераспределение потоков на основе соответствующих функций MPLS (MPLS-based traffic engineering — MPLS TE);
- Виртуальные частные сети на основе MPLS.

Контрольные вопросы

1. Каким образом при распределении исходящего потока по требованию находящееся в восходящем направлении LSR-устройство узнает, что ему нужна метка?
2. FIB представляет собой информационную базу пересылки (Forwarding Information Base). Чем она отличается от LFIB — информационной базы пересылки по метке (Label Forwarding Information Base)?
3. Каковы два режима работы протокола LDP?
4. Рекомендуется, чтобы соседние LSR-устройства работали в одном режиме протокола LDP. Что произойдет, если находящееся в восходящем направлении LSR-устройство работает в режиме распределения исходящего потока без запроса, а выходное LSR-устройство — в режиме запрашиваемого исходяшего потока?
5. Если маршрутизатор производителя уже использует высокоскоростную коммутацию и кэширование для передачи фреймов, то производительность не является достаточным мотивом для использования коммутации MPLS. Существуют ли иные причины, которые могут сделать целесообразным внедрение MPLS в такой сети?

Дополнительные источники

- McDysan, David, Ph.D. *QoS and Traffic Management in IP and ATM Networks.* McGraw-Hill Professional Publishing: New York, 2000.
- Pepelnjak, Ivan, Jim Guishard and Jeff Apcar, *Advanced MPLS and VPN Architectures*, Volume II, Cisco Press, 2003.
- Pepelnjak, Ivan, and Jim Guishard, *MPLS and VPN Architectures*, CCIP Edition, Cisco Press, 2002.
- Вивек Олвейн, *Структура и реализация современной технологии MPLS.* ИД "Вильямс", 2004.
- http://www.cisco.com/warp/public/732/Tech/mpls/
- http://www.ietf.org/html.charters/mpls-charter.html
- http://www.ietf.org/rfc/rfc2702.txt
- http://www.mplsrc.com/



В этой главе...

- Объяснена необходимость в технологии DLSw
- Описаны преимущества технологии DLSw по сравнению с мостовой маршрутизацией от источника
- Описан транспортный протокол, используемый коммутаторами DLSw
- Описана базовая структура DLSw
- Рассмотрена классификация процессов DLSw по названиям и функциям
- Описана процедура открытия канала

Глава 33

Технология DLSw

Введение

Технология *коммутации каналов (Data-Link Switching — DLSw)* является способом передачи данных протоколов SNA IBM и NetBIOS по IP-сетям. Она служит альтернативой алгоритму *мостовой маршрутизации от источника* (Source-Route Bridging — SRB), широко применявшемуся до появления технологии DLSw для передачи данных протоколов SNA и NetBIOS в сетях Token Ring. В целом технология DLSw предназначена для выполнения некоторых коммуникационных требований, которые не удается удовлетворить при помощи маршрутизации SRB, особенно в глобальных сетях. В этой главе выполняется сравнение технология DLSw и SRB, описываются лежащие в их основе протоколы, а также дается краткий обзор их стандартных операций.

Технология DLSw впервые появилась в 1992 г. как фирменная разработка корпорации IBM. В 1993 г. она была передана на рассмотрение комитета IETF как RFC 1434. DLSw подробно описана в RFC 1795 IETF, выпущенном в апреле 1995 г. Технология DLSw является совместной разработкой исследовательских групп Advanced Peer-to-Peer Networking (APPN) Implementors Workshop (AIW) и Data-Link Switching Related Interest Group (DLSw RIG).

В RFC 1795 описаны три основные функции DLSw приведенные ниже.

- Поддержка протокола "коммутатор-коммутатор" (Switch-to-Switch Protocol — SSP) представляет собой протокол соединения между двумя узлами или маршрутизаторами DLSw.
- Подтверждение SNA-соединений DLC для снижения вероятности простоев на канальном уровне в глобальных сетях.
- Локальное преобразование соединений DLC в каналы DLSw.

Каждая из этих функций будет подробно описана ниже.

В 1997 г. группа IETF выпустила стандарт DLSw 2 (RFC 2166), куда вошли улучшения документа RFC 1795. К имеющимся возможностям DLSw добавились следующие:

- групповая адресация IP (многоадресатная рассылка);
- одноадресные ответы протокола UDP на широковещательные запросы DLSw;
- усовершенствованная маршрутизация для соединения по требованию (peer-on-demand);
- срочные TCP-соединения.

Все эти свойства позволяют использовать DLSw как масштабируемую технологию для глобальных сетей. В DLSw 1 транзакции осуществляются по протоколу TCP. Поэтому многие операции в среде DLSw занимают каналы между узлами. Например, для групповой адресации требуется несколько TCP-соединений между источником и каждым узлом. Во второй версии DLSw многоадресатная расылка осуществляется путем негарантированной доставки традиционными методами групповой адресации.

Следует обратить внимание на то, что RFC 2166 не заменяет RFC 1795, а расширяет его функциональные возможности и обеспечивает обратную совместимость.

Операционная система Cisco поддерживает третью версию DLSw, получившую название DLSw+. DLSw+ появилась раньше DLSw 2 и имела даже больше усовершенствований по сравнению с базовой версией DLSw. DLSw+ полностью соответствует RFC 1795. Ее улучшения могут использоваться в том случае, если оба узла являются устройствами Cisco, поддерживающими DLSw+.

В настоящей главе основное внимание уделяется базовым функциям DLSw, описанным в RFC 1795.

Общая структура среды DLSw показана на рис. 33.1.

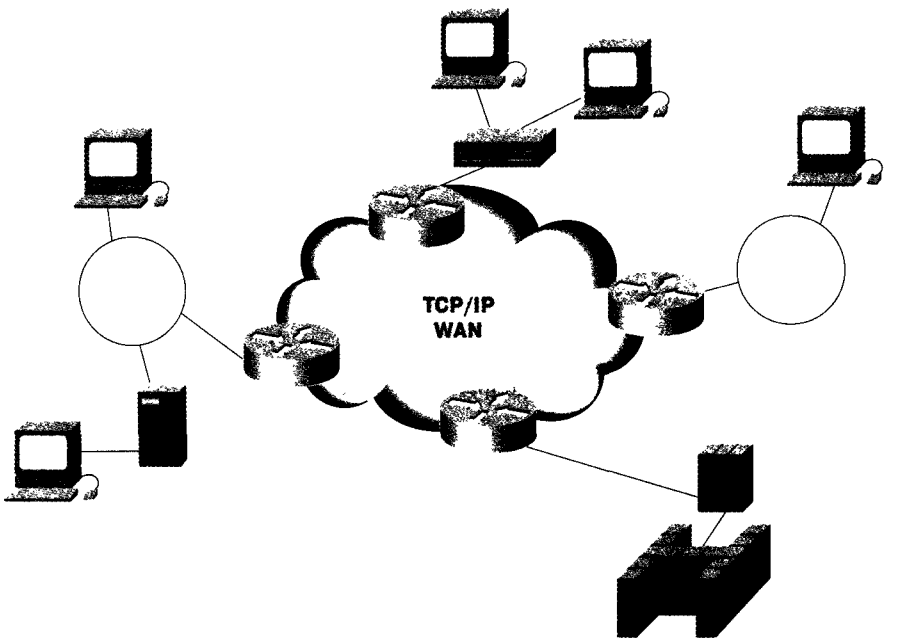


Рис. 33.1. Канал DLSw упрощает обмен данными SNA в глобальных IP-сетях

Сравнение DLSw и SRB

Принципиальная разница между технологиями SRB и DLSw заключается в возможности локального подтверждения соединения. Объем потоков данных протоколов SNA и NetBIOS зависит от подтверждений канального уровня и "пустых" сообщений, свидетельствующих о поддержке соединения и доставке данных. Если данные ориентированы на соединение, то локальный узел или маршрутизатор DLSw прерывают ка-

нальное управление. Поэтому подтверждения канального уровня и "пустые" сообщения не должны передаваться по глобальной сети. Однако по алгоритму SRB управление передачей данных является сквозным, в результате чего увеличивается вероятность простоев при соединениях по глобальной сети.

Хотя SRB во многих случаях является жизнеспособной технологией, некоторые недостатки ограничивают ее применение для передачи данных по протоколам SNA и NetBIOS в глобальной сети. Главными среди них являются следующие ограничения:

- количество узлов SRB не должно превышать семи.
- возможна обработка только широковещательных фреймов (фреймов анализатора SRB или запросов имен NetBIOS).
- передача излишних сообщений (подтверждения и "пустые" сообщения).
- отсутствие управления потоком и системы приоритетов.

На рис. 33.2 изображена схема сквозного SRB-соединения по глобальной сети.

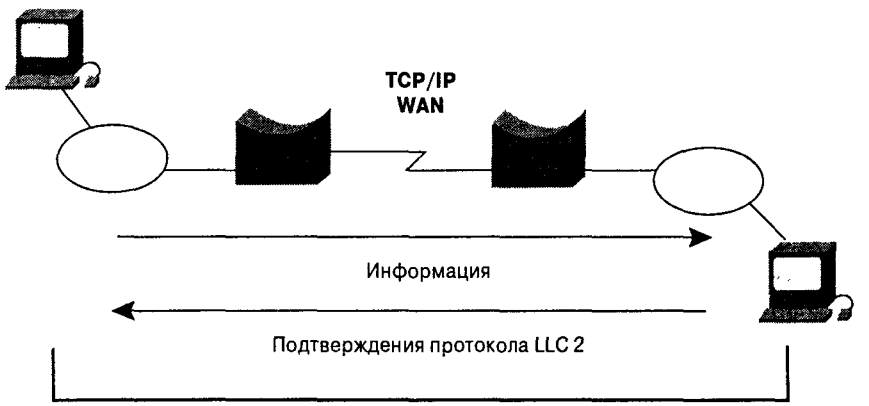


Рис. 33.2. Сквозное SRB-соединение по глобальной сети TCP/IP

Локальное подтверждение соединений DLC в технологии DLSw дает ряд преимуществ по сравнению с системами SRB. Благодаря локальному подтверждению данные DLSw могут передаваться по глобальной сети без подтверждений канального уровня и "пустых" сообщений. Кроме того, локальное подтверждение снижает вероятность простоев на канальном уровне в глобальных сетях. Аналогичным образом в DLSw гарантируется, что широковещательные рассылки поисковых фреймов будут управляться средствами DLSw после того, когда будет найден адрес нужной системы. На рис. 33.3 показана передача сообщений и использование локальных подтверждений в среде DLSw.

Поддержка SNA в технологии DLSw

Одним из преимуществ технологии DLSw является поддержка более широкого по сравнению с SRB диапазона устройств и сред. DLSw работает в нескольких типичных

средах SNA и поддерживает локальные сети IEEE 802.2 с физическими модулями SNA PU 2, PU 2.1 и PU 4, а также системы на основе NetBIOS.

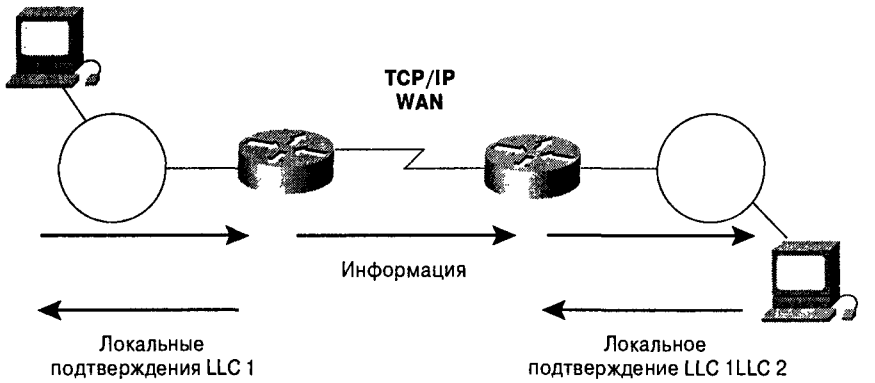


Рис. 33.3. В DLSw для управления потоком данных используется локальное подтверждение

DLSw поддерживает протокол синхронного управления передачей данных (Synchronous Data Link Control — SDLC), включая системы PU 2 (первичные и вторичные) и PU 2.1. В системах SDLC каждое физическое устройство (Physical Unit — PU) протокола SDLC представляется протоколу DLSw SSP в виде уникальной пары адресов управления доступом к среде передачи (MAC) и точки доступа к серверу (SAP). В системах Token Ring узел DLSw является мостом маршрутизации от источника. Удаленные системы Token Ring при соединении через DLSw-узел рассматриваются как смежные кольца. Такое мнимое смежное кольцо, называемое виртуальным, создается для каждого узла DLSw. На рис. 33.4 показаны различные узлы IBM, связанные с глобальной сетью TCP/IP через устройства DLSw, в данном случае маршрутизаторы.

Протокол SSP

Протокол "коммутатор-коммутатор" (Switch-to-Switch Protocol — SSP) представляет собой протокол, используемый узлами DLSw (маршрутизаторами) для того, чтобы устанавливать соединения, определять местонахождение ресурсов, передавать данные, управлять потоком данных и устранять ошибки. В этом протоколе фактически заключается основа технологии DLSw. Вообще говоря, протокол SSP не обеспечивает полной маршрутизации между узлами, поскольку этим в основном занимаются общие протоколы маршрутизации, такие как RIP, OSPF и IGRP/EIGRP. Вместо этого протокол SSP коммутирует пакеты на канальном уровне SNA, а также инкапсулирует пакеты в протокол TCP/IP для передачи по IP-сетям и использует протокол TCP как способ надежной передачи данных между узлами DLSw. На рис. 33.5 показано место SSP в общей архитектуре SNA, а также соответствие SSP эталонной модели OSI.

Функционирование DLSw

Коммутация каналов DLSw включает в себя нескольких этапов. Одноранговые устройства DLSw устанавливают между собой TCP-соединения. Эти TCP-соединения являются основой для обмена данными DLSw. Поскольку TCP обеспечивает надежную и гаранти-

руемую доставку данных протокола IP, а также их инкапсуляцию в формат протокола — в данном случае соответствующий протоколам NetBIOS и SNA, данные передаются с гарантией доставки и целостности. После установления соединения одноранговые устройства DLSw сообщают друг другу о поддерживаемых функциях. Это особенно важно в том случае, когда DLSw-узлы изготовлены различными производителями. После этого одноранговые DLSw-устройства устанавливают каналы между конечными системами SNA или NetBIOS, по которым можно передавать информационные фреймы.

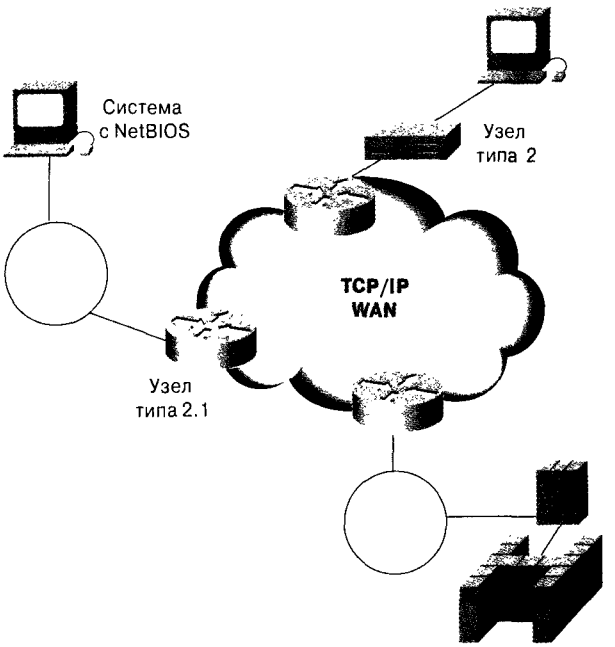


Рис. 33.4. SNA-узлы связаны через глобальную сеть TCP/IP при помощи DLSw

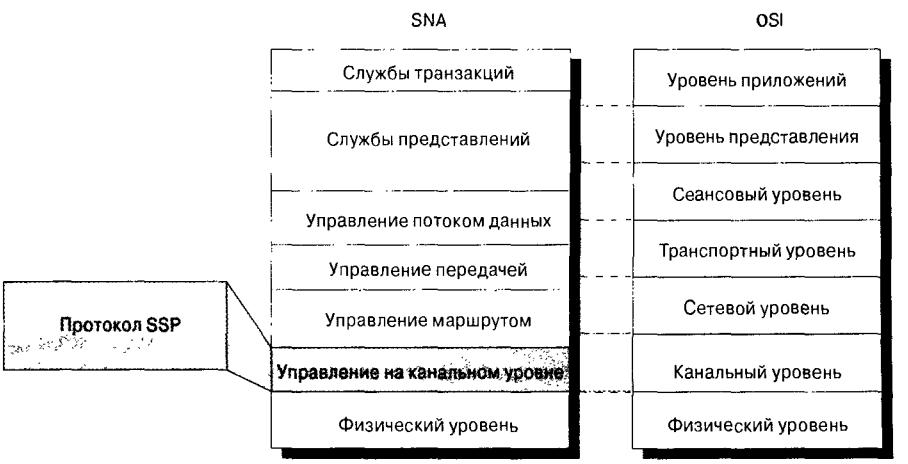


Рис. 33.5. Протокол SSP устанавливает соответствие между компонентами канального уровня SNA и эталонной моделью OSI

Процессы DLSw

Функционирование DLSw можно разделить на три основных компонента: обмен сведениями о функциях, открытие канала и управление потоком. Для DLSw *обмен сведениями о функциях* означает обмен информацией о возможностях сеанса DLSw. Этот обмен осуществляется в начале сеанса и в его процессе. *Открытие канала* в DLSw происходит между конечными системами. Оно заключается в определении местонахождения системы-получателя и установке управляющих канальных соединений между конечными системами и их локальным маршрутизатором. *Управление потоком* в DLSw позволяет установить независимое однонаправленное управление потоком между одноранговыми устройствами. Более подробно эти процессы будут описаны ниже.

Обмен сведениями о функциях DLSw

Обмен сведениями о функциях DLSw основан на управляющем сообщении "коммутатор-коммутатор", в котором описываются возможности коммутатора-источника. Управляющее сообщение обмена сведениями о функциях посылается после установки соединения между коммутаторами или, в случае изменения некоторых рабочих параметров, о котором нужно сообщить коммутатору-партнеру, — во время обмена данными. При таком обмене идентифицируются и согласуются некоторые возможности. Одноранговые DLSw-устройства обмениваются следующими сведениями:

- номер версии DLSw;
- начальный размер окна приема;
- поддержка NetBIOS;
- список поддерживаемых каналов SAP (Link SAP — LSAP);
- количество поддерживаемых сеансов TCP;
- списки MAC-адресов;
- списки имен NetBIOS;
- поддержка поисковых фреймов.

Открытие канала DLSw

Процесс открытия канала DLSw между двумя конечными системами состоит из определения местонахождения системы-получателя и установки соединения для управления на канальном уровне (DLC) между конечными системами и их локальными маршрутизаторами. Специальные сообщения об открытии канала зависят от типа передаваемых данных.

Одна из основных функций DLSw состоит в предоставлении механизма транспортировки данных протокола SNA. Как показано на рис. 33.6, открытие SNA-канала включает в себя несколько этапов.

Сначала SNA-устройства в локальной сети находят другие SNA-устройства, посылая служебный фрейм с MAC-адресом SNA-получателя. Когда узел DLSw, обеспечивающий межсетевой обмен, принимает служебный фрейм, он посылает своим одноранговым устрйствам DLSw фрейм *canureach* (от англ. can you reach — "кто может со мной связаться?"). Назначение этого фрейма состоит в том, чтобы запросить все одноранговые устрйства DLSw, могут ли они определить местонахождение искомого

устройства. Если какое-либо из таких устройств DLSw имеет доступ к указанному MAC-адресу, то оно посылает фрейм *icanreach* (от англ. I can reach — "я могу связаться"), которое означает, что имеется одноранговое устройство DLSw, которое может обеспечить канал связи с данным устройством.

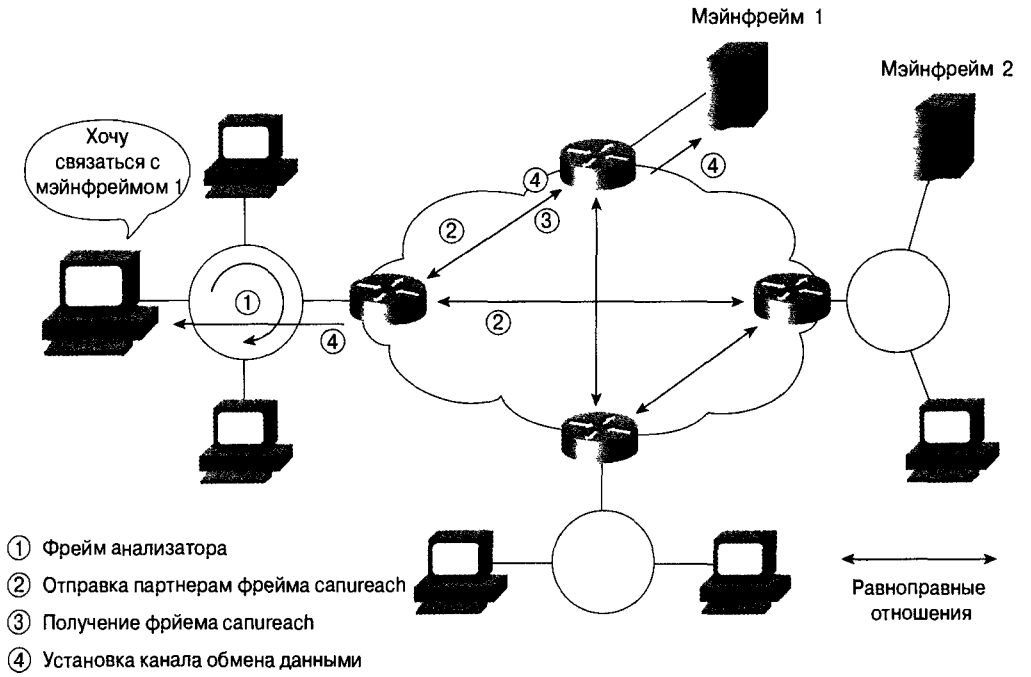


Рис. 33.6. Поток открытия канала DLSw

После обмена фреймами canureach и icanreach одноранговые устройства DLSw открывают между собой канал из DLC-соединений между каждым маршрутизатором и локально связанной с ним конечной SNA-системой (не более двух соединений) и TCP-соединения между одноранговыми устройствами DLSw. Получившийся канал однозначно определяется идентификаторами источника и получателя. Каждый SNA-идентификатор DLSw-канала состоит из MAC-адреса, точки доступа к службе канала (Link-Service Access Point — LSAP) и идентификатора порта DLC. Приоритет канала определяется при его открытии.

Процедура открытия канала NetBIOS очень похожа на открытие канала SNA, с незначительными отличиями. Главное из них заключается в том, что при открытии канала NetBIOS узлы DLSw посылают запрос Name Query, где указывается имя NetBIOS (а не запрос canureach, определяющий MAC-адрес). В ответ DLSw-узлы, открывающие канал NetBIOS, вместо сообщения icanreach посылают сообщение "имя опознано" (recognized name query).

Управление потоком DLSw

Управление потоком DLSw подразумевает *адаптивное пошаговое продвижение* между DLSw-маршрутизаторами. При согласовании управления потоком между одноранговыми устройствами DLSw устанавливаются два независимых однонаправленных

механизма управления потоком. Адаптивное пошаговое продвижение использует механизм управления окнами, который динамически адаптируется к доступности буфера. Окна можно увеличивать, уменьшать, делить пополам и закрывать. Это позволяет DLSw-узлам управлять пошаговым продвижением потоков данных, пересылаемых по сети, и гарантирует их целостность и доставку.

Индикаторы управления потоком DLSw

Количество *разрешенных модулей* (модулей, которые отправитель имеет право послать) (granted units) получатель может увеличить при помощи одного из индикаторов управления потоком. Управление потоком DLSw осуществляется с помощью приведенных ниже функций индикаторов.

- **Повторение.** Увеличить количество разрешенных модулей до текущего размера окна.
- **Инкрементация.** Увеличить размер окна на 1 и адаптировать количество разрешенных модулей к новым размерам окна.
- **Декрементация.** Уменьшить размер окна на 1 и адаптировать количество разрешенных модулей к новым размерам окна.
- **Закрытие.** Закрыть окно и уменьшить количество разрешенных модулей до 0, т.е. полностью прекратить передачу в данном направлении, пока не будет послан индикатор инкремента.
- **Разделить пополам.** Уменьшить размер окна вдвое и адаптировать количество разрешенных модулей к новым размерам окна.
- **Управление потоком.** Индикаторы и подтверждения управления потоком могут передаваться вместе с информационными пакетами или высылаться отдельно как независимые управляющие сообщения. Индикаторы закрытия всегда посылаются в виде отдельных сообщений.

Примеры адаптивного пошагового продвижения

В качестве примеров критериев адаптивного пошагового продвижения можно привести доступность буфера, загрузку канала, длину выходной очереди и приоритет потока данных. Ниже приведены примеры того, как с помощью этих критериев можно влиять на пошаговое продвижение.

- **Доступность буфера.** Если размеры буферов памяти в DLSw-узле уменьшаются до критических пределов, то узел может уменьшить размер окна, чтобы снизить скорость передачи данных. Когда доступность буфера увеличится, узел может увеличить размер окна для увеличения скорости передачи данных между одноранговыми устройствами DLSw.
- **Загрузка канала.** Если нагрузка на канал между DLSw-партнерами слишком велика, то можно уменьшить размер окна, чтобы снизить нагрузку на канал и предотвратить потери пакета между узлами.
- **Длина исходящей очереди.** Пакеты, передаваемые DLSw-узлом, обычно помещаются в выходную очередь. Эта область памяти выделена для данных, передаваемых одним устройством другому. Если размер очереди приближается к предельному или очередь переполняется, то можно сократить количество разрешенных модулей, пока заполнение очереди не вернется на приемлемый уровень.

- **Приоритет потока даиных.** Одна из уникальных возможностей протокола SSP состоит в его способности располагать потоки данных в соответствии с их приоритетом. Приоритет указывается в соответствующем поле фрейма сообщения DLSw. Изменяя количество разрешенных модулей для определенных каналов DLSw, узлы могут назначать каналам разные приоритеты.

Форматы DLSw-сообщений

Имеется два формата заголовков сообщений, передаваемых между DLSw-узлами:

- управляющие;
- информационные.

Заголовки управляющих сообщений вставляются во все сообщения, кроме информационных фреймов (Iframes) и независимых сообщений управления потоком (Independent Flow Control Message — IFCM). Эти сообщения имеют заголовки информационного формата.

Поля управляющего и информационного DLSw-форматов показаны на рис. 33.7. Их описание дается ниже.

На рис. 33.7 показаны следующие поля.

- **Номер версии.** Если это поле равно 0x31 (ASCII 1), т.е. 49 в десятичной системе счисления, то данное устройство идентифицируется как устройство, использующее DLSw 1. Впоследствии это поле обеспечит функциональную совместимость между узлами DLSw с разными версиями стандарта DLSw. В настоящее время все устройства соответствуют DLSw 1, так что пока десятичное значение данного поля всегда равно 49.
- **Длина заголовка.** Для управляющего сообщения это поле равно 0x48, что указывает на длину сообщения в 72 байта. Для информационных и независимых сообщений управления потоком значение этого поля равно 0x10, т.е. их длина составляет 16 байтов.
- **Длина сообщения.** Определяет количество байтов в поле данных, следующем за заголовком.
- **Удаленный канальный коррелятор и идентификатор удаленного DLC-порта.** Эти поля образуют 64-разрядный идентификатор канала, который однозначно идентифицирует DLC-канал в пределах DLSw-узла. Сквозной канал определяется парой собственных идентификаторов, которые, наряду с локальными канальными идентификаторами, однозначно определяют этот сквозной канал. В памяти каждого DLSw-узла хранится таблица таких пар идентификаторов: один — для локального, другой — для удаленного конца канала. Если в поле направления передачи фрейма содержится значение 0x01, то этой паре присваивается то же значение, что и у получателя, а если значение 0x02, то значение источника.
- **Тип сообщения.** Определяет тип сообщения DLSw. Значение задается в двух полях (14-й и 23-й байты) заголовка управляющего сообщения. При анализе полученного SSP-сообщения используется только первое поле. Второе поле в новых системах приема данных игнорируется, но сохраняется для обратной совместимости с версиями RFC 1434 и, если потребуется, может использоваться в будущих версиях.

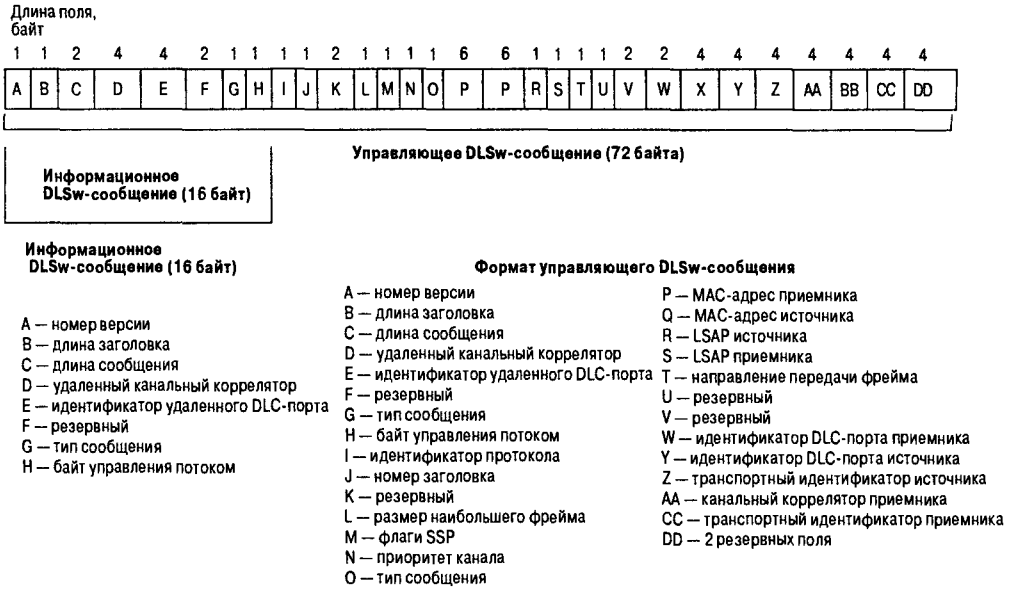


Рис. 33.7. Поля управляющего и информационного DLSw-форматов

- **Байт управления потоком.** Содержит индикатор управления потоком, подтверждение управления потоком и биты оператора управления потоком.
- **Идентификатор протокола.** Если значение данного поля равно 0x42, то оно соответствует десятичному значению 66.
- **Номер заголовка.** Если значение данного поля равно 0x01, то оно соответствует десятичному значению 1.
- **Максимальный размер фрейма.** Размер наибольшего из передаваемых по DLSw-соединению фреймов. Учет этого поля гарантирует, что две конечные станции согласуют между собой размер используемых в данном канале фреймов, который не потребует от DLSw-партнеров повторной сегментации фреймов.
- **Флаги SSP.** Дополнительная информация о SSP-сообщении. Определения флагов (бит 7 — старший, бит 0 — младший) показаны в табл. 33.1.

Таблица 33.1. Определения SSP-флагов

Бит	Название	Значение
7	SSPex	1 — служебное сообщение (canureach или icanreach)
6–0	Резервный	Отсутствует. Зарезервированные поля. Равны 0 при передаче и игнорируются при получении

- **Приоритет канала.** Три младших бита этого байта определяют один из приоритетов: не поддерживается, низкий, средний, высокий и наивысший. При открытии канала каждая конечная точка предоставляет своему партнеру по каналу информацию о приоритете. Инициатор канала выбирает, какой приоритет

будет эффективным для функционирования канала. Если узлы не используют приоритет, то в этом поле указывается значение "не поддерживается".

- **MAC-адрес получателя.** Вместе с SAP канала получателя, MAC-адресом и SAP канала источника определяет логическую сквозную ассоциацию, называемую идентификатором канала связи.
- **MAC-адрес источника.** MAC-адрес конечной станции-отправителя.
- **LSAP источника.** SAP исходного устройства. Используется для логического опознавания передаваемых данных.
- **LSAP получателя.** SAP устройства-получателя.
- **Направление передачи фреймов.** Для фреймов, посылаемых из DLSw-узла источника DLSw-получателю, это поле равно 0x01, а для фреймов, посылаемых из DLSw-узла получателя DLSw-источнику, — 0x02.
- **Длина DLC-заголовка.** Если это поле равно 0 для дейтаграмм SNA и 0x23 для дейтаграмм NetBIOS, то оно означает длину заголовка в 35 байтов. Заголовок NetBIOS содержит следующую информацию:
  - — поле управления доступом (Access Control — AC);
  - — поле управления фреймами (Frame Control — FC);
  - — MAC-адрес получателя (Destination MAC Address — DA);
  - — MAC-адрес источника (Source MAC Address — SA);
  - — маршрутная информация (Routing Information — RI); дополняется до 18 байтов);
  - — SAP получателя (DSAP);
  - — SAP источника (SSAP);
  - — поле управления LLC (UI).
- **Канальный коррелятор и идентификатор DLC-порта источника.** Образуют 64-разрядный идентификатор канала, который однозначно определяет DLC-канал в пределах данного DLSw-узла. Сквозной канал идентифицируется парой собственных идентификаторов, которые вместе с канальными идентификаторами однозначно определяют данный сквозной канал. В памяти каждого DLSw-узла должна храниться таблица этих пар идентификаторов: одна — для локальной, а другая — для удаленной конечной станции канала.
- **Транспортный идентификатор источника.** Определяет порт TCP/IP в DLSw-узле в пределах данной локальной сети. Каждый DLSw-узел, отправляя сообщения DLSw-партнеру, должен преобразовывать эти значения, а также ассоциированные значения для идентификатора порта DLC и канального коррелятора.
- **Канальный коррелятор получателя.** Вместе с идентификатором DLC-порта получателя образует 64-разрядный идентификатор канала, который однозначно определяет DLC-канал в пределах данного DLSw-узла. Сквозной канал идентифицируется парой собственных идентификаторов, которые вместе с канальными идентификаторами однозначно определяют данный сквозной канал. В памяти каждого DLSw-узла должна храниться таблица этих пар идентификаторов: одна для локальной, а другая для удаленной конечной станции канала.
- **Транспортный идентификатор.** Определяет порт TCP/IP в DLSw-узле в пределах данной локальной сети. Каждый DLSw-узел, отправляя сообщения DLSw-

партнеру, должен преобразовывать эти значения, а также ассоциированные значения для идентификатора порта DLC и канального коррелятора.

Контрольные вопросы

1. DLSw обеспечивает подтверждение на канальном уровне. Что означает подтверждение на канальном уровне? В чем его преимущества?
2. Какой транспортный протокол используется для передачи данных протокола SSP DLSw? Каковы его преимущества и недостатки?
3. Назовите и опишите три этапа работы DLSw.
4. Какие протоколы поддерживает DLSw?
5. Что такое стандартный процесс 2-уровня, используемый без DLSw?
6. В DLSw используются два типа сообщений. Каковы эти сообщения и у какого из них заголовок больше? Есть ли между ними что-либо общее?

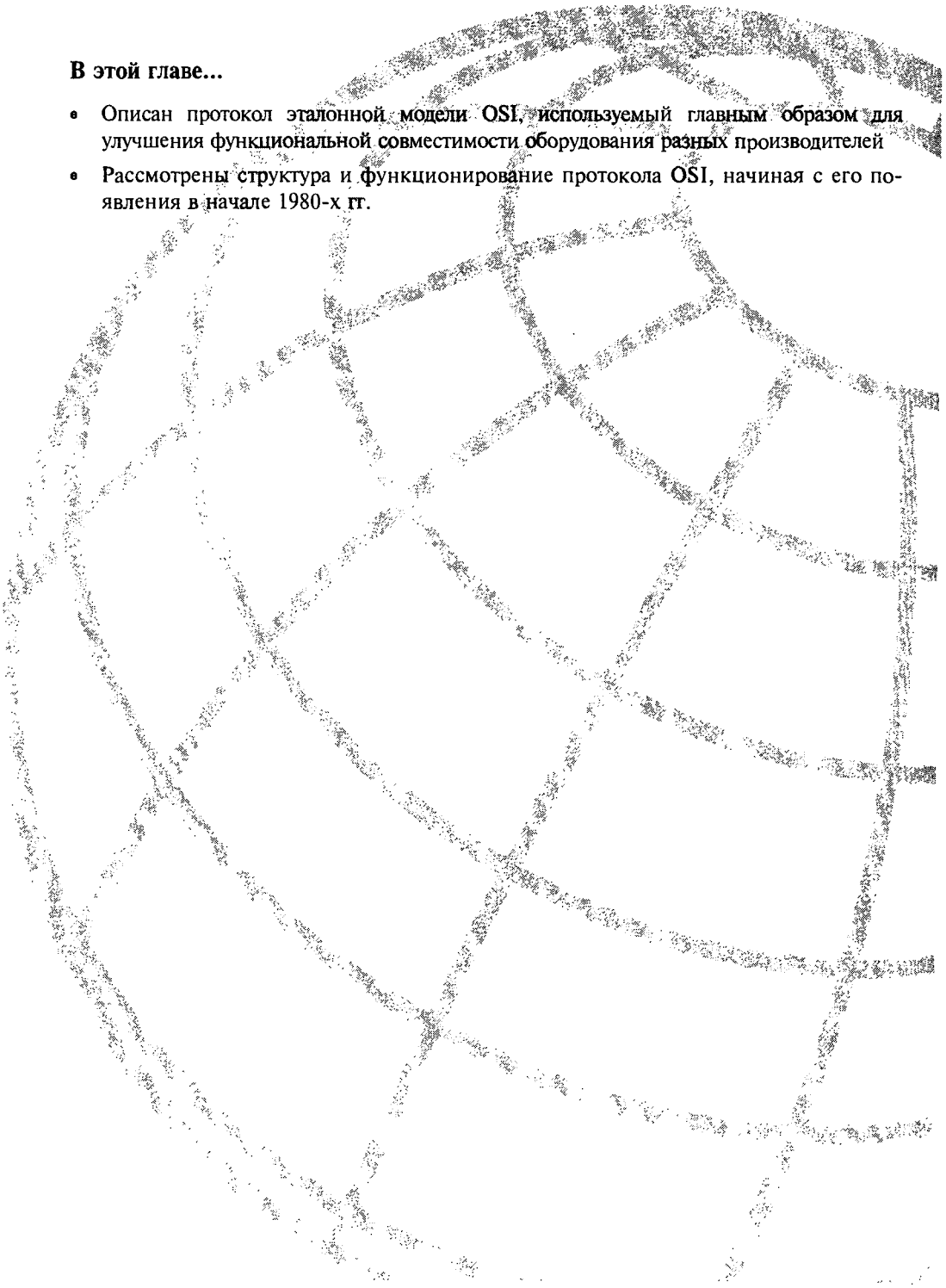
Часть VI

Сетевые протоколы

Глава 34. Протоколы взаимодействия открытых систем
Глава 35. Протоколы Internet
Глава 36. Протокол IPv6
Глава 37. Протоколы NetWare
Глава 38. Протоколы AppleTalk
Глава 39. Протоколы сетевой архитектуры IBM
Глава 40. Протоколы DECnet

В этой главе...

- Описан протокол эталонной модели OSI, используемый главным образом для улучшения функциональной совместимости оборудования разных производителей
- Рассмотрены структура и функционирование протокола OSI, начиная с его появления в начале 1980-х гг.



Глава 34

Протоколы взаимодействия открытых систем

Введение

В пакет протоколов взаимодействия открытых систем (Open System Interconnection — OSI) входит ряд стандартных протоколов, основанных на эталонной модели OSI. Эти протоколы являются частью международной программы развития протоколов передачи данных по компьютерным сетям и других стандартов, улучшающих функциональную совместимость оборудования различных производителей. Программа OSI появилась в ответ на потребность в международных сетевых стандартах. OSI предназначена для улучшения обмена данными между аппаратными и программными системами с разными базовыми архитектурами.

Спецификации OSI были задуманы и реализованы двумя международными организациями по стандартизации: международной организацией по стандартизации (International Organization for Standardization — ISO) и сектором телекоммуникационных стандартов международного телекоммуникационного союза (International Telecommunication Union-Telecommunications Standards Sector — ITU-T). В настоящей главе представлен краткий обзор стека протоколов OSI и показано его соответствие общей эталонной модели OSI.

Сетевые протоколы OSI

На рис. 34.1 показана связь стека протоколов OSI с уровнями эталонной модели OSI. Более подробно компоненты стека будут рассмотрены далее в настоящей главе, а протоколы маршрутизации OSI — в главе 48 "Протоколы маршрутизации OSI".

Физический и канальный уровни OSI

Стек протоколов OSI содержит ряд стандартных протоколов доступа к среде передачи на физическом и канальном уровнях. Большое разнообразие протоколов доступа к среде передачи, поддерживаемых в стеке протоколов OSI, позволяет другим стекам протоколов легко сосуществовать с OSI в одной и той же сети. Поддерживаются следующие протоколы доступа к среде передачи: IEEE 802.2 LLC, IEEE 802.3, Token Ring/IEEE 802.5, FDDI и X.25.

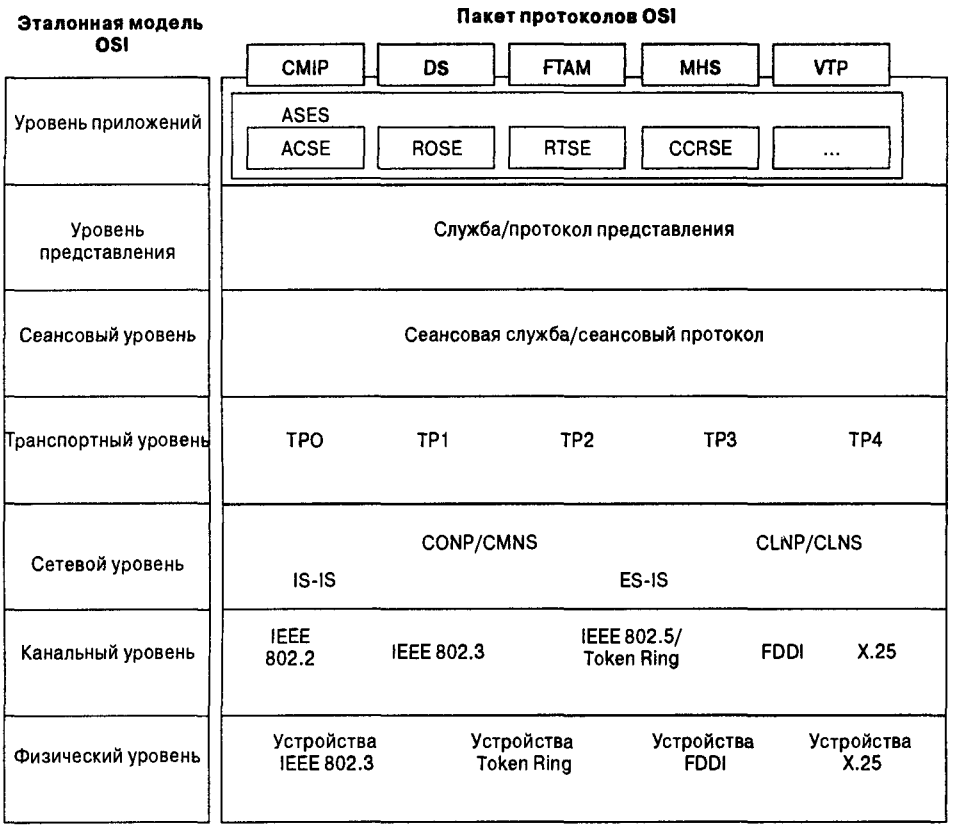


Рис. 34.1. Соответствие пакета протоколов OSI уровням эталонной модели OSI

Сетевой уровень OSI

Для пакета протоколов OSI на сетевом уровне определены два протокола маршрутизации: протокол "конечная система-промежуточная система" (End System-to-Intermediate System — ES-IS) и протокол "промежуточная система-промежуточная система" (Intermediate System-to-Intermediate System — IS-IS). Кроме того, в пакете OSI реализованы два вида сетевых служб: службы, ориентированные на соединение, и службы, не требующие установки соединения.

Стандарты уровней OSI

Кроме стандартов, которые определяют протоколы и службы сетевого уровня OSI, существуют приведенные ниже стандарты, описывающие спецификации сетевого уровня OSI.

- **ISO 8648.** Определяет внутреннюю организацию сетевого уровня (internal organization of the network layer — IONL), согласно которой сетевой уровень делится на три подуровня, чтобы поддерживать разные типы подсетей.

- **ISO 8348.** Определяет адресацию сетевого уровня и описывает поддерживаемые сетевым уровнем OSI службы, ориентированные на соединение, и службы, не требующие подтверждения соединения.
- **ISO TR 9575.** Описывает структуру, понятия и терминологию, используемые для протоколов маршрутизации OSI.

Службы OSI, не требующие подтверждения соединения

Службы OSI, не требующие подтверждения соединения, реализуются при помощи протокола CLNP и службы CLNS. CLNP и CLNS описаны в стандарте ISO 8473.

Протокол сетевой службы, не требующий подтверждения соединения (Connectionless Network Protocol — CLNP) представляет собой протокол сетевого уровня OSI, предназначенный для передачи данных верхнего уровня по каналам, не требующим подтверждения соединения, и для регистрации ошибок. CLNP является интерфейсом между службой CLNS и верхними уровнями.

CLNS предоставляет службы сетевого уровня для транспортного уровня при помощи протокола CLNP.

В отличие от сетевой службы, работающей в режиме соединения (Connection-Mode Network Service — CMNS), служба, не требующая подтверждения соединения (Connectionless Network Service — CLNS), не устанавливает и не прерывает соединение, поскольку для каждого пакета, передающегося через сеть, маршруты определяются отдельно.

Кроме того, служба CLNS обеспечивает доставку методом наименьших затрат (best-effort), т.е. не гарантирует, что данные не будут потеряны, искажены, перепутаны или скопированы. Обнаружение и исправление ошибок службы CLNS выполняется протоколами транспортного уровня.

Службы OSI, ориентированные на соединение

Службы OSI, ориентированные на соединение, реализованы при помощи протокола CONP и службы CMNS.

Ориентированный на соединение сетевой протокол (Connection-Oriented Network Protocol — CONP) представляет собой протокол сетевого уровня OSI, предназначенный для передачи данных верхнего уровня по каналам, требующим подтверждения соединения, и для регистрации ошибок. CONP основан на протоколе пакетного уровня (Packet-Layer Protocol — PLP) X.25 и описывается стандартом ISO 8208 "X.25 Packet-Layer Protocol for DTE".

Протокол CONP служит интерфейсом между службой CMNS и верхними уровнями. Именно служба сетевого уровня, описанная в стандарте ISO 8878, играет роль интерфейса между транспортным уровнем и CONP.

Сетевая служба, работающая в режиме соединения (Connection-Mode Network Service — CMNS), выполняет функции, связанные с явным выбором маршрутов для обмена данными между элементами транспортного уровня. В число этих функций входят установка, поддержка и прекращение соединения. Кроме того, в отличие от CLNS, CMNS также поддерживает механизм запросов качества обслуживания (QoS).

Адресация сетевого уровня

Адресация сетевого уровня OSI реализуется при помощи двух типов иерархических адресов: адресов точки доступа к сетевой службе и заголовков сетевых элементов.

Точка доступа к сетевой службе (Network Service Access Point — NSAP) представляет собой абстрактную точку на границе между сетевым и транспортным уровнями. NSAP является точкой, в которой транспортному уровню предоставляется доступ к сетевым службам OSI. Каждому элементу транспортного уровня выделяется одна точка NSAP и индивидуальный NSAP-адрес в объединенной сети OSI.

Формат такого адреса показан на рис. 34.2.

Рис. 34.2. Каждому элементу транспортного уровня присваивается отдельный NSAP-адрес OSI

Поля NSAP-адреса

Существуют два поля NSAP-адреса: поле первоначального домена (initial domain part — IDP) и поле адреса в домене (domain-specific part — DSP).

Поле IDP делится на две части: идентификатор формата авторизации (authority format identifier — AFI) и идентификатор начального домена (initial domain identifier — IDI). AFI содержит информацию о структуре и содержании полей IDI и DSP — например, является ли длина IDI переменной и использует ли DSP десятичную или двоичную запись. IDI определяет элемент, который может присваивать значения разделу DSP NSAP-адреса.

Поле DSP делится на четыре части сетевым администратором. Поле управления адресом предусматривает дальнейшее управление адресацией, добавляя второй идентификатор авторизации и передавая управление адресами подчиненным элементам. Поле зоны определяет зону в пределах домена и используется для маршрутизации. Поле станции определяет станцию в пределах зоны и также используется для маршрутизации. Поле селектора определяет конкретный n-селектор в пределах станции и, подобно другим полям, используется для маршрутизации. Зарезервированный n-селектор 00 определяет адрес как заголовок сетевого элемента (network entity title — NET).

NSAP-адреса конечной системы

Конечная система (End System — ES) OSI часто имеет несколько NSAP-адресов — по одному для каждого транспортного элемента. В этом случае NSAP-адреса транспортных элементов обычно различаются только последним байтом (называемым n-селектором). На рис. 34.3 показаны отношения между транспортным элементом, NSAP и сетевой службой.

Заголовок сетевого элемента (Network Entity Title — NET) используется для того, чтобы определить сетевой уровень системы, не ассоциируя эту систему с конкретным элементом транспортного уровня (как это делает NSAP-адрес). Заголовки NET полезны для адресации промежуточных систем (intermediate systems — IS), таких как маршрутизаторы, которые не выполняют функций интерфейса с транспортным уровнем. У промежуточной системы IS может быть один или несколько заголовков NET, если она присутствует в нескольких зонах или доменах.

Протоколы OSI транспортного уровня

На транспортном уровне пакет протоколов OSI реализует два типа служб: службы, ориентированные на соединение, и службы, не требующие подтверждения соединения.

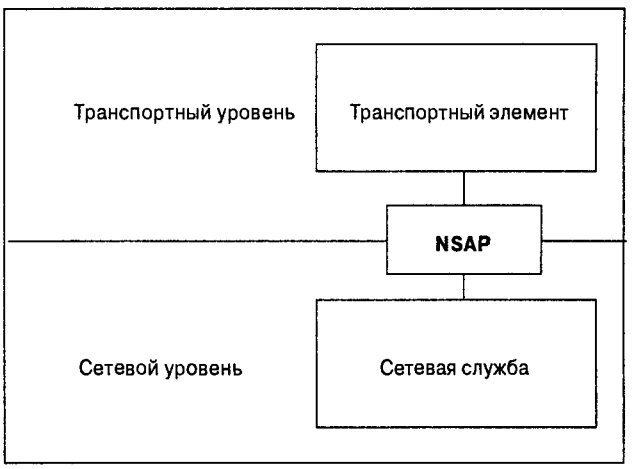


Рис. 34.3. NSAP обеспечивает связь между транспортным элементом и сетевой службой

В пакет OSI входит пять протоколов транспортного уровня, ориентированных на соединение, — от транспортного протокола класса 0 до транспортного протокола класса 4. Службы, не требующие подтверждения соединения, поддерживаются только транспортным протоколом класса 4.

Транспортный протокол класса 0 (TP0) — самый простой из транспортных протоколов. Он выполняет функции сегментации и повторной сборки. TP0 требует сетевой службы, ориентированной на соединение.

Транспортный протокол класса 1 (TP1) выполняет сегментацию и повторную сборку и может устранять основные ошибки. TP1 упорядочивает модули данных протокола (protocol data units — PDU). Если слишком много PDU не получат подтверждения получения, то протокол TP1 передаст их повторно или переустановит соединение. TP1 требует сетевой службы, ориентированной на соединение.

Транспортный протокол класса 2 (TP2) выполняет сегментацию и повторную сборку, а также мультиплексирование и демультиплексирование потоков данных, проходящих по одному виртуальному каналу. TP2 требует сетевой службы, ориентированной на соединение.

Транспортный протокол класса 3 (TP3) позволяет устранять основные ошибки, выполняет сегментацию и повторную сборку, а также мультиплексирование и демультиплексирование потоков данных, проходящих по одному виртуальному каналу. TP3 также упорядочивает модули PDU и, если слишком много модулей PDU не получат подтверждения получения, передает их повторно или переустанавливает соединение. TP3 требует сетевой службы, ориентированной на соединение.

Транспортный протокол класса 4 (TP4) позволяет устранять основные ошибки, выполняет сегментацию и повторную сборку, а также обеспечивает мультиплексирование и демультиплексирование потоков данных, проходящих по одному виртуальному каналу. TP4 упорядочивает PDU и, если слишком много PDU не получат подтверждения о приеме, передает их повторно или переустанавливает соединение. TP4 поддерживает надежное транспортное обслуживание и работает как со службами, ориентированными на соединение, так и со службами, не требующими подтверждения соединения. Он основан на протоколе TCP из стека протоколов Internet и является единственным классом протоколов OSI, поддерживающим сетевые службы, не требующие подтверждения соединения.

Протоколы OSI сеансового уровня

Реализация сеансового уровня пакета протоколов OSI состоит из сеансового протокола и сеансовой службы. Сеансовый протокол позволяет пользователям сеансовой службы (SS-пользователям) общаться с сеансовой службой. SS-пользователь представляет собой элемент, запрашивающий службы сеансового уровня. Такие запросы делаются в точках доступа к сеансовой службе (session-service access points — SSAP). SS-пользователи однозначно идентифицируются по SSAP-адресу. На рис. 34.4 показано взаимодействие между SS-пользователем, точкой доступа SSAP, сеансовым протоколом и сеансовой службой.

Сеансовая служба выполняет для SS-пользователей четыре основных функции. Во-первых, она устанавливает и прекращает соединения между SS-пользователями и синхронизирует обмен данными между ними. Во-вторых, она выполняет всевозможные согласования об использовании маркеров сеансового уровня, которые должны быть у SS-пользователей для того, чтобы начать обмен данными. В-третьих, она вносит в передаваемые данные точки синхронизации, что позволяет восстановить сеанс в случае ошибок или разъединения. В-четвертых, она позволяет SS-пользователям прервать сеанс и продолжить его позднее в определенной точке.

Сеансовая служба описывается в документах ISO 8306 и ITU-T X.215, а сеансовый протокол — документами ISO 8307 и ITU-T X.225. Версия сеансового протокола, не требующая подтверждения соединения, определена стандартом ISO 9548.

Протоколы OSI уровня представления

Реализация уровня представлений пакета протоколов OSI состоит из протокола представлений и службы представлений. Протокол представлений позволяет пользователям службы представлений (PS-пользователям) обмениваться данными со службой представлений.

PS-пользовательпредставляет собой элемент, запрашивающий службы уровня представлений. Такие запросы делаются в точках доступа к службе представлений (presentation-service access points — PSAP). PS-пользователи однозначно идентифицируются по PSAP-адресам.

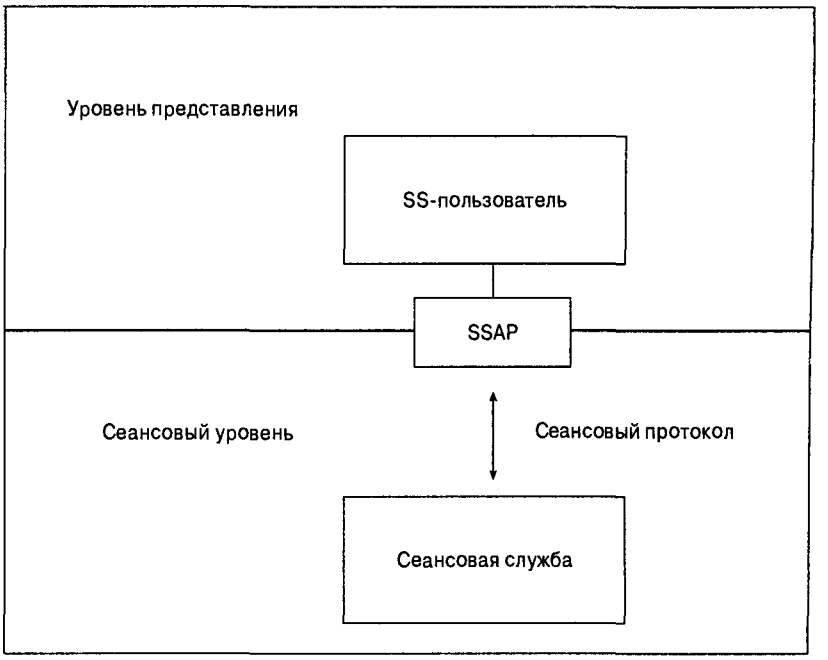


Рис. 34.4. Функции сеансового уровня обслуживают функции уровня представления через точки доступа SSAP

Служба представлений согласовывает синтаксическое преобразование данных и преобразует данные в синтаксические форматы PS-пользователей. Служба представлений используется двумя PS-пользователями для выбора используемого синтаксического преобразования. Затем элементы службы представления преобразуют данные, поступающие от PS-пользователя, в формат переноса.

Служба представления OSI определена документами ISO 8822 и ITU-T X.216, а протокол OSI уровня представления — документами ISO 8823 и ITU-T X.226. Версия протокола представлений, не требующая подтверждения соединения, определена стандартом ISO 9576.

Протоколы OSI уровня приложений

Реализация уровня приложений стека протоколов OSI состоит из нескольких элементов приложений. Элемент приложения представляет собой часть процесса приложения, относящаяся к функционированию стека протоколов OSI. Элемент приложения состоит из элемента пользователя и элемента службы приложения (application service element — ASE).

Элемент пользователя представляет собой часть элемента приложения, использующую ASE, чтобы удовлетворить коммуникационные потребности процесса приложения. ASE представляет собой часть элемента приложения, предоставляющая службы элементам пользователей и, следовательно, процессам приложения. Элементы ASE также служат интерфейсами с нижними уровнями OSI. На рис. 34.5 показаны составляющие одного процесса приложения (элемент приложения, элемент пользователя и ASE) и его взаимосвязи с PSAP и службой представлений.

Элементы ASE делятся на две категории: сервисные элементы общих приложений (common-application service entities — CASE) и сервисные элементы конкретных приложений (specific-application service entities — SASE). В одном элементе приложения могут присутствовать и те, и другие одновременно.

CASE-элементы

Сервисные элементы общего назначения (CASE — Common-Application Service Element) представляют собой ASE-элементы, обеспечивающие службы, которые используются многими процессами приложения. Часто один элемент приложения использует несколько CASE-элементов. В спецификации OSI определены описанные ниже четыре CASE-элемента.

- **ACSE** Сервисный элемент управления ассоциациями. (Association Control Service Element — ACSE). Создает ассоциации между двумя элементами приложения для подготовки обмена данными между приложениями.

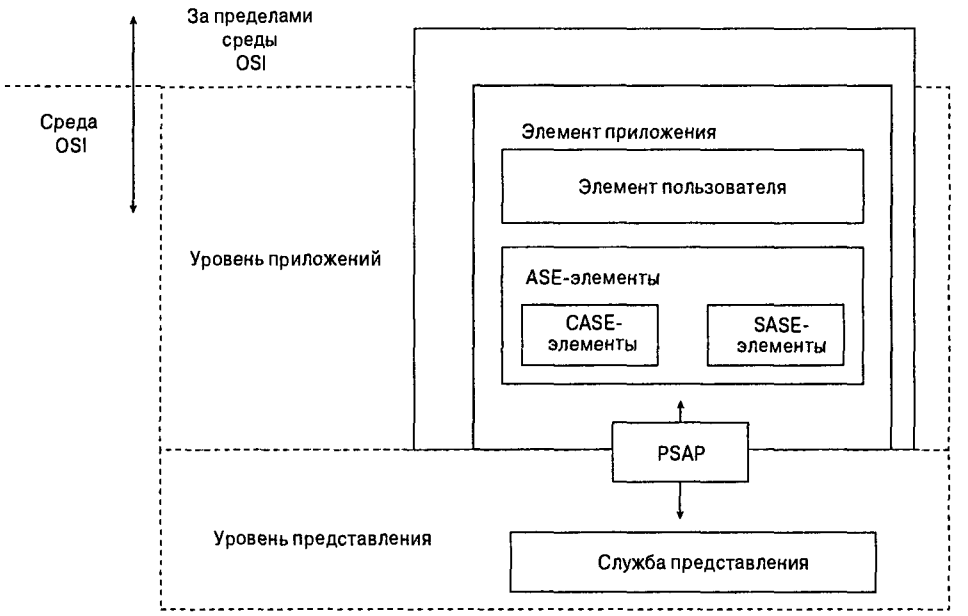


Рис. 34.5. Процесс приложения зависит от PSAP и службы приложения

- **ROSE** Сервисный элемент удаленных операций. (Remote Operations Service Element — ROSE). Реализует механизм "запрос-ответ", обеспечивающий выполнение различных удаленных операций через ассоциацию приложений, установленную ACSE.
- **RTSE Сервисный элемент надежной передачи** (Reliable Transfer Service Element — RTSE). Позволяет ASE-элементам надежно передавать сообщения, сохраняя прозрачность сложных средств нижних уровней.
- **CCRSE Сервисные элементы передачи, согласования и восстановления** (Commitment, Concurrence, and Recovery Service Elements — CCRSE). Эти элементы координируют диалоги между несколькими элементами приложения.

SASE-элементы

Сервисные элементы конкретных приложений (Specific-Application Service Elements — SASE) представляют собой ASE-элементы, которые поддерживают службы, используемые специфическими процессами приложения, такими как передача файлов, доступ к базе данных и порядок ввода.

Процессы протоколов приложений OSI

Процесс приложения представляет собой элемент приложения, который служит интерфейсом между приложением и уровнем приложений OSI. Ниже перечислены некоторые стандартные процессы приложений OSI.

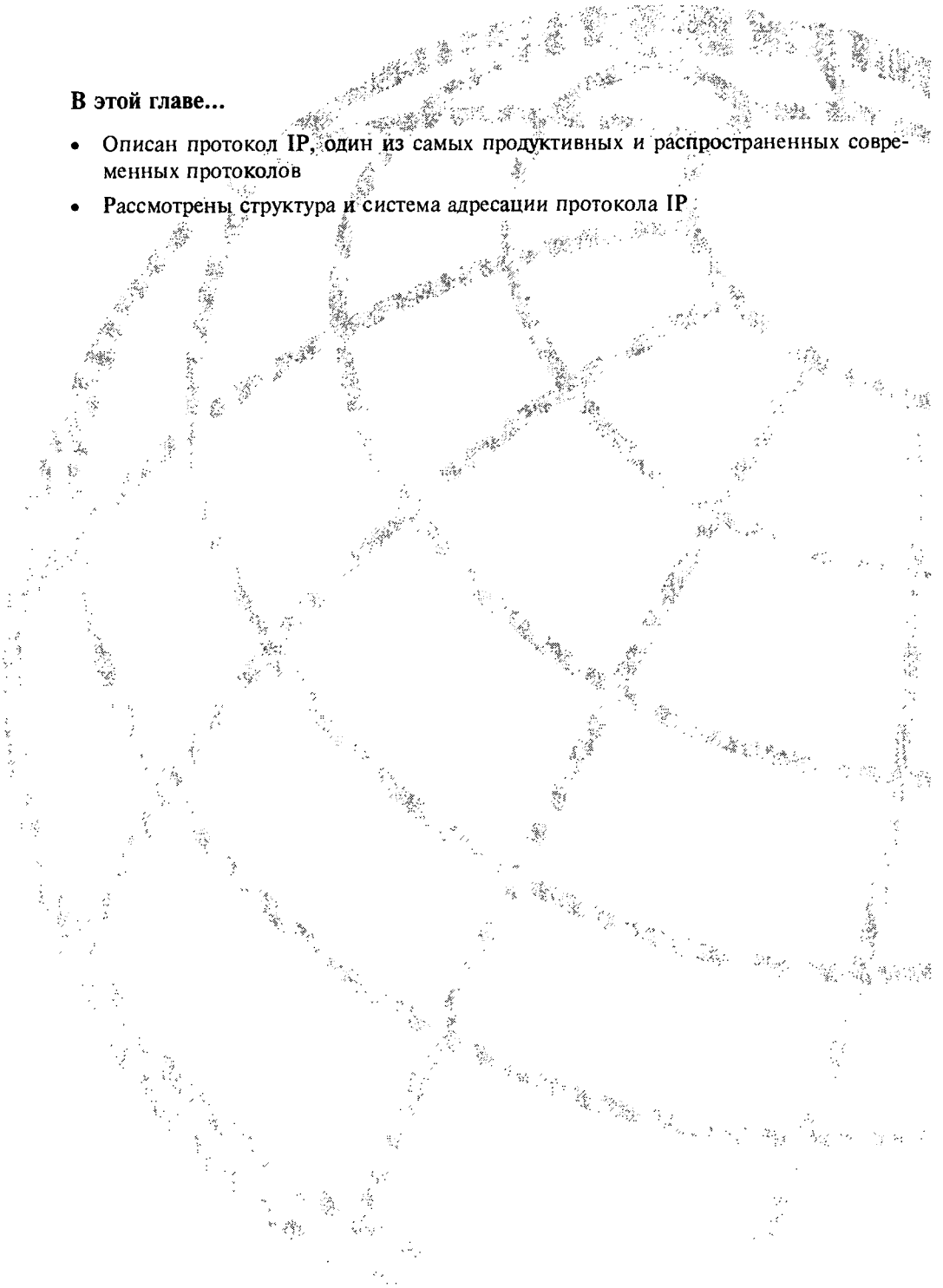
- **Протокол общей управляющей информации (Common Management-Information Protocol — CMIP)** Выполняет функции управления сетью, обеспечивая обмен управляющей информацией между конечными системами и управляющими станциями. Протокол CMIP специфицирован в документации ITU-T X.700 и по своим функциям аналогичен протоколам SNMP и NetView.
- **Службы каталогов DS (Directory Services — DS).** Играют роль распределенного каталога, используемого для идентификации и адресации узла в объединенных сетях OSI. Спецификации служб DS приводятся в ITU-T X.500.
- **Протокол передачи, доступа и управления файлами FTAM (File Transfer, Access, and Management — FTAM).** Обеспечивает передачу файлов и распределенный доступ к ним.
- **Система обработки сообщений (Message Handling System — MHS).** Обеспечивает механизм передачи электронных сообщений между приложениями, используя службы промежуточного хранения.
- **Протокол виртуального терминала VTP (Virtual Terminal Protocol — VTP).** Обеспечивает эмуляцию терминала, позволяющую компьютерной системе выглядеть в отдаленной ES так, как если бы она была непосредственно подключенным терминалом.

Контрольные вопросы

1. Какие два протокола маршрутизации определены в пакете OSI?
2. Опишите протокол сетевой службы OSI, не требующий подтверждения соединения.
3. Опишите протокол сетевой службы OSI, ориентированный на соединение.
4. Как реализуются запросы служб на сеансовом уровне в протоколах OSI?
5. Что такое CASE-элементы?
6. Назовите среды, поддерживаемые пакетом протоколов OSI.
7. Как был создан пакет протоколов OSI?
8. Опишите протоколы сеансового уровня в пакете протоколов OSI.
9. Опишите протоколы уровня представлений пакета протоколов OSI.
10. Назовите две категории ASE-элементов.

В этой главе...

- Описан протокол IP, один из самых продуктивных и распространенных современных протоколов
- Рассмотрены структура и система адресации протокола IP



Глава 35

Протоколы Internet

Введение

Протоколы Internet образуют наиболее распространенный сегодня набор протоколов, поскольку они могут быть использованы для обмена данными между любыми соединенными сетями и одинаково хорошо подходят как для локальных, так и для глобальных сетей. В набор протоколов Internet входят протоколы обмена данными, из которых двумя наиболее известными являются протокол управления передачей (Transmission Control Protocol — TCP) и Internet-протокол (Internet Protocol — IP).

В набор протоколов Internet входят не только протоколы нижнего уровня (такие, как TCP и IP), но и общие приложения, например, электронная почта, эмуляция терминала и передача файлов. Эта глава представляет собой общее введение в спецификации, образующие набор протоколов Internet. В ней будут рассмотрены IP-адресация и основные протоколы верхнего уровня, используемые в Internet. Специальные протоколы маршрутизации будут рассмотрены в части VII настоящей книги.

Первые версии протоколов Internet появились в середине 1970-х гг. XX века, когда управление перспективных исследовательских программ (Defense Advanced Research Projects Agency — DARPA) заинтересовалось созданием сети с коммутацией пакетов, которая могла бы осуществлять обмен данными между разнородными вычислительными системами, установленными в исследовательских институтах. Для обеспечения связи между неоднородными сетями DARPA финансировало исследования Стэндфордского университета, а также компании Bolt, Beranek, and Newman (BBN). Результатом их работы стал набор протоколов Internet, работа над которым завершилась в конце 1970-х гг.

Протокол TCP/IP был включен туда позже, вместе с BSD UNIX, и с тех пор стал основой Internet и World Wide Web (WWW). Протоколы Internet (включая новые и обновленные протоколы) и политики специфицированы в документах RFC (Request For Comments), которые были опубликованы, рецензированы и проанализированы сообществом Internet. В новых RFC содержатся более подробные описания этих протоколов. Для того чтобы проиллюстрировать масштабы применения протоколов Internet, на рис. 35.1 показано большинство протоколов из набора протоколов Internet и соответствующие им уровни модели OSI. В данной главе описываются основные элементы и операции этих и других протоколов Internet.

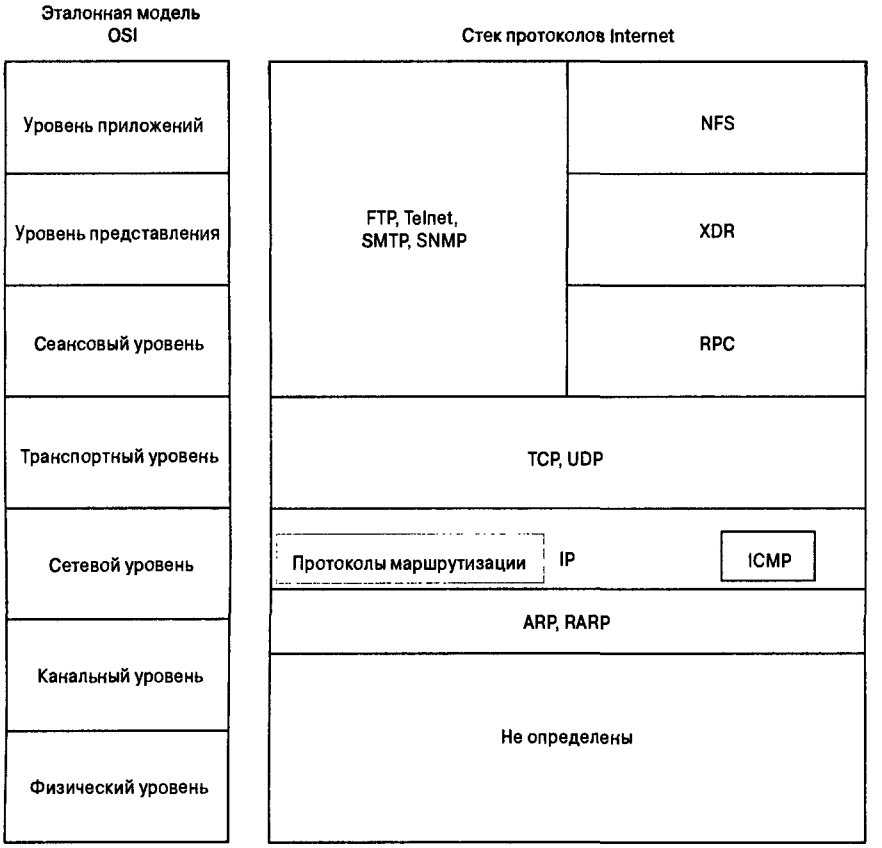


Рис. 35.1. Стек протоколов Internet охватывает все уровни эталонной модели OSI

Протокол IP

Протокол IP представляет собой протокол сетевого (3-го) уровня, который содержит информацию об адресации и управляющую информацию для маршрутизации пакетов. Протокол IP описан в RFC 791 и является основным протоколом сетевого уровня в наборе протоколов Internet. Вместе с протоколом управления передачей (TCP) протокол IP образует основу протоколов Internet. Протокол IP имеет две основные функции: обеспечение передачи дейтаграмм по объединенной сети методом негарантированной доставки без подтверждения соединения и обеспечение фрагментации и повторной сборки дейтаграмм для поддержки каналов передачи данных с различными размерами максимального передаваемого модуля данных (MTU).

Формат IP-пакета

IP-пакет содержит несколько видов информации (рис. 35.2).
Поля IP-пакета, показанные на рис. 35.2, описаны ниже.

- **Версия.** Версия используемого протокола IP.

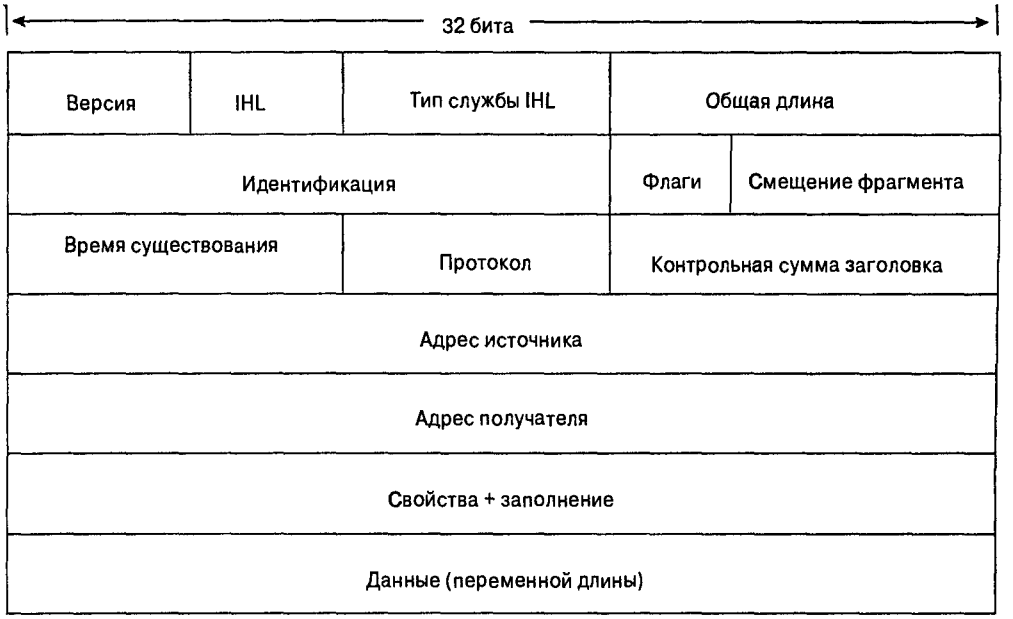


Рис. 35.2. IP-пакет

- **Длина IP-заголовка** (IP header length — IHL). Длина заголовка дейтаграммы в 32-разрядных словах.
- **Тип службы.** Задает требуемый протоколом верхнего уровня способ обработки текущей дейтаграммы и присваивает дейтаграммам различные степени важности.
- **Общая длина.** Длина всего IP-пакета в байтах, включая данные и заголовок.
- **Идентификация.** Целое число, которое идентифицирует данную дейтаграмму. Это поле используется для облегчения соединения фрагментов дейтаграмм.
- **Флаги.** Трехразрядное поле, в котором 2 младших бита управляют фрагментацией. Младший бит определяет, может ли пакет быть фрагментирован, а средний — является ли пакет последним в серии фрагментированных пакетов. Третий (старший) бит не используется.
- **Смещение фрагмента.** Позиция данных фрагмента относительно начала данных в исходной дейтаграмме, что позволяет IP-процессу правильно восстановить исходную дейтаграмму.
- **Время существования.** Счетчик, который постепенно уменьшается до нуля, после чего дейтаграмма отбрасывается во избежание бесконечного цикла передачи пакетов.
- **Протокол.** Протокол верхнего уровня, принимающий входящие пакеты после окончании обработки их протоколом IP.
- **Контрольная сумма заголовка.** Используется для проверки целостности IP-заголовка.
- **Адрес источника.** Определяет узел-отправитель.
- **Адрес получателя.** Определяет принимающий узел.

- **Свойства.** Позволяет протоколу IP задавать дополнительные операции, такие как обеспечение безопасности.
- **Данные.** Информация верхнего уровня.

IP-адресация

Как и в любом протоколе сетевого уровня, схема IP-адресации неразрывно связана с процессом маршрутизации IP-дейтаграмм по объединенной сети. Каждый IP-адрес имеет специфические компоненты и соответствует основному формату. Как будет описано ниже, IP-адреса делятся на категории и используются для создания адресов подсетей. Каждому узлу в сети TCP/IP присваивается уникальный 32-разрядный логический адрес, который делится на две главные части: номер сети и номер узла. Номер сети определяет сеть и, если сеть является частью Internet, должен присваиваться Информационным центром Internet (Internet Network Information Center — InterNIC). Провайдер служб Internet может получить у InterNIC блоки сетевых адресов и самостоятельно выделять адресное пространство по мере необходимости. Номер узла определяет узел в сети и присваивается администратором локальной сети.

Формат IP-адреса

32-разрядный IP-адреспредставляет собой 4 группы по 8 битов, разделенные точками и обычно записываемые в десятеричном формате (так называемая десятичная запись с точками — dotted decimal notation). Каждый бит октета имеет двоичный вес (128, 64, 32, 16, 8, 4, 2, 1). Минимальное значение октета равно 0, максимальное — 255. Основной формат IP-адреса показан на рис. 35.3.

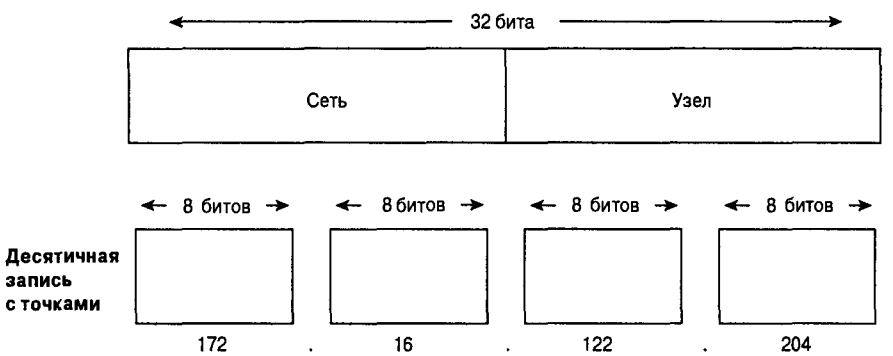


Рис. 35.3. Формат IP-адреса

Классы IP-адресов

IP-адреса делятся на пять классов: A, B, C, D и E. Для коммерческого использования предназначены только классы A, B, и C. Класс сети определяется первыми слева (старшими) битами. Справочная информация о пяти классах IP-адресов представлена в табл. 35.1.

На рис. 35.4 показан формат классов коммерческих IP-адресов. Следует обратить внимание на старшие биты в каждом классе.

Таблица 35.1. Справочная информация о пяти классах IP-адресов

Класс IP-адреса	Формат	Назначение	Старший бит (биты)	Диапазон адресов	Количество битов, сеть/узел	Максимальное количество узлов
A	N.H.H.H*	Несколько крупных организаций	0	1.0.0.0 — 126.0.0.0	7/24	16777214** (2^{24}-2)
B	N.N.H.H	Средние организации	1, 0	128.1 — 191.254.0.0	14/16	65543 (2^{16}-2)
C	N.N.N.H	Сравнительно мелкие организации	1,1, 0	192.0.1.0 — 223.255.254.0	22/8	245 (2^{8}-2)
D	—	Многоадресные группы (RFC 1112)	1,1,1, 0	224.0.0.0 — 239.255.255.255	Не для коммерческого использования	—
E	—	Экспериментальный	1,1,1,1	240.0.0.0 — 254.255.255.255	—	—

* N — номер сети, H — номер узла.

** Один адрес зарезервирован как широковещательный и еще один — для сети.

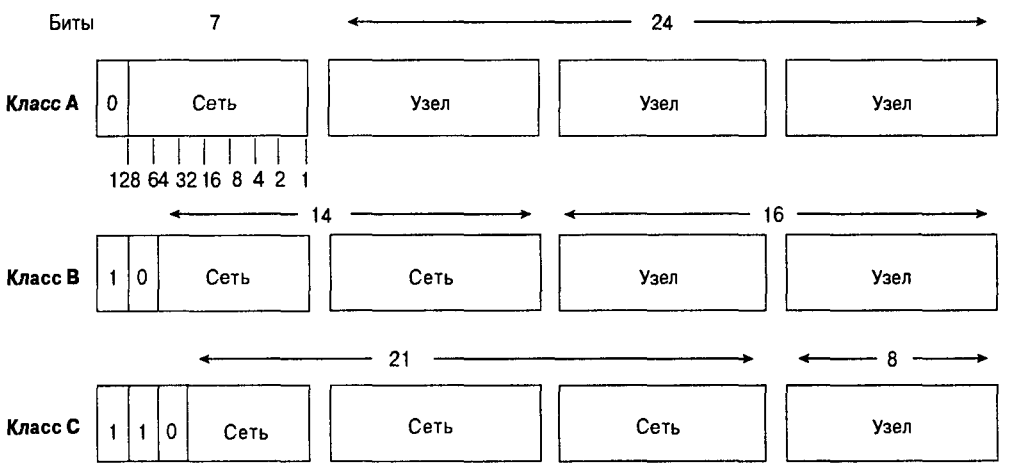


Рис. 35.4. Для коммерческого использования доступны IP-адреса форматов A, B и C

Класс адреса легко определить по его первому октету, сравнив это значение с диапазоном классов по следующей таблице. Например, в IP-адресе 172.31.1.2 первый октет равен 172. Поскольку 172 лежит в пределах от 128 до 191, 172.31.1.2 является адресом класса B. На рис. 35.5 представлены диапазоны возможных значений первого октета каждого класса адресов.

IP-адресация подсети

IP-сети иногда делятся на сети меньшего размера, называемые подсетями. Подсети предоставляют сетевому администратору некоторые преимущества, такие как повы-

шенная гибкость, более эффективное использование сетевых адресов и возможность ограничить широковещательные потоки данных (чтобы они не проходили через маршрутизатор).

Класс адреса	Первый октет, десятичная запись	Старшие биты
Класс A	1 — 126	0
Класс B	128 — 191	10
Класс C	192 — 223	110
Класс D	224 — 239	1110
Класс E	240 — 254	1111

Рис. 35.5. У каждого класса адресов существует свой диапазон допустимых значений первого октета

Подсети администрируются локально. При этом внешне вся сеть выглядит единой, и ее информация о внутренней структуре извне недоступно.

Сетевой адрес может разбиваться на несколько подсетей. Например, в состав сети 172.16.0.0 могут входить подсети 172.16.1.0, 172.16.2.0, 172.16.3.0 и 172.16.4.0. (Наличие всех нулей в адресной части узла указывает на то, что это адрес не узла, а сети).

Маска IP-подсети

Адрес подсети создается "заимствованием" битов из поля узла и использованием их для поля подсети. Количество заимствованных битов из поля узла не является постоянным и определяется маской подсети. На рис. 35.6 показано, как заимствуются биты из поля адреса узла для создания поля адреса подсети.

Маски подсети имеют тот же формат и представление, что и IP-адреса. Однако в маске подсети во всех разрядах, определяющих зоны сети и подсети, стоит двоичная единица, а во всех разрядах, определяющих поле узла, — двоичный ноль. Пример маски подсети показан на рис. 35.7.

Биты маски подсети должны повторять старшие (первые слева) биты поля узла (рис. 35.8). Подробнее маски подсети класса B и C будут описаны ниже. Адреса класса A в этой главе не обсуждаются, поскольку они обычно делятся на подсети на границе 8 битов.

Для подсетей класса B и C существуют различные типы масок подсети.

Стандартная маска подсети для адреса класса B без подсетей — 255.255.0.0, а маска подсети для адреса 171.16.0.0 класса B, где для подсети отводится 8 битов, — 255.255.255.0. Значение этих 8 битов — 2^8-2 (1 — для сетевого и 1 — для широковещательного адреса) = 254 возможных подсетей по 2^8-2 = 254 узла в каждой.

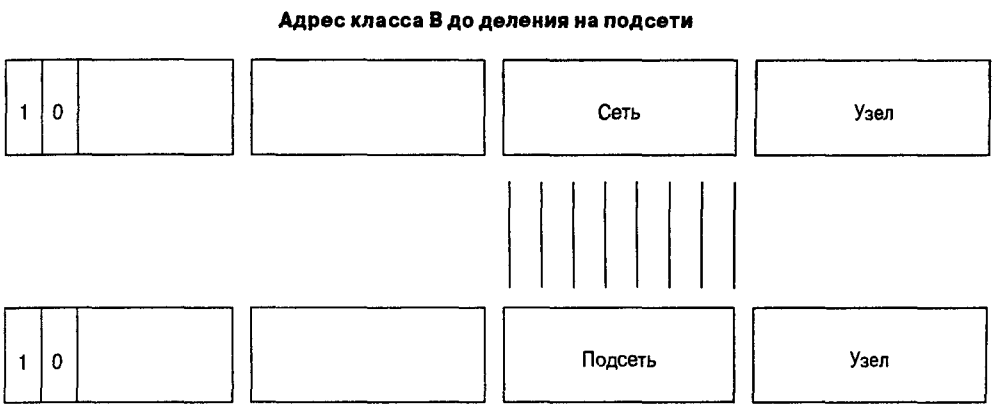


Рис. 35.6. Для создания поля адреса подсети заимствуются биты из поля адреса узла

	Сеть	Сеть	Подсеть	Узел
Двоичное представление	11111111	11111111	11111111	00000000
Десятичное представление с разделителями	255	255	255	0

Рис. 35.7. Пример маски подсети, состоящей из двоичных нулей и единиц

128	64	32	16	8	4	2	1		
1	0	0	0	0	0	0	0	=	128
1	1	0	0	0	0	0	0	=	192
1	1	1	0	0	0	0	0	=	224
1	1	1	1	0	0	0	0	=	240
1	1	1	1	1	0	0	0	=	248
1	1	1	1	1	1	0	0	=	252
1	1	1	1	1	1	1	0	=	254
1	1	1	1	1	1	1	1	=	255

Рис. 35.8. Для маски подсети используются старшие биты поля узла

Маска подсети для адреса 192.168.2.0 класса С, где для подсети отводится 5 битов, имеет вид 255.255.255.248. Если для подсети отводится 5 битов, то количество возможных подсетей равно $2^5-2 = 31$, при этом в каждой из них будет $2^3-2 = 6$ узлов.

При проектировании сетей классов В и С для определения необходимого количества подсетей и узлов, а также выбора соответствующей маски сети можно воспользоваться справочными данными, приведенными в табл. 35.2 и 35.3.

Таблица 35.2. Параметры подсетей класса В

Количество битов	Маска подсети	Количество подсетей	Количество узлов
2	255.255.192.0	2	16382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16382	2

Таблица 35.3. Параметры подсетей класса С

Количество битов	Маска подсети	Количество подсетей	Количество узлов
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

Определение номера сети по маске подсети

Маршрутизатор определяет адрес сети (а точнее, подсети). Вначале маршрутизатор извлекает из входящего пакета IP-адрес получателя и восстанавливает маску внутренней подсети. Затем путем логического умножения он получает номер сети, причем IP-адрес узла получателя удаляется, а номер сети получателя остается. После этого маршрутизатор находит номер сети получателя и сравнивает его с исходящим интерфейсом. Наконец, он передает фрейм по заданному IP-адресу. Подробнее операция логического умножения описывается в следующем разделе.

Операция логического умножения

Логическое умножение (логическое И) пары двоичных чисел подчиняется следующим трем основным правилам: 1 И 1 = 1, 1 И 0 = 0, 0 И 0 = 0 (табл. 35.4). Для запоминания операций логического умножения существует два простых правила: логическое умножение любого числа на 1 не изменяет его, а результат логического умножения любого числа на 0 всегда равен 0.

Таблица 35.4. Правила логического умножения

Вход	Вход	Выход
1	1	1
1	0	0
0	1	0
0	0	0

Как видно из рис. 35.9, при логическом умножении IP-адреса получателя на маску подсети получается номер подсети, который и используется маршрутизатором для передачи пакета.

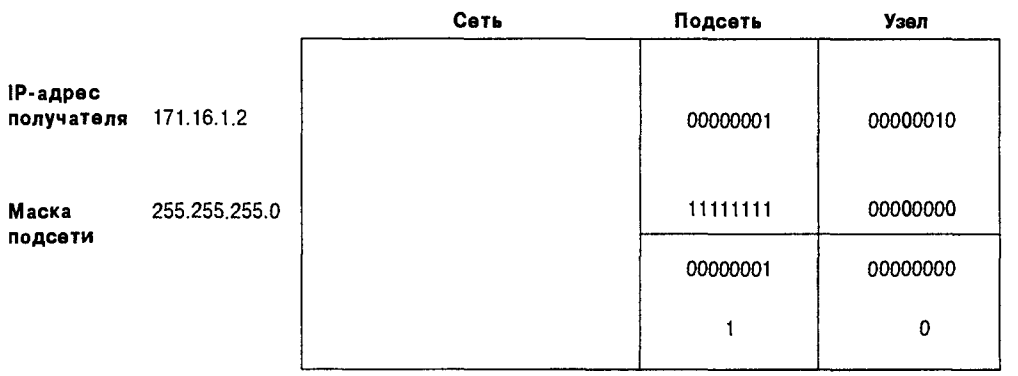


Рис. 35.9. Логическое умножение IP-адреса получателя и маски подсети дает номер подсети

Основные сведения о протоколе ARP

Для обмена данными между двумя компьютерами в одой сети каждый из них должен знать физический адрес другого (или MAC-адрес). Путем широковещательной рассылки протоколов преобразования адресов (Address Resolution Protocols — ARP) узел может динамически узнать адрес MAC-уровня, соответствующий IP-адресу сетевого уровня.

После получения MAC-адреса IP-устройства создают кэш ARP для хранения полученной схемы преобразования адресов IP-MAC, так что при повторном контакте с устройством широковещательная рассылка ARP не требуется. Если устройство не отвечает в течение определенного времени, выделенная для него область кэша освобождается.

Кроме того, для преобразования MAC-адресов в IP-адреса используется протокол обратного преобразования адресов (Reverse Address Resolution Protocol — RARP). RARP является логической противоположностью ARP и может использоваться на бездисковых

рабочих станциях, которые при запуске не знают своего IP-адреса. Протокол RARP требует наличия сервера RARP с таблицей преобразования MAC-адресов в IP-адреса.

Маршрутизация Internet

Устройства маршрутизации в Internet традиционно называются шлюзами (gateway). Однако в современной терминологии термином "шлюз" обозначают устройство, выполняющее преобразование протоколов уровня приложений между другими устройствами. Внутренними шлюзами называют устройства, выполняющие эти преобразования между компьютерами или сетями в пределах одной области управления либо подчинения, например во внутренней сети компании. Такие системы называются автономными. Внешние шлюзы выполняют функции протоколов между независимыми сетями. Маршрутизаторы Internet образуют иерархическую структуру. Те из них, что используются для обмена информацией внутри автономных систем, называются внутренними и выполняют свою задачу при помощи различных протоколов стандарта протокола маршрутизации внутреннего шлюза (Interior Gateway Protocol — IGP), таких, например, как протокол маршрутной информации RIP (Routing Information Protocol — RIP).

Маршрутизаторы, предназначенные для передачи информации между автономными системами, называются внешними и используют протоколы маршрутизации внешнего шлюза EGP (Exterior Gateway Protocol — EGP), такие, например, как протокол граничного шлюза (Border Gateway Protocol — BGP).

Примечание

Отдельные протоколы маршрутизации, в том числе BGP и RIP, будут рассмотрены отдельно, в последующих главах.

IP-маршрутизация

Протоколы IP-маршрутизации являются динамическими. Динамическая маршрутизация требует, чтобы маршрут автоматически регулярно вычислялся программным обеспечением устройств маршрутизации — в отличие от статической маршрутизации, при которой маршруты устанавливаются сетевым администратором и не изменяются до тех пор, пока сам администратор этого не сделает.

Для динамической маршрутизации применяется таблица IP-маршрутизации, состоящая из пар "адрес получателя/следующий узел". Запись в такой таблице, может интерпретироваться следующим образом: "чтобы достичь сети 172.31.0.0, нужно отправить пакет через интерфейс 0 Ethernet (E0)".

IP-маршрутизация определяет характер перемещения IP-дейтаграмм по объединенным сетям — от узла к узлу. Однако в начале "путешествия" весь маршрут неизвестен. Следующий пункт назначения вычисляется на каждой остановке путем сопоставления адреса назначения дейтаграммы с записью в таблице маршрутизации текущего узла.

Участие каждого узла в процессе маршрутизации ограничивается передачей пакетов в соответствии с внутренней информацией. Узлы не следят за успешным прохождением пакета до конечного пункта. В случае аномальной маршрутизации протокол IP не сообщает источнику об ошибках. Эта задача возлагается на другой протокол Internet — протокол ICMP, описанный в следующем разделе.

Протокол ICMP

Протокол управляющих сообщений в сети Internet (Internet Control Message Protocol — ICMP) представляет собой Internet-протокол сетевого уровня, создающий пакеты сообщений с отчетами об ошибках и другой информацией об обработке IP-пакетов, которые предназначены для источника. Протокол ICMP описан в RFC 792.

Сообщения протокола ICMP

Протокол ICMP генерирует несколько видов сообщений, в том числе сообщения о недоступности получателя, перенаправлении маршрута, истечении лимита времени, анонсировании маршрутизатора, а также запросы маршрутизатора, эхо-запрос и эхо-ответ. Если ICMP-сообщение не может быть доставлено, второе такое сообщение не создается во избежание бесконечного потока ICMP-сообщений.

Если маршрутизатор посылает сообщение о недоступности получателя, то это означает, что маршрутизатор неспособен передать пакет по конечному адресу назначения. Тогда маршрутизатор отбрасывает исходный пакет. Недоступность получателя может быть вызвана двумя причинами. Чаще всего это происходит потому, что исходный узел указывает несуществующий адрес. Реже возникает ситуация, в которой у маршрутизатора отсутствует маршрут к узлу получателя.

Сообщения о недоступности получателя делятся на четыре основных типа: недоступность сети, узла, протокола и порта. Сообщения о недоступности сети обычно означают ошибку в маршрутизации или адресации пакетов. Сообщения о недоступности узла обычно указывают на ошибку доставки, такую как неверная маска подсети. Сообщения о недоступности протокола обычно означают, что узел получателя не поддерживает протокол верхнего уровня, указанный в пакете. Сообщения о недоступности порта подразумевают, что заняты TCP-сокет или порт.

ICMP-сообщение эхо-запроса, которое формируется командой **ping**, может посылаться любым узлом для проверки доступности узла в объединенной сети. Если узел доступен, то в ответ посылается ICMP-сообщение эхо-ответа.

ICMP-сообщение о перенаправлении маршрута посылается маршрутизатором на исходный узел для более эффективной маршрутизации. Маршрутизатор также отправляет исходный пакет по назначению. Перенаправление маршрута позволяет делать компактные списки маршрутизации узлов, поскольку при этом необходимо знать адрес только одного маршрутизатора, даже если он не предоставляет наилучшего маршрута. Но и после получения ICMP-сообщения о перенаправлении маршрута некоторые устройства могут продолжать использовать менее эффективный маршрут.

ICMP-сообщение об истечении лимита времени посылается маршрутизатором в случае обнуления поля времени существования IP-пакета (выражается в пройденных узлах или секундах). Поле времени существования предотвращает бесконечную циркуляцию пакетов по объединенной сети, если последняя содержит маршрутную петлю. В этом случае маршрутизатор отбрасывает исходный пакет.

Протокол IDRP

Протокол обнаружения маршрутизатора (ICMP Router-Discovery Protocol — IRDP) использует объявления и запросы маршрутизаторов, чтобы определить адреса маршрутизаторов соседних подсетей. Каждый маршрутизатор периодически рассылает с

каждого своего интерфейса широковещательные объявления. Получая эти сообщения, узлы узнают адреса маршрутизаторов соседних подсетей. Вместо того чтобы ожидать незапрашиваемые сообщения, узлы могут использовать для запроса немедленных объявлений сообщения маршрутизаторов.

IRDP обладает некоторыми преимуществами по сравнению с другими методами определения адресов соседних маршрутизаторов. Он не требует от узлов распознавания протоколов маршрутизации, а от администратора — ручной настройки.

Объявления маршрутизатора сообщают узлам о наличии соседних маршрутизаторов, но не несут информации о качестве маршрута. Если для достижения узла получателя узел использует ближайший, но не оптимальный маршрутизатор, он получает сообщение о лучшем варианте маршрута.

Протокол TCP

Протокол управления передачей (Transmission Control Protocol — TCP) обеспечивает надежную передачу данных в среде IP. TCP относится к транспортному уровню эталонной модели OSI (4-й уровень). TCP предоставляет такие службы, как потоковая передача данных, надежность, эффективное управление потоком, дуплексный режим и мультиплексирование.

При потоковой передаче данных TCP передает неструктурированный поток байтов, идентифицируемых по порядковым номерам. Эта служба полезна для приложений, поскольку им не приходится разбивать данные на блоки перед их передачей по протоколу TCP. TCP группирует байты в сегменты и передает их на уровень протокола IP для пересылки.

Надежность TCP обеспечивается сквозной, ориентированной на соединение, передачей пакетов по объединенной сети. Она достигается упорядочением байтов при помощи номеров подтверждения передачи, по которым получатель определяет, какой байт должен поступить следующим. Байты, не получившие подтверждения в течение определенного времени, передаются заново. Надежный механизм протокола TCP позволяет устройствам обрабатывать потерянные, задержанные, дублированные и неверно прочитанные пакеты. Механизм лимита времени позволяет устройствам распознавать потерянные пакеты и запрашивать их повторную передачу.

TCP обеспечивает эффективное управление потоком. При отправке подтверждений источнику данных принимающий TCP-процесс указывает наибольший порядковый номер, который он может принять без переполнения внутренних буферов.

В дуплексным режиме TCP-процесс может одновременно пересылать и принимать пакеты.

Наконец, мультиплексирование TCP означает одновременную передачу по одному соединению нескольких диалогов верхнего уровня.

Установка TCP-соединения

Для использования надежных транспортных служб TCP-узлы должны устанавливать друг с другом сеансы, ориентированные на соединение. Установка соединения выполняется по механизму, называемому *трехэтапной синхронизацией* (three-way handshake).

Этот механизм синхронизирует обе стороны соединения, позволяя им согласовать начальные порядковые номера. Он также обеспечивает готовность обеих сторон к передаче данных и информированность каждой из сторон о готовности другой. Это не-

обходимо во избежание передачи или повторной передачи пакетов в процессе установки сеанса или после его разрыва.

Каждый узел выбирает случайным образом порядковый номер, чтобы следить за приемом и передачей байтов потока. Затем механизм трехэтапной синхронизации работает следующим образом.

Первый узел (Узел А) инициирует соединение, отправляя пакет с начальным порядковым номером и битом синхронизации SYN для индикации запроса соединения. Второй узел (Узел В) получает SYN, записывает порядковый номер X и отвечает подтверждением SYN (вместе с ACK = X + 1). Узел В указывает собственный порядковый номер (SEQ = Y). Тогда, если ACK равен 20, то это означает, что узел принял байты с 0 по 19 и ожидает следующий байт 20. Эта технология называется подтверждением передачи. Затем Узел А подтверждает прием всех байтов, посланных Узлом В с подтверждением передачи, указывая следующий байт, который Узел А ожидает получить (ACK = Y + 1). После этого может начинаться передача данных.

Подтверждение приема и повторная передача

Простой транспортный протокол может обеспечивать надежность и такую технологию управления потоком, при которой исходный узел посылает пакет, запускает таймер и ждет подтверждения приема перед отправкой нового пакета. Если подтверждение не получено по истечении времени, узел передает пакет еще раз. Эта технология называется *подтверждением приема и повторной передачей* (Positive Acknowledgment and Retransmission — PAR).

Присваивая каждому пакету порядковый номер, PAR позволяет узлам отслеживать пакеты, потерянные или дублированные вследствие сетевых задержек и преждевременной повторной передачи. Номера последовательностей посылаются обратно как уведомления в возможности отслеживания подтверждений приема.

Однако PAR неэффективно использует пропускную способность, потому что перед отправкой нового пакета узел должен ждать подтверждения и, следовательно, пакет можно передавать только один за другим.

Скользящее окно TCP

Скользящее окно TCP позволяет использовать пропускную способность сети более эффективно, чем PAR, поскольку с его помощью узелы могут отправлять несколько байтов или пакетов, не дожидаясь подтверждения.

В TCP принимающий узел определяет текущий размер окна каждого пакета. Так как по TCP-соединению данные передаются в виде потока байт, размеры окон тоже выражаются в байтах. Таким образом, окнопредставляет собой количество байт данных, которые отправитель может послать до ожидания подтверждения приема. Начальные размеры окон определяются при настройке соединения, но могут изменяться при передаче данных для управления потоком. Например, нулевой размер окна означает запрет на передачу данных.

Предположим, что TCP-отправителю надо послать с помощью скользящего окна последовательность байт (пронумерованных от 1 до 10) получателю с размером окна 5. Отправитель помещает в окно первые 5 байт, передает их все сразу и ждет подтверждения приема.

Получатель отвечает с ACK, равным 6, показывая, что получил байты с 1 по 5 и ждет байта 6. В том же пакете получатель показывает, что размер его окна равен 5. Отправитель сдвигает скользящее окно на 5 байт вправо и передает байты с 6 по 10. Получатель отвечает ACK, равным 11, показывая, что он ожидает байта 11. В этом пакете получатель может указать, что его размер окна равен 0 (поскольку, например, его внутренние буферы заполнены). Тогда отправитель больше не сможет посылать байты, пока получатель не пошлет другой пакет с ненулевым размером окна.

Формат TCP-пакета

Поля и полный формат TCP-пакета показаны на рис. 35.10.

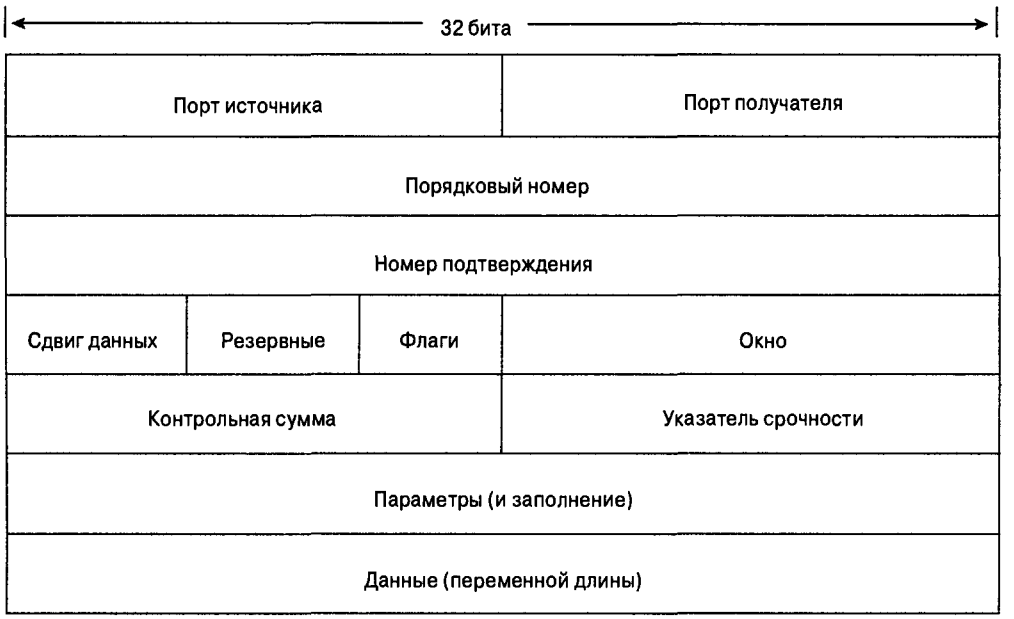


Рис. 35.10. Формат TCP-пакета

Описание полей TCP-пакета

Ниже описаны поля TCP-пакета, показанные на рис. 35.10.

- **Порт источника и порт получателя.** Точки, в которых процессы верхнего уровня источника и получателя принимают услуги TCP.
- **Порядковый номер.** Обычно это номер, присвоенный первому байту данных в текущем сообщении. При установке соединения может также использоваться для обозначения исходного порядкового номера в предстоящей передаче.
- **Номер подтверждения.** Порядковый номер следующего байта данных, который ожидает получить получатель.
- **Сдвиг данных.** Число 32-разрядных слов в заголовке TCP.
- **Резервные.** Область, зарезервированная для использования в будущем.

- **Флаги.** Различная управляющая информация, в том числе биты SYN и ACK, используемые для установки соединения, и бит FIN для разрыва соединения.
- **Окно.** Размер приемного окна получателя (объем буфера для входящих данных).
- **Контрольная сумма.** Показывает, не был ли заголовок поврежден при передаче.
- **Указатель срочности.** Указывает на первый байт срочных данных в пакете.
- **Параметры.** Различные дополнительные параметры TCP.
- **Данные.** Информация верхнего уровня.

Протокол UDP

Протокол передачи дейтаграмм пользователя UDP (User Datagram Protocol — UDP) представляет собой протокол транспортного уровня (уровень 4), не требующий подтверждения соединения, и принадлежащий семейству протоколов Internet. В сущности, UDP является интерфейсом между IP и протоколами верхнего уровня. Порты протокола UDP различают приложения, запущенные на одном устройстве.

В отличие от TCP, UDP не добавляет IP надежности, управления потоком, или функций исправления ошибок. Из-за простоты UDP его заголовки короче и требуют меньше сетевых ресурсов, чем TCP.

UDP полезен в ситуациях, когда мощные механизмы обеспечения надежности протокола TCP не обязательны, например, когда управление потоком и коррекцию ошибок можно возложить на протокол верхнего уровня.

UDP является транспортным протоколом для нескольких известных протоколов уровня приложений, в том числе NFS, SNMP, DNS и TFTP.

Как показано на рис. 35.11, формат пакета UDP содержит четыре поля: порт источника, порт получателя, длина и контрольная сумма.

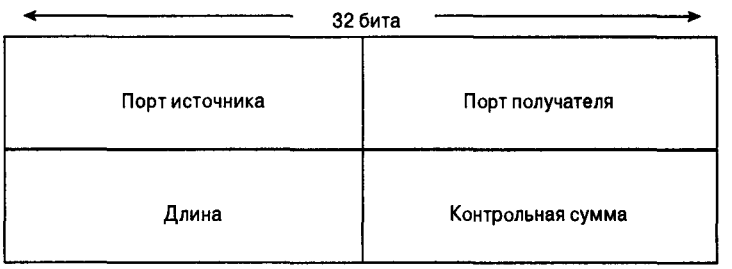


Рис. 35.11. Заголовок пакета UDP

Поля портов источника и получателя содержат 16-разрядные номера портов протокола UDP для демультиплексирования дейтаграмм при приеме процессов уровня приложений. Поле длины определяет размер UDP-заголовка и данных. Поле контрольной суммы может служить для проверки целостности UDP-заголовка и данных.

Internet-протоколы уровня приложений

В набор протоколов Internet входит много протоколов уровня приложений, в том числе следующие протоколы.

- **FTP Протокол передачи файлов (File Transfer Protocol — FTP).** Обеспечивает способ передачи файлов между компьютерными системами.
- **SNMP Простой протокол сетевого управления (Simple Network Management Protocol — SNMP).** Сообщает об аномальных условиях в сети и устанавливает пределы допустимых значений.
- **Telnet.** Протокол эмуляции терминала.
- **X Windows.** Распределенная оконная и графическая система для обмена данными между X-терминалами и рабочими станциями UNIX.
- **NFS Сетевая файловая система (Network File System — NFS), представление внешней информации XDR (External Data Representation — XDR) и удаленный вызов процедуры RPC (Remote Procedure Call — RPC).** Вместе они обеспечивают прозрачный доступ к ресурсам удаленной сети.
- **SMTP Простой протокол передачи электронной почты (Simple Mail Transfer Protocol — SMTP).** Обеспечивает услуги электронной почты.
- **DNS Служба доменных имен (Domain Name System — DNS).** Преобразует имена сетевых узлов в сетевые адреса.

Эти протоколы верхнего уровня и поддерживаемые ими приложения перечислены в табл. 35.5.

Таблица 35.5. Протоколы верхнего уровня и их приложения

Приложения	Протоколы
Передача файлов	FTP
Управление сетью	SNMP
Эмуляция терминала	Telnet
Распределенные файловые службы	NFS, XDR, RPC, X Windows
Электронная почта	SMTP
Распределенные службы имен	DNS

Резюме

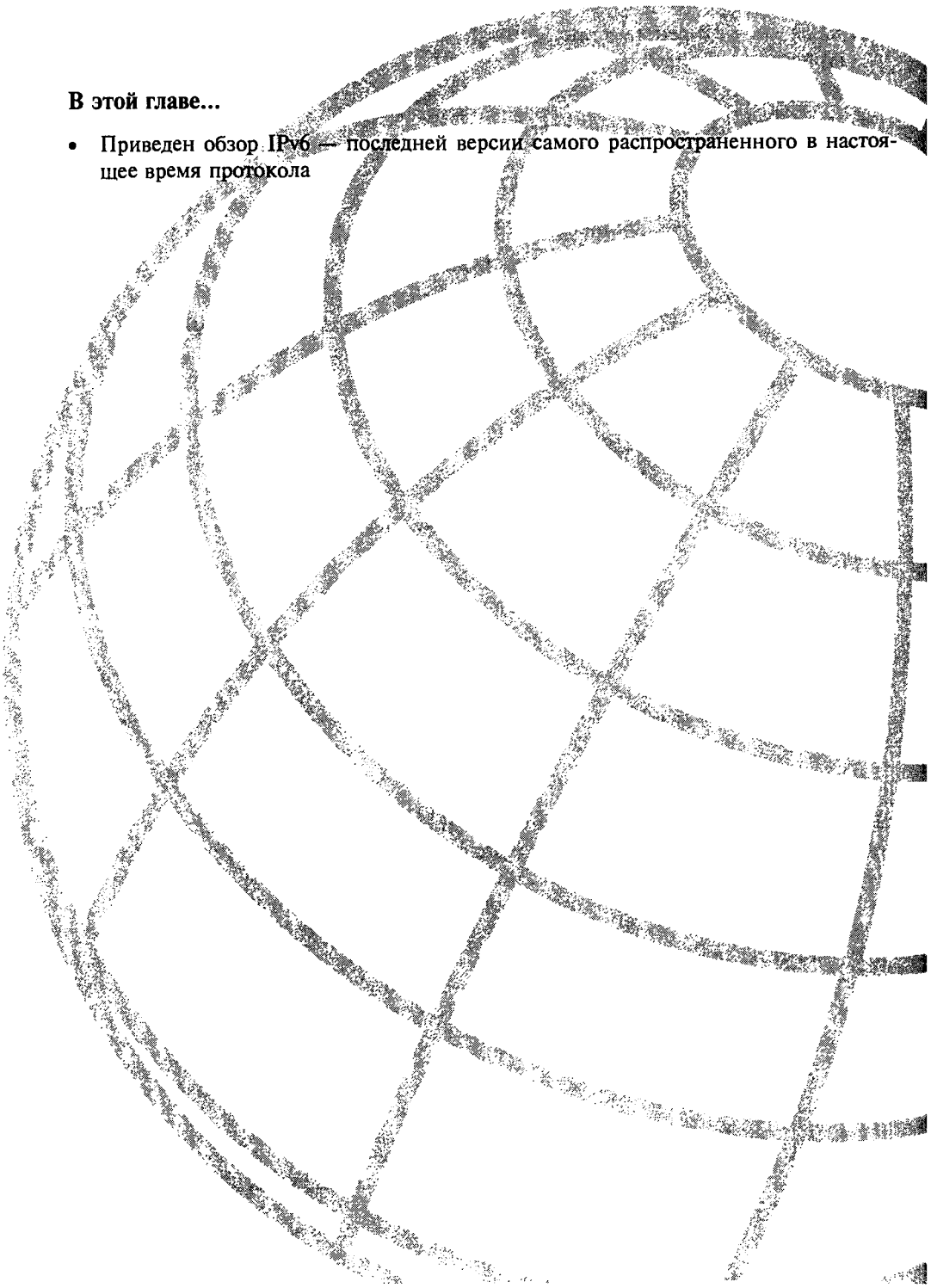
TCP/IP определяет большой набор широко используемых в настоящее время протоколов. IP-адреса применяются в Internet для доставки данных на компьютеры по всему миру. В набор протоколов входят транспортные протоколы, такие как TCP/IP, обеспечивающие гарантированную, ориентированную на соединение, доставку данных. В набор входят и транспортные протоколы, не требующие подтверждения соединения, наподобие UDP, обеспечивающие более быструю доставку данных, а также протоколы уровня приложений, соответствующие открытым стандартам. Эти открытые стандарты и простота взаимодействия между компьютерными системами являются причинами столь широкого распространения TCP/IP в настоящее время.

Контрольные вопросы

1. Где содержатся описания протоколов Internet?
2. Каковы две основные задачи IP?
3. Какое поле IP-пакета предотвращает зацикливание пакетов в неверно сконфигурированной сети?
4. В каком виде обычно представляется IP-адрес?
5. Как определяется класс IP-адреса?
6. Каково назначение маски подсети в IP-адресе?
7. Каково назначение протокола ARP?
8. Каково назначение протокола ICMP?
9. Какой тип доставки данных предоставляет TCP?
10. Чем протокол UDP отличается от протокола TCP?

В этой главе...

- Приведен обзор IPv6 — последней версии самого распространенного в настоящее время протокола



Глава 36

Протокол IPv6

Протокол IPv6 является одним из основных новейших стандартов. Несмотря на то, что официально он еще не признан, он заслуживает внимания. Вполне возможно, что к моменту утверждения IPv6 представленная здесь информация устареет, поэтому ее следует использовать как руководство по IPv6, но не как точные сведения.

В настоящее время выходит много книг, посвященных подробному описанию этого нового стандарта. В них можно получить более подробную информацию о данном протоколе. Развитие этого стандарта отражается в RFC, доступных в Internet. Однако понять такие документы сразу непросто: чтобы разобраться во многочисленных RFC, касающихся разных аспектов разработки IPv6, требуется некоторая предварительная подготовка.

На сегодняшний день самой распространенной является четвертая версия протокола IP (Internet Protocol Version 4, см. главу 35 "Протоколы Internet"). Однако уже сейчас возникают сомнения насчет его возможности обслуживать сообщество Internet в будущем. Окончательный вариант IPv4 был создан в 70-х гг. XX века, и его возраст начинает сказываться. Основная причина выпуска IPv6 — адресация, а точнее — недостаток адресов, поскольку многие эксперты полагают, что 4 миллиарда адресов, доступных в IPv4, вскоре будут исчерпаны. На первый взгляд это число кажется очень большим, однако много больших блоков адресов выделены правительственным службам и крупным организациям. IPv6 мог бы решить многие проблемы, однако, к сожалению, он еще не до конца разработан и не является стандартом.

Над IPv6 работали лучшие разработчики и инженеры с начала 90-х гг. Были написаны сотни RFC с подробным описанием основных тем, в том числе таких как расширенная адресация, упрощенный формат заголовка, метки потоков, аутентификация и обеспечение конфиденциальности.

Расширенная адресация означает переход от 32-разрядных к 128-разрядным адресам. Кроме того, она поддерживает новейшие методы одноадресатной и широковещательной передачи данных, вводит шестнадцатеричные IP-адреса и новые разделители: вместо точки (".") используется двоеточие (":"). Формат заголовка пакета IPv6 показан на рис. 36.1.

Заголовок пакета IPv6

Длина упрощенного заголовка составляет 40 битов. Он состоит из полей версии, класса, метки потока, длины поля полезной нагрузки, следующего заголовка,

максимально допустимого количества переходов, адреса источника, адреса получателя, данных и полезной нагрузки.

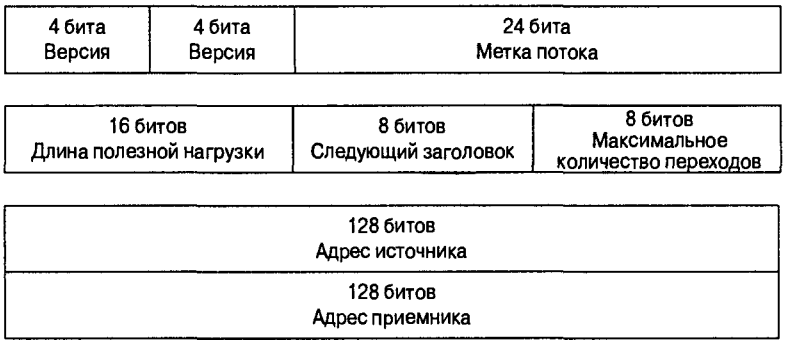


Рис. 36.1. Формат заголовка пакета IPv6

Шестнадцатеричный формат

Как известно, шестнадцатеричные числа представляет собой запись чисел с основанием 16, подобно тому как десятичные числа записываются по основанию 10. В десятичной системе счет идет от 0 до 9, после чего появляется единица в старшем разряде и получается 10. В шестнадцатеричной системе счет идет от 0 до F. Значения от A до F соответствуют десятичным значениям от 10 до 15 (рис. 36.2).

Основание 10	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Основание 16	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F

Рис. 36.2. Шестнадцатеричные значения от A до F соответствуют десятичным числам от 10 до 15

Счет выглядит следующим образом: 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 и т.д.

Адресация

Рассмотрим пример адреса IPv6. Этот шестнадцатеричный адрес состоит из восьми частей, разделенных двоеточиями. Каждая часть с номером *n* может представлять собой 16-битовое число, а 8 таких частей обеспечивают адрес длиной 128 битов (16×8 = 128).

Адрес представляет собой число вида n:n:n:n:n:n:n:n, где n — 4-разрядное шестнадцатеричное целое число, в результате получается 128-разрядный адрес (16×8 = 128).

Способы передачи

В IPv6 предусмотрены следующие новые способы передачи:

- одноадресатная (unicast);
- многоадресатная (multicast);
- широковещательная (anycast).

Одноадресная передача

Одноадресатная передача (unicast) представляет собой обмен данными между одним узлом и одним получателем. Посылаемые по единичному адресу пакеты доставляются интерфейсу, определяемому этим адресом, как показано на рис. 36.3.

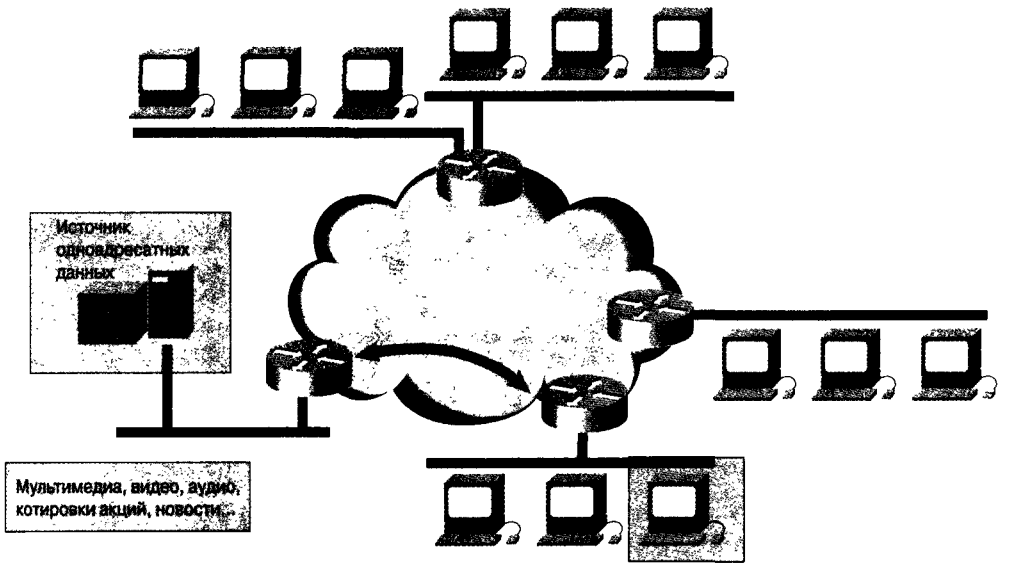


Рис. 36.3. При одноадресатной передаче пакеты пересылаются на определенный интерфейс

Многоадресатная передача

При многоадресатной передаче (multicast) происходит обмен данными между одним узлом и несколькими получателями. Пакеты передаются на все интерфейсы, идентифицируемые этим групповым адресом (рис. 36.4).

Широковещательная передача

При широковещательной передаче (anycast) пакеты доставляются ближайшему интерфейсу, идентифицируемому данным адресом. Широковещательная передача представляет собой обмен данными между одним отправителем и несколькими получателями, определяемыми списком адресов (рис. 36.5).

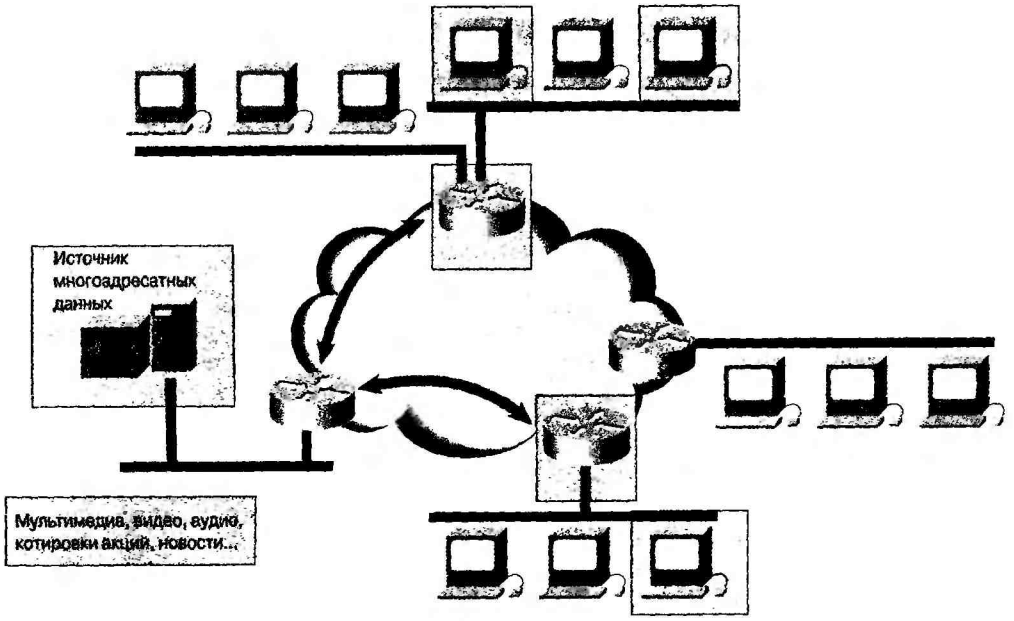


Рис. 36.4. При многоадресатной передаче пакеты направляются всем узлам некоторой подсети и принимаются ожидающими их устройствами

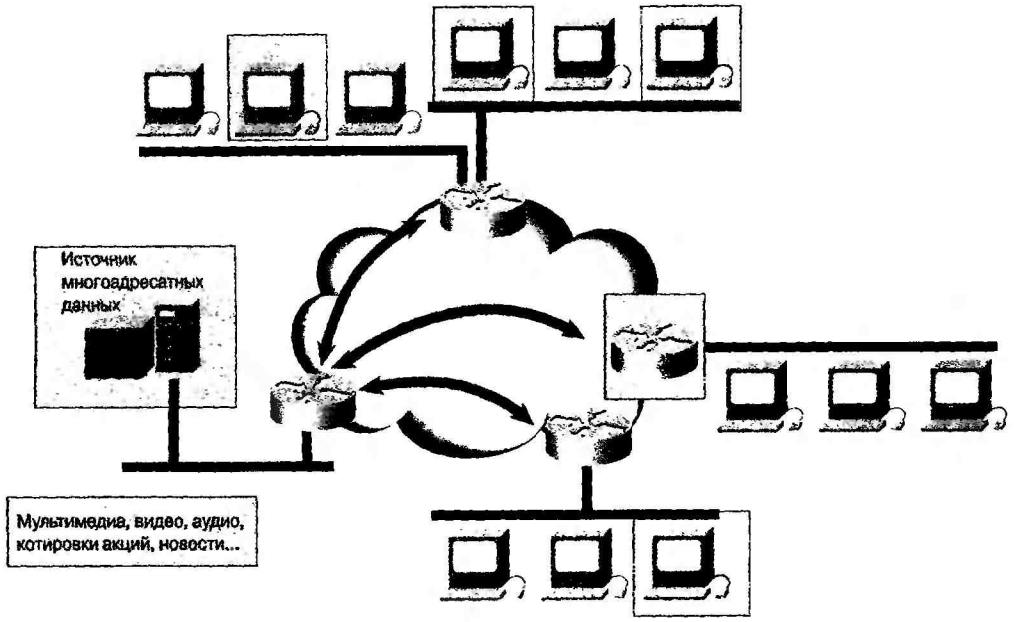


Рис. 36.5. При широковещательной передаче пакеты отправляются на определенный список адресов, среди которых могут быть как конечные узлы, так и маршрутизаторы

Резюме

Некоторые преимущества IPv6 очевидны: увеличенное адресное пространство, встроенное обеспечение качества обслуживания (QoS), улучшенная маршрутизация и расширение диапазона служб. Однако для практической реализации протокола IPv6 требуется преодолеть ряд препятствий. Главное для большинства пользователей— решить вопрос: в чем состоит необходимость перехода с IPv4 на IPv6? Приложение, которое настоятельно этого потребует, еще не появилось, но оно может появиться скорее, чем кажется. Второй вопрос — стоимость. Возможно, все обойдется заменой оборудования, что не так уж дорого. У всех крупных маршрутизаторов есть возможность обновления операционной системы IOS, что, очевидно, и потребуется сделать. Вероятно, больше работы потребуют второстепенные сетевые устройства, такие как принтеры и сетевые факсы. Их нужно будет настроить таким образом, чтобы они поддерживали новое адресное пространство. Однако в протоколе IPv6 предусмотрены схемы поддержки старого и нового адресных пространств, так что это, вероятно, не будет препятствием. Последний вопрос — обучение персонала. Рано или поздно это произойдет, поскольку всем пользователям сетей пора привыкать к 128-разрядной адресации, основанной на шестнадцатеричных MAC-адресах. Это затрагивает все новые сферы адресации и для многих станет дискомфортным изменением.

Подобный вывод может показаться отрицательным, однако достоинства IPv6 должны перевесить все проблемы переходного периода. Вопрос состоит не в том, стоит ли переходить на IPv6, а в том, когда это нужно делать. Четырехкратное расширение адресного пространства необходимо развивающимся областям применения IP, о которых можно услышать еженедельно. Уже сейчас производятся IP-автомобили. Это требует мобильности, которая обеспечивается протоколом IPv6.

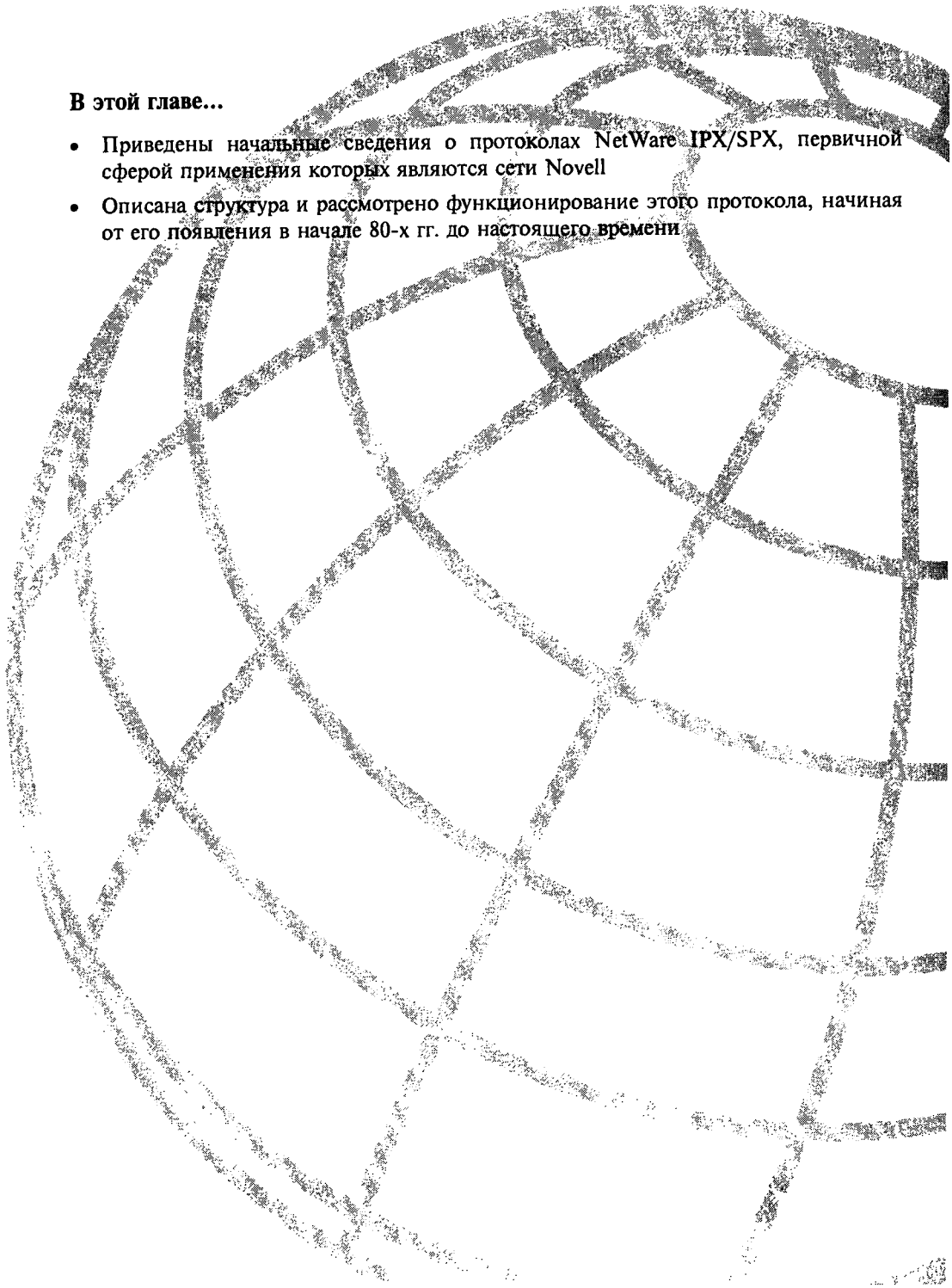
Конечно, в данном разделе не были рассмотрены некоторые важные свойства IPv6, такие как качество обслуживания, мобильный IP, автоконфигурация и безопасность. Все эти темы очень важны, однако, пока работа над IPv6 не закончена, за самой последней информацией по ним следует обратиться на Web-узлы IETF. Кроме того, сейчас появляются новые книги о IPv6, где более подробно описываются заголовки адресов и формат пакетов IPv6.

Контрольные вопросы

1. Какой стандарт принят в настоящее время?
2. Что является основной причиной разработки IPv6?
3. Сколько битов использует новая расширенная адресация?
4. В чем состоят другие преимущества расширенной адресации?
5. Какие новые способы передачи появились в IPv6?
6. Что такое одноадресатная передача?
7. Что такое многоадресатная передача?
8. Что такое широковещательная передача?

Дополнительные источники

- http://www-6bone.lbl.gov/6bone
- http://www.cisco.com/warp/customer/732/ipv6/index.html
- http://www.ietf.org/html.charters/ipngwg-charter.html
- http://playground.Sun.COM:80/pub/ipng/html



В этой главе...

- Приведены начальные сведения о протоколах NetWare IPX/SPX, первичной сферой применения которых являются сети Novell
- Описана структура и рассмотрено функционирование этого протокола, начиная от его появления в начале 80-х гг. до настоящего времени

Глава 37

Протоколы NetWare

Введение

NetWare представляет собой сетевую операционную систему (Network Operating System — NOS), обеспечивающую прозрачный удаленный доступ к файлам и другие многочисленные распределенные сетевые службы, в том числе совместное использование принтеров и поддержку различных приложений, таких как передача электронной почты и доступ к базам данных. Протоколы NetWare соответствуют пяти верхним уровням модели OSI и, следовательно, управляются любым протоколом 2-го (канального) уровня. Кроме того, NetWare работает практически с любыми типами компьютерных систем — от персональных компьютеров до мэйнфреймов. В настоящей главе описаны основные протоколы передачи данных, поддерживаемые NetWare.

Протоколы NetWare были разработаны компанией Novell в начале 80-х гг. Они произошли от сетевого стандарта XNS (Xerox Network Systems), созданного корпорацией Xerox в конце 70-х гг. и основанного на архитектуре "клиент/сервер". Клиенты (иногда называемые рабочими станциями) посылают серверам запросы на обслуживание, такое как доступ к файлу или принтеру.

Клиент-серверная архитектура NetWare поддерживает прозрачный для пользователя удаленный доступ через вызовы удаленных процедур. Удаленный вызов процедуры происходит в тот момент, когда программа, работающая на локальном компьютере клиента, посылает вызов процедуры удаленному серверу. Затем сервер выполняет удаленно вызванную процедуру и возвращает требуемую информацию локальному клиенту.

На рис. 37.1 показаны стек протоколов NetWare, протоколы доступа к среде передачи, на базе которых работают протоколы NetWare и взаимосвязь между протоколами NetWare и эталонной моделью OSI. Компоненты этих протоколов и их функционирование рассматриваются ниже.

Доступ NetWare к среде передачи

Стек протоколов NetWare поддерживает несколько протоколов доступа к среде передачи (2-й уровень), в том числе Ethernet/IEEE 802.3, Token Ring/IEEE 802.5, FDDI и PPP. Различные способы доступа к среде передачи NetWare показаны на рис. 37.2.

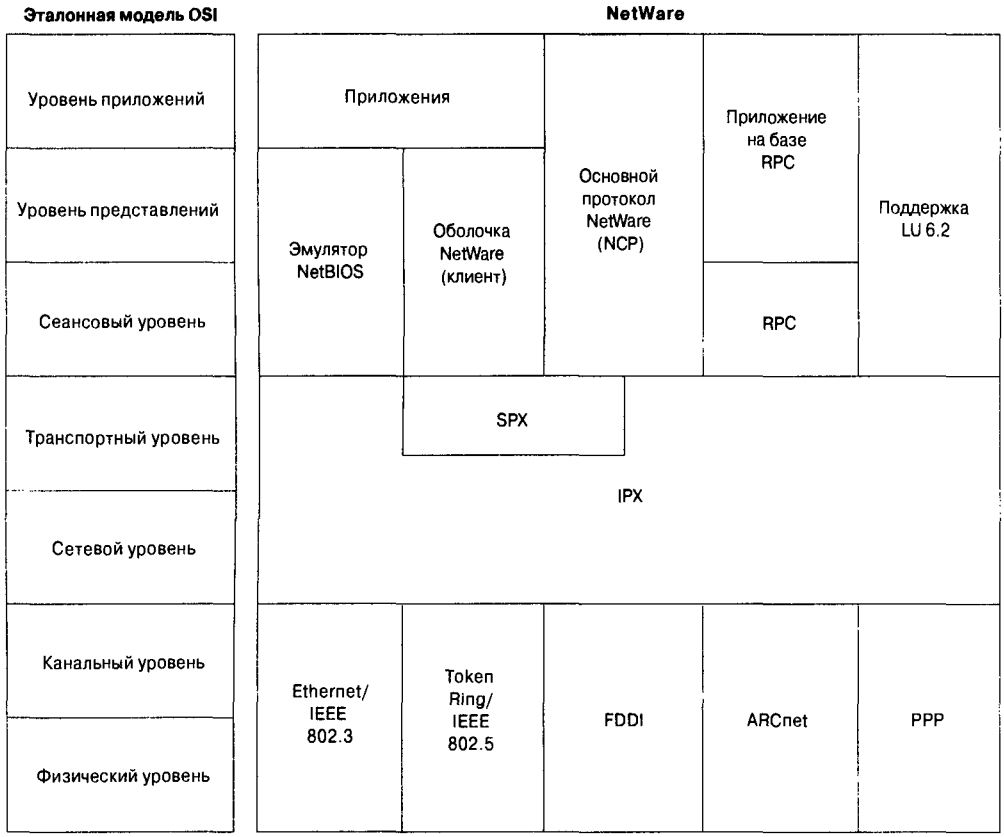


Рис. 37.1. Набор протоколов NetWare полностью соответствует уровням OSI

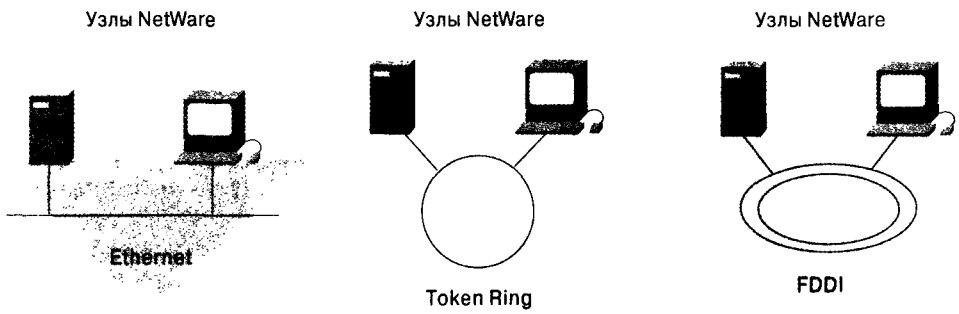


Рис. 37.2. NetWare поддерживает наиболее распространенные протоколы доступа к среде передачи

Основные сведения о протоколе IPX

Протокол межсетевого пакетного обмена IPX (Internetwork Packet Exchange — IPX) представляет собой оригинальный протокол NetWare 3-го (сетевого) уровня, используемый для маршрутизации пакетов между сетями. IPX представляет собой

дейтаграммный сетевой протокол, не требующий подтверждения соединения и, следовательно, аналогичен протоколу IP, используемому в сетях TCP/IP.

IPX использует службы протокола маршрутной информации RIP (Routing Information Protocol — RIP) или протокола канальных служб в среде NetWare (NetWare Link-State Protocol — NLSP). Протокол RIP IPX рассылает обновленную информацию о маршрутах каждые 60 с. Для выбора наилучшего маршрута IPX RIP использует в качестве единицы измерения времени *интервалы таймера* или *такты* (tick), которые, в сущности, являются ожидаемой задержкой для маршрута определенной длины. Один интервал таймера составляет 1/18 с. Если обнаружатся два маршрута с одинаковым количеством таких интервалов, то протокол IPX RIP осуществляет выбор одного из них по количеству прохождений пакета через маршрутизатор (hop). Протокол IPX RIP несовместим с реализациями RIP, используемыми в других сетевых средах.

Подобно другим сетевым адресам, адреса сети Novell IPX должны быть уникальными. Эти адреса представлены в шестнадцатеричном формате и состоят из двух частей: номера сети и номера узла. Номер сети IPX назначается сетевым администратором и имеет длину 32 бита. Номер узла обычно является MAC-адресом одного из системных сетевых адаптеров (Network Interface Card — NIC) и его длина составляет 48 битов.

Использование протоколом IPX MAC-адреса позволяет системе предсказывать MAC-адреса передающих узлов, применяемых в канале передачи данных. (В отличие от IP-сетей, в которых часть IP-адреса, определяющая адрес узла, не связана с MAC-адресом, вследствие чего IP-узлы для определения MAC-адреса получателя должны использовать протокол преобразования адресов [Address Resolution Protocol — ARP]).

Типы инкапсуляции протокола IPX

Протокол Novell NetWare IPX поддерживает несколько схем инкапсуляции на одном интерфейсе маршрутизатора, что позволяет присваивать сети несколько номеров. Инкапсуляция представляет собой процесс упаковки информации протокола верхнего уровня и данных в фреймы. NetWare поддерживает следующие четыре схемы инкапсуляции.

- **Фирменная схема Novell,** также называемая исходной схемой 802.3, или Novell Ethernet_802.3. Является первоначальной схемой инкапсуляции, используемой ОС Novell. Она включает в себя поле длины по спецификации IEEE, но не включает заголовок IEEE 802.2 (LLC). Сразу за полем длины спецификации 802.3 следует заголовок IPX.
- **Схема 802.3,** называемая также Novell_802.2. Является стандартом IEEE 802.3 для формата фреймов.
- **Ethernet, 2-я версия,** называемая также Ethernet-II или ARPA. Ethernet 2 включает в себя стандартный заголовок Ethernet версии 2, состоящий из полей адреса отправителя и получателя, после которых находится поле EtherType.
- **SNAP,** называемая также Ethernet_SNAP. Дополняет заголовок IEEE 802.2 типом кода, аналогичным тому, который был определен в спецификации Ethernet 2.

Эти типы инкапсуляции показаны на рис. 37.3.

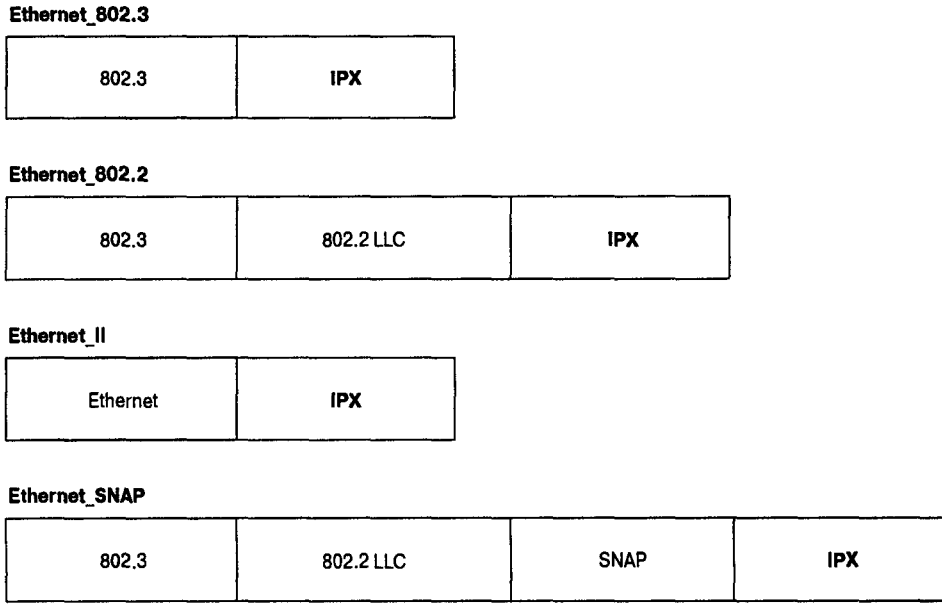


Рис. 37.3. Типы инкапсуляции протокола IPX

Протокол SAP

Протокол анонсирования службы (Service Advertisement Protocol — SAP) представляет собой протокол стека IPX, по которому сетевые ресурсы, такие как файловые серверы и серверы печати, анонсируют свои адреса и предоставляемые службы. Согласно протоколу SAP извещения рассылаются каждые 60 секунд. Службы идентифицируются шестнадцатеричным номером, называемым SAP-идентификатором (например, 4 — файловый сервер, 7 — сервер печати).

Протокол SAP начинает функционировать, когда маршрутизаторы "прослушивают" сообщения SAP и формируют таблицу всех известных служб и соответствующих им сетевых адресов. Затем каждые 60 секунд маршрутизаторы рассылают свои SAP-таблицы. Клиенты Novell могут послать запрос на доступ к отдельному файлу, принтеру или шлюзовой службе. Локальный маршрутизатор отвечает на запрос, сообщая сетевой адрес запрашиваемой службы, после чего клиент может непосредственно подключиться к службе.

В настоящее время SAP распространен в сетях на базе NetWare 3.11 и более ранних версий, реже — в сетях NetWare 4.0, поскольку рабочие станции могут размещать службы по согласованию с сервером службы каталогов NetWare (NetWare Directory Service — NDS). Тем не менее, протокол SAP все же требуется рабочим станциям в сетях NetWare 4.0 во время запуска для нахождения сервера NDS.

Фильтры SAP

Благодаря идентификатору протокола SAP извещения SAP могут быть отфильтрованы входными и выходными портами маршрутизаторов или фильтроваться как поступающие от определенного маршрутизатора. Фильтры SAP предохраняют сеть от перегрузки и особенно полезны в больших сетях Novell, с сотнями служб SAP.

Обычно применение фильтров SAP рекомендуется для служб, не требующих отдельной сети. Например, удаленным узлам, возможно, нет необходимости получать извещения о службах печати, расположенных на центральном узле. Выходной фильтр SAP на центральном узле (предпочтительный вариант) или входной фильтр SAP, использующий идентификатор SAP для сервера печати на удаленном узле, не позволит маршрутизатору включить службы печати в обновления SAP.

Транспортный уровень NetWare

Протокол последовательного обмена пакетами (Sequenced Packet Exchange — SPX) является наиболее распространенным транспортным протоколом NetWare 4-го уровня эталонной модели OSI. В наборе протоколов NetWare SPX располагается выше IPX. SPX является надежным протоколом, ориентированным на соединение, дополняющим службу дейтаграмм протокола IPX 3-го (сетевого) уровня. Протокол SPX является развитием протокола передачи последовательных пакетов (Sequenced Packet Protocol — SPP) сетевого стандарта Xerox (Xerox Network Systems — XNS). Стандарт Novell также поддерживает передачу данных протокола Internet с помощью протокола передачи дейтаграмм пользователя UDP (User Datagram Protocol — UDP). Дейтаграммы IPX инкапсулируются в заголовки UDP/IP для транспортировки по объединенным IP-сетям.

Протоколы и службы верхнего уровня NetWare

NetWare поддерживает широкий спектр протоколов верхнего уровня, в том числе оболочку NetWare (NetWare Shell), удаленный вызов процедур NetWare (NetWare Remote Procedure Call), базовый протокол NetWare (NetWare Core Protocol) и базовую сетевую систему ввода/вывода (Network Basic Input/Output System).

Оболочка NetWare запускает работу клиентов (которых специалисты по NetWare часто называют рабочими станциями) и перехватывает вызовы ввода/вывода (Input/Output — I/O) приложений, чтобы определить необходимость доступа к сети для их выполнения. Если приложение запрашивает доступ к сети, то оболочка NetWare пакетирует запрос и отсылает его программному обеспечению нижнего уровня для обработки и передачи по сети. Если запрос приложения не требует доступа к сети, то он передается локальным ресурсам ввода/вывода. Клиентские приложения не имеют информации о доступе к сети, необходимом для выполнения их вызовов.

Удаленный вызов процедур NetWare (NetWare Remote Procedure Call — NetWare RPC) представляет собой другой поддерживаемый Novell распространенный механизм переадресации, по своей концепции похожий на оболочку NetWare.

Базовый протокол NetWare (NetWare Core Protocol — NCP) представляет собой набор серверных процедур для обслуживания запросов приложений, поступающих, например, от оболочки NetWare. В число служб NPC входят доступ к файлам и принтерам, управление именами, системы учета использования ресурсов, системы защиты и файловая синхронизация.

Кроме того, NetWare поддерживает интерфейс сеансового уровня NetBIOS спецификаций IBM и Microsoft. Программы эмуляции NetWare NetBIOS позволяют выполнять

в среде NetWare программы, написанные для промышленного стандарта интерфейса NetBIOS.

Службы NetWare уровня приложений

Службами уровня приложений NetWare являются служба обработки сообщений NetWare (NetWare Message-Handling Service — NetWare MHS), механизм двоичного дерева (Btrieve), загружаемые модули NetWare (NetWare Loadable Modules — NLM) и адресуемых сетевых элементов (Network-Addressable Units — NAU) логического блока IBM 6.2 (Logical Unit — LU). Служба MHS NetWare является системой доставки сообщений, обеспечивающей передачу сообщений электронной почты. Btrieve представляет собой реализацию Novell-механизма двоичного дерева (binary tree — btree) для доступа к базе данных. Элементы NLM являются дополнительными модулями, подключаемыми к системе NetWare. В настоящее время существуют NLM производства Novell и других производителей, в том числе альтернативные стеки протоколов, службы связи и баз данных. В аспекте поддержки элементов NAU IBM LU 6.2 NetWare обеспечивает соединения по схеме "точка-точка" и обмен информацией по сетям IBM. Для прохождения по сети IBM пакеты NetWare инкапсулируются в пакеты LU 6.2.

Формат пакета IPX

Пакеты IPX являются основным элементом обеспечения межсетевого обмена ОС Novell NetWare. Формат пакета IPX NetWare показан на рис. 37.4.

Структура IPX-пакета

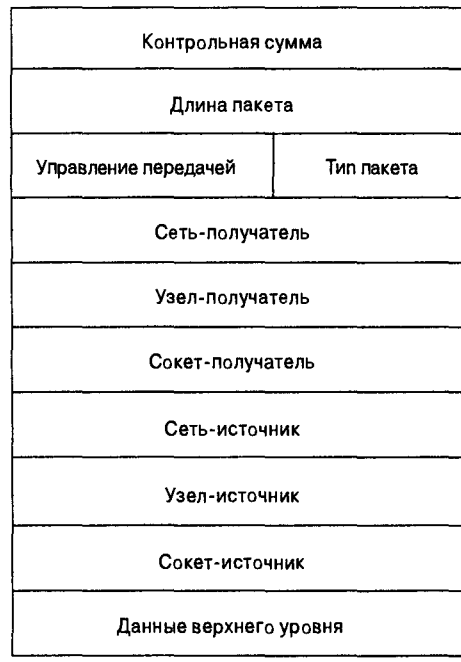


Рис. 37.4. Пакет IPX NetWare

Ниже описаны поля пакета IPX, показанные на рис. 37.4.

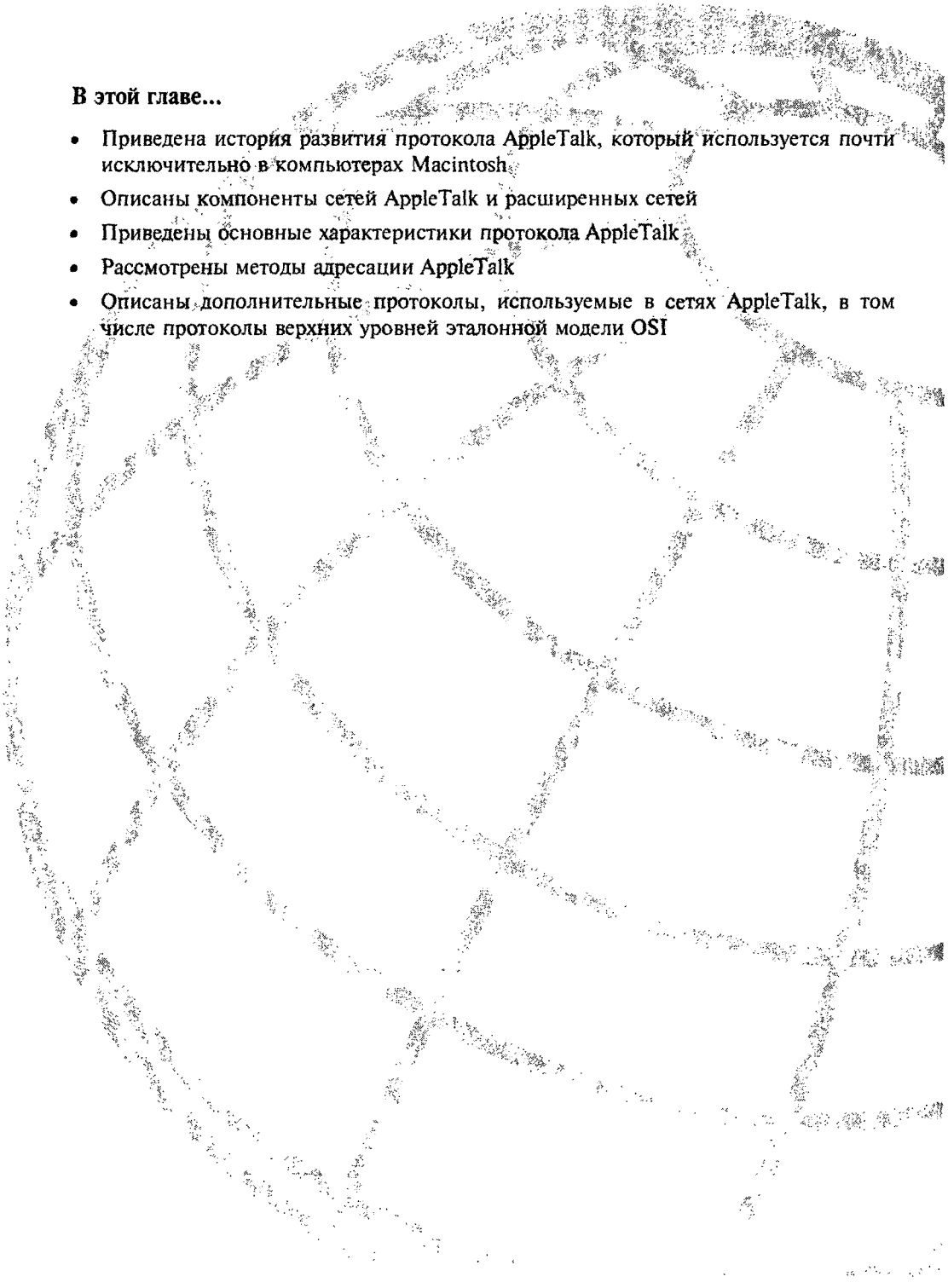
- **Контрольная сумма.** Если все 16 бит этого поля равны 1 (FFFF), то контрольная сумма не используется.
- **Длина пакета.** Длина полной схемы IPX в байтах. Пакеты IPX могут быть любой длины, насколько позволяет максимальный размер передаваемого модуля (Maximum Transmission Unit — MTU) в среде передачи данных. Фрагментация пакетов не допускается.
- **Управление передачей.** Количество маршрутизаторов, через которые прошел пакет. Когда эта величина достигает 16, пакет отбрасывается из-за предположения о возможной маршрутной петле.
- **Тип пакета.** Определяет, какой протокол верхнего уровня должен принять информацию из пакета. Обычно это поле принимает одно из двух значений:
  - 5 — протокол SPX;
  - 17 — протокол NCP.
- **Сеть-получатель, узел-получатель и сокет-получатель.** Информация о получателе.
- **Сеть-источник, узел-источник и сокет-источник.** Информация об источнике.
- **Данные верхнего уровня.** Информация для процессов верхнего уровня.

Резюме

Протоколы IPX до сих пор используются в миллионах компьютеров в сетях NetWare. Однако в этой среде происходит значительное смещение от протокола IPX в сторону протокола IP, и тенденция поддержки протокола IP в сетевом окружении Novell, вероятно, будет продолжаться.

Контрольные вопросы

1. Какие два типа протоколов маршрутизации используются протоколом IPX.
2. Какая информация используется протоколом RIP IPX для определения маршрута передачи данных по сети?
3. На какие две части делится адрес IPX?
4. Как станции Novell обнаруживают доступные в сети службы?
5. Какой протокол используется на транспортном уровне?
6. Как станции IPX преобразуют MAC-адреса в адреса протокола IPX?
7. Какое нововведение в NetWare 4.0 уменьшает необходимость в протоколе SAP?
8. Какие службы обеспечиваются базовым протоколом NetWare (NetWare Core Protocol)?
9. Опишите поддержку NetBIOS в сетях NetWare.
10. Необходимо ли фильтровать данные протокола SAP?



В этой главе...

- Приведена история развития протокола AppleTalk, который используется почти исключительно в компьютерах Macintosh
- Описаны компоненты сетей AppleTalk и расширенных сетей
- Приведены основные характеристики протокола AppleTalk
- Рассмотрены методы адресации AppleTalk
- Описаны дополнительные протоколы, используемые в сетях AppleTalk, в том числе протоколы верхних уровней эталонной модели OSI

Глава 38

Протоколы AppleTalk

Введение

AppleTalk представляет собой набор протоколов, разработанный фирмой Apple Computer в начале 1980-х гг. в связи с появлением компьютеров Macintosh. Протоколы AppleTalk создавались с целью дать возможность нескольким пользователям совместно использовать такие ресурсы, как файлы и принтеры. Устройства, предоставляющие данные ресурсы, называются серверами, а устройства, использующие эти ресурсы (например, пользовательские компьютеры Macintosh), — клиентами. Таким образом, AppleTalk является одним из ранних вариантов распределенной сетевой системы "клиент/сервер". В этой главе представлено краткое описание сетевой архитектуры AppleTalk.

Пакет протоколов AppleTalk был спроектирован с прозрачным сетевым интерфейсом. Другими словами, взаимодействие между клиентскими и серверными компьютерами в сети требует минимального вмешательства со стороны пользователя. Кроме того, действительные операции, осуществляемые протоколами AppleTalk, остаются невидимыми для пользователя, которому становятся известны только результаты их выполнения. Существуют две версии AppleTalk: AppleTalk Phase 1 и AppleTalk Phase 2.

Первая спецификация AppleTalk, AppleTalk Phase 1, была разработана в начале 80-х годов специально для локальных рабочих групп. Отсюда следуют два основных ограничения AppleTalk Phase 1. Первое ограничение протокола AppleTalk Phase 1 заключается в том, что в сетевых сегментах такого протокола может содержаться не более 135 узлов и 135 серверов, второе — в том, что он поддерживает только нерасширенные сети. Расширенные и нерасширенные сети будут рассмотрены более подробно в настоящей главе.

Вторая, расширенная реализация AppleTalk, AppleTalk Phase 2, предназначалась для более крупных, объединенных сетей. В AppleTalk Phase 2 были устранены основные ограничения AppleTalk Phase 1 и сделан ряд улучшений. В частности, в AppleTalk Phase 2 допускается произвольная комбинация из 253 узлов или серверов в одном сегменте сети AppleTalk, поддерживаются как нерасширенные, так и расширенные сети.

Компоненты сетей AppleTalk

Сети AppleTalk имеют иерархическую структуру и состоят из четырех основных компонентов: сокетов, узлов, сетей и зон. На рис. 38.1 показана иерархическая организа-

ция этих компонентов в объединенной сети AppleTalk. Каждое из указанных понятий будет кратко описано в следующих разделах.

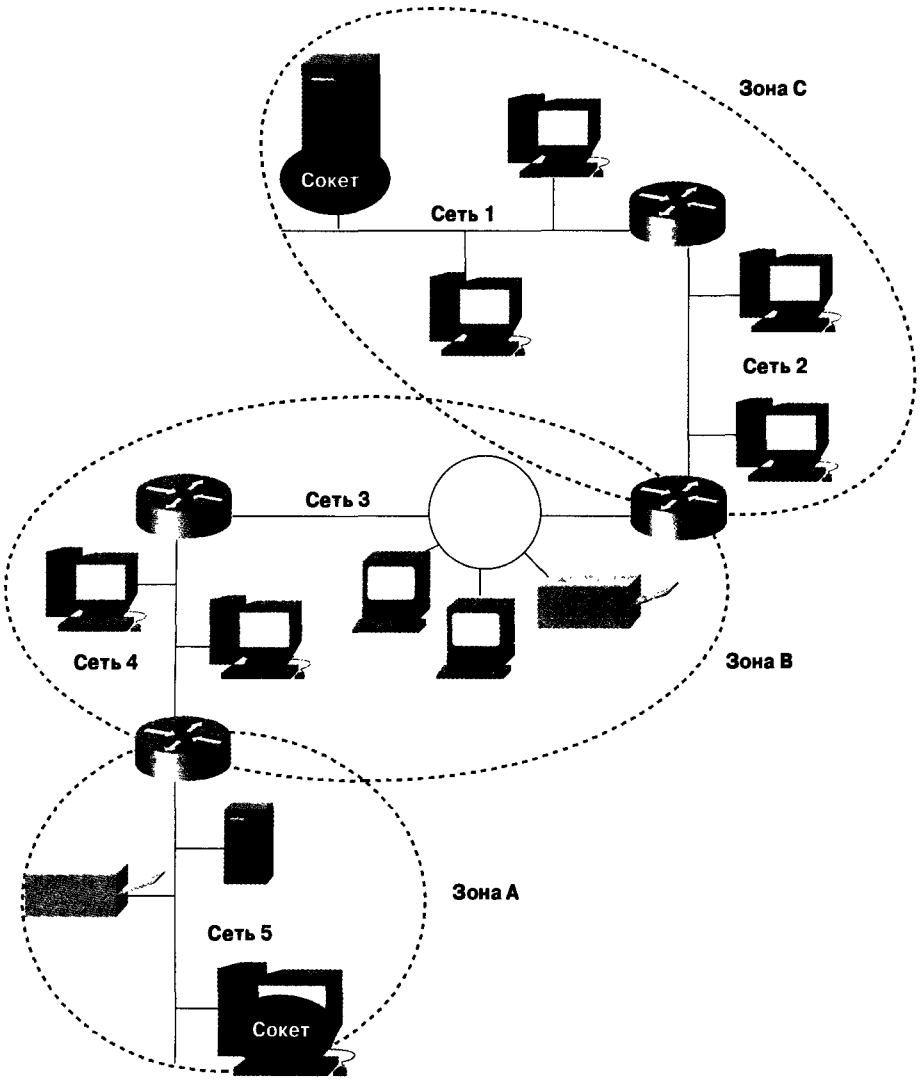


Рис. 38.1. Объединенная сеть AppleTalk состоит из иерархически организованных компонентов

Сокеты

Сокет AppleTalk представляет собой уникально адресуемое место в узле AppleTalk и логическую точку взаимодействия программных процессов AppleTalk верхнего уровня и протокола доставки дейтаграмм (Datagram Delivery Protocol — DDP) сетевого уровня. Такие процессы верхнего уровня называют клиентами сокета. В распоряжении клиентов сокета находится один или несколько сокетов, которые используются для передачи и получения дейтаграмм. Сокеты могут назначаться статически или

динамически. Статически назначаемые сокеты резервируются для использования определенными протоколами или другими процессами. Динамически назначаемые сокеты назначаются клиентам протоколом DDP по запросу. Узел AppleTalk может содержать до 254 различных номеров сокетов. Взаимосвязь между сокетами в узле AppleTalk и DDP на сетевом уровне показана на рис. 38.2.

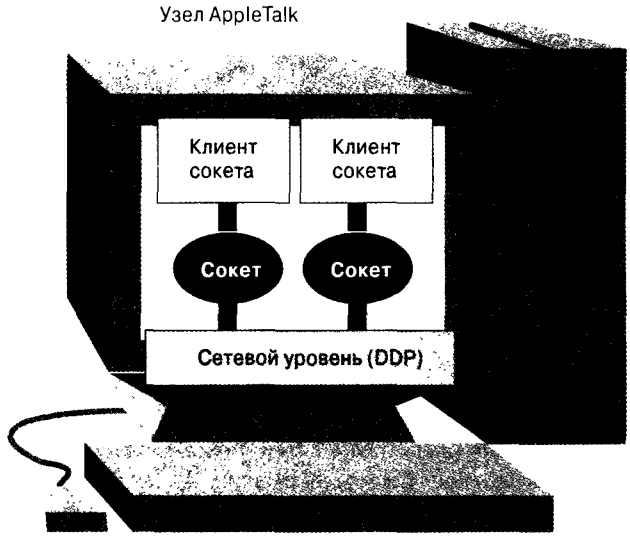


Рис. 38.2. Клиенты сокета используют сокеты для передачи и получения дейтаграмм

Узлы

Под *узлом* AppleTalk понимается устройство, подключенное к сети AppleTalk. Таким устройством может быть компьютер Macintosh, принтер, персональный компьютер IBM, маршрутизатор или другое подобное устройство. В каждом узле AppleTalk происходит ряд программных процессов, называемых сокетами. Как уже отмечалось, назначением этих сокетов является идентификация программных процессов, происходящих в устройстве. Каждый узел в сети AppleTalk принадлежит к одной сети и определенной зоне.

Сети

Сеть AppleTalk состоит из одного логического кабеля и нескольких присоединенных к нему узлов. Логический кабель представляет собой либо единственный физический кабель, либо несколько физических кабелей, соединенных между собой мостами или маршрутизаторами. Сеть AppleTalk может быть нерасширенной или расширенной. Подробнее эти виды сетей описаны в следующих разделах.

Нерасширенные сети

Нерасширенная сеть AppleTalk представляет собой физический сетевой сегмент с общим сетевым номером, который может принимать значения от 1 до 1024. Например, номера 100 и 562 являются допустимыми сетевыми номерами в нерасширенной сети. Каждый номер узла в нерасширенной сети должен быть уникальным, а в сегменте нерасширенной

сети может быть только одна зона AppleTalk. (Зоной называется логическая группа узлов или сетей.) Версия AppleTalk Phase 1 поддерживает только нерасширенные сети. Однако в современных сетях нерасширенные сетевые конфигурации встречаются редко. Их вытесняют расширенные сети. Нерасширенная сеть AppleTalk показана на рис. 38.3.

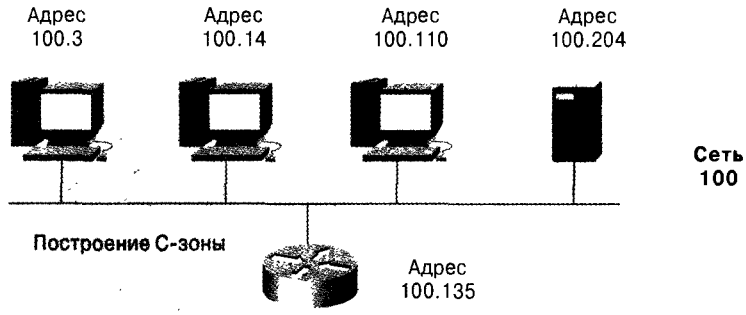


Рис. 38.3. У нерасширенной сети может быть только один сетевой номер

Расширенные сети

Расширенная сеть AppleTalk представляет собой физический сегмент сети, которому может быть присвоено несколько сетевых номеров. Такая конфигурация называется кабельным диапазоном. Кабельные диапазоны AppleTalk могут иметь как один, так и несколько последовательных сетевых номеров. Например, в расширенной сети могут существовать сеть кабельных диапазонов 3-3 (унитарная) и сеть 3-6. Как и в других наборах протоколов, таких как TCP/IP и IPX, каждая комбинация сетевого номера и номера узла в расширенной сети должна быть уникальной, и ее адрес должен однозначно ее идентифицировать. В расширенной сети может быть несколько зон AppleTalk, сконфигурированных в одном сетевом сегменте, и узлы расширенной сети могут принадлежать любой из зон, относящихся к расширенной сети. Как правило, конфигурации расширенных сетей вытесняют конфигурации нерасширенных сетей. Расширенная сеть представлена на рис. 38.4.

Зоны

Зона сети AppleTalk представляет собой логическую группу узлов или сетей, определенную сетевым администратором при конфигурировании сети. Узлы и сети, принадлежащие зоне сети AppleTalk, не обязательно должны быть физически смежными. На рис. 38.5 показана объединенная сеть AppleTalk, состоящая из трех несмежных зон.

Физический и канальный уровни в сетях AppleTalk

Подобно другим распространенным наборам протоколов, например TCP/IP и IPX, доступ к сети в архитектуре AppleTalk зависит от таких протоколов нижнего уровня, как Ethernet, Token Ring и FDDI. В протоколах AppleTalk существует четыре основных метода доступа к сети: EtherTalk, LocalTalk, TokenTalk и FDDITalk.

Рис. 38.4. У расширенной сети может быть несколько сетевых номеров

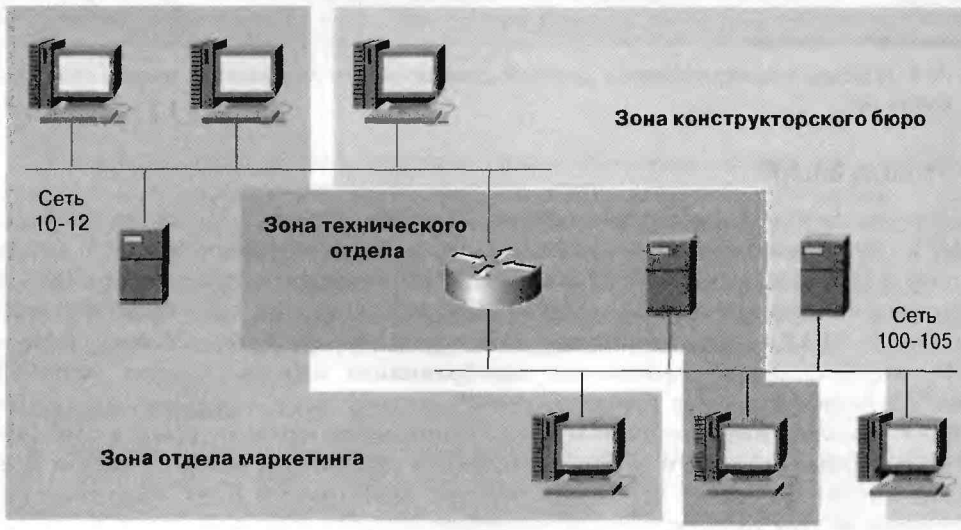


Рис. 38.5. Узлы или сети одной зоны не обязательно должны быть физически смежными

Эти реализации канальных уровней преобразуют адреса и выполняют другие функции, позволяющие собственным протоколам AppleTalk обмениваться данными посредством стандартных промышленных интерфейсов аналогичных интерфейсам IEEE 802.3 (с помощью EtherTalk), Token Ring/IEEE 802.5 (с помощью TokenTalk) и FDDI (с помощью FDDITalk). Кроме того, AppleTalk использует собственный сетевой интерфейс, известный как LocalTalk. На рис. 38.6 показано соответствие реализаций сетевого доступа AppleTalk эталонной модели OSI.

EtherTalk

EtherTalk расширяет канальный уровень, чтобы дать возможность протоколам AppleTalk оперировать на верхнем уровне стандартной реализации IEEE 802.3. Организация сетей EtherTalk в точности повторяет сети IEEE 802.3, поддерживая ту же скорость, размер сегмента и количество активных узлов сети. Это позволяет распространять Apple-

Talk на любую из нескольких тысяч существующих сегодня сетей, построенных на базе Ethernet. Обмен данными между протоколами верхнего уровня архитектуры AppleTalk и протоколами Ethernet управляется протоколом доступа к среде передачи данных EtherTalk (EtherTalk Link Access Protocol — ELAP).

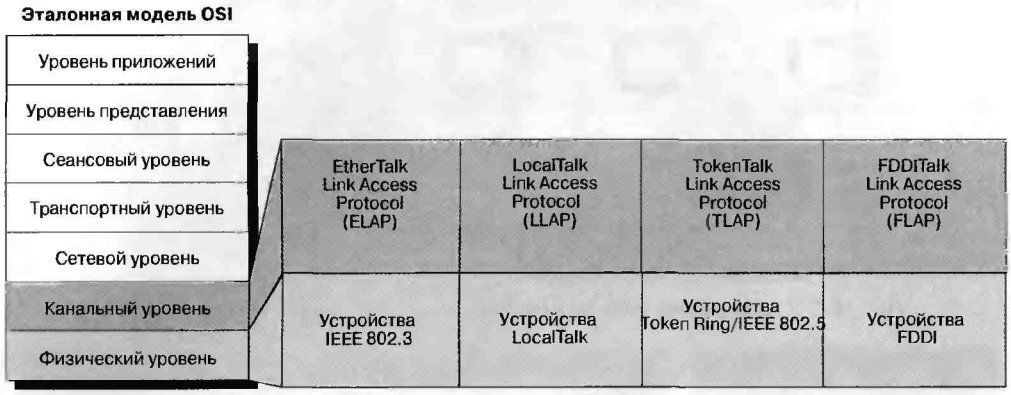


Рис. 38.6. Реализации сетевого доступа AppleTalk соответствуют двум нижним уровням эталонной модели OSI

Протокол ELAP

Протокол доступа к среде передачи данных EtherTalk (EtherTalk Link Access Protocol — ELAP) управляет взаимодействием между собственными протоколами AppleTalk и стандартным канальным уровнем IEEE 802.3. Протоколы верхнего уровня AppleTalk не распознают стандартные адреса устройств IEEE 802.3, поэтому для корректной передачи адресов ELAP использует таблицу соответствий адресов (Address Mapping Table — AMT), поддерживаемую протоколом преобразования адресов в сетях AppleTalk (AppleTalk Address Resolution Protocol — AARP).

ELAP управляет взаимодействием между протоколами верхнего уровня в сетях AppleTalk и канальным уровнем путем инкапсуляции (включения) данных в модули протоколов канального уровня 802.3. При передаче DDP-пакетов ELAP выполняет инкапсуляцию на трех уровнях:

- заголовок протокола доступа к подсети (Subnetwork Access Protocol — SNAP);
- заголовок протокола логического управления каналом IEEE 802.2 (IEEE 802.2 Logical Link Control — LLC);
- заголовок IEEE 802.2.

Этот процесс инкапсуляции, выполняемый протоколом ELAP, более подробно описан в следующем разделе.

Процесс передачи данных в протоколе ELAP

Для передачи данных через физическую среду протокол ELAP использует специальный процесс. Вначале ELAP принимает DDP-пакет, требующий передачи. Затем он находит адрес протокола, обозначенный в DDP-заголовке, и обращается к протоколу AMT для получения адреса соответствующего устройства IEEE 802.3. После этого ELAP помещает в начале DDP-пакета три заголовка: SNAP, 802.2 LLC и IEEE 802.3. При включении

в пакет последнего заголовка в поле адреса получателя помещается адрес устройства, полученный от AMT. Результат — фрейм IEEE 802.3 — помещается в физическую среду для передачи получателю.

Протокол LocalTalk

Протокол LocalTalk, являющийся реализацией канального уровня, разработанной Apple Computer для набора протоколов AppleTalk, был спроектирован как экономичное сетевое решение для связи с локальными рабочими группами. Устройства LocalTalk обычно встраиваются в продукты компании Apple, легко подключаемые к сети посредством недорогой витой пары. Сети LocalTalk организованы на базе шинной топологии, что означает последовательное соединение устройств друг с другом. Длина сегментов сети ограничена 300 метрами, а максимальное количество активных узлов в них не должно превышать 32. Несколько сетей LocalTalk могут соединяться между собой с помощью маршрутизаторов или других подобных промежуточных устройств. Связь между протоколом канального уровня LocalTalk и протоколами верхних уровней осуществляется при помощи протокола доступа к среде передачи данных LocalTalk (LocalTalk Link Access Protocol — LLAP).

Протокол LLAP

Протокол доступа к среде передачи данных LocalTalk (LocalTalk Link Access Protocol — LLAP) представляет собой протокол сетевого доступа, используемый в сетях LocalTalk для обеспечения надежной и безошибочной передачи фреймов между узлами AppleTalk. Это означает, что LLAP не обеспечивает доставку дейтаграмм; такая функция возлагается на протоколы высших уровней сетевой архитектуры AppleTalk. Протокол LLAP отвечает только за управление доступом узлов к физической среде передачи и динамическое получение адресов узлов канальным уровнем.

Управление доступом узлов к физической среде передачи

В протоколе LLAP используется схема доступа к сети, известная как множественный доступ с контролем несущей и обнаружением коллизий (Carrier Sense Multiple Access with Collision Detection — CSMA/CD), посредством которой узлы проверяют канал связи в отношении его занятости. Для того чтобы узел смог начать передачу данных, канал связи должен быть незанятым в течение определенного случайного периода времени. Во избежание коллизий (т.е. одновременной передачи данных двумя и более узлами) протокол LLAP использует обмен данными, известный как квитирование установки соединения. Успешное квитирование установки соединения между узлами эффективно резервирует канал. Если два узла выполняют квитирование одновременно, возникает коллизия. В этом случае оба сообщения повреждаются и пакеты отбрасываются. Квитирование остается незавершенным, и посылающие узлы делают заключение о коллизии. После коллизии устройство остается в бездействии некоторый случайный период времени, а затем повторяет передачу. Этот процесс подобен механизму доступа в Ethernet.

Получение адресов узлов

LLAP получает адреса узлов канального уровня динамически. Данный процесс позволяет назначить канальному уровню уникальный, но не обязательно постоянный

адрес. При создании узла LLAP назначает ему случайным образом выбранный идентификатор узла (ID). Уникальность этого идентификатора определяется путем передачи специального пакета, адресованного случайно выбранному идентификатору узла. Если поступает ответ, значит, такой ID уже существует. Узлу присваивается другой случайный ID, и снова производится посылка пакета; этот процесс повторяется до прекращения получения ответов. Если новый узел не получает ответ на первое сообщение, он делает еще несколько попыток передачи пакета. Если и после такой серии передач ответа не последует, делается заключение об уникальности ID, и узел использует этот ID в качестве своего адреса на канальном уровне.

Протокол TokenTalk

TokenTalk расширяет канальный уровень, чтобы дать возможность набору протоколов AppleTalk работать со стандартной реализацией IEEE 802.5/Token Ring. Сети TokenTalk организованы точно так же, как сети IEEE 802.5/Token Ring, обеспечивают ту же скорость и состоят из такого же количества активных узлов. Связь между протоколами канального уровня, используемыми с Token Ring, и протоколами верхних уровней осуществляется при помощи протокола TLAP.

Протокол TLAP

Протокол доступа к среде передачи данных TokenTalk (TokenTalk Link Access Protocol — TLAP) управляет взаимодействием между собственными протоколами сетей AppleTalk и стандартным канальным уровнем IEEE 802.5. Протоколы верхних уровней в сетях AppleTalk не распознают стандартные адреса устройств IEEE 802.5, поэтому для корректной передачи адресов TLAP использует AMT, поддерживаемую AARP. При передаче DDP-пакетов TLAP выполняет инкапсуляцию на следующих уровнях:

- заголовок протокола SNAP;
- заголовок протокола LLC;
- заголовок IEEE 802.5;
- процесс передачи данных TLAP.

Передача данных TLAP через физическую среду происходит в несколько этапов. При получении DDP-пакета, требующего передачи, TLAP находит в его заголовке адрес протокола и обращается к AMT за адресом соответствующего устройства IEEE 802.5/Token Ring. Затем TLAP помещает в начало DDP-пакета три заголовка: SNAP, 802.2 LLC и IEEE 802.5/Token Ring. После этого в поле адреса получателя помещается адрес устройства, полученный из AMT. Результат, фрейм IEEE 802.5/Token Ring, помещается в физическую среду для передачи получателю.

Протокол FDDITalk

Протокол FDDITalk расширяет канальный уровень, чтобы дать возможность набору протоколов AppleTalk работать со стандартной реализацией ANSI FDDI. Сети FDDITalk организованы подобно сетям IEEE 802.5/Token Ring, обеспечивая ту же скорость и имея то же количество активных узлов сети.

Протокол FLAP

Протокол доступа к среде передачи данных TokenTalk (FDDITalk Link Access Protocol — FLAP) управляет взаимодействием между собственными протоколами в сетях AppleTalk и стандартным канальным уровнем FDDI. Протоколы верхних уровней AppleTalk не распознают стандартные адреса устройств FDDI, поэтому для корректной передачи адресов FLAP использует AMT, поддерживаемую AARP. При передаче DDP-пакетов FLAP выполняет инкапсуляцию на следующих уровнях:

- заголовок протокола SNAP;
- заголовок протокола LLC;
- заголовок FDDI;
- процесс передачи данных FLAP.

Как и TLAP, передача данных через физическую среду при помощи FLAP происходит поэтапно. Получив DDP-пакет, требующий передачи, FLAP находит в заголовке DDP адрес протокола и обращается к AMT за адресом соответствующего устройства FDDI. Затем FLAP присоединяет к началу DDP-пакета три заголовка: SNAP, 802.2 LLC и FDDI. После этого в поле адреса получателя помещается адрес устройства, полученный от AMT. Результат, фрейм FDDI, помещается в физическую среду для передачи получателю.

Сетевые адреса

Для идентификации и обозначения местоположения устройств в сети AppleTalk используются адреса, подобные таким распространенным протоколам, как TCP/IP и IPX. Эти адреса, назначаемые динамически, описываются в следующем разделе. Они состоят из описанных ниже трех элементов.

- **Номер сети.** 16-разрядное число, которое идентифицирует сеть AppleTalk (нерасширенную или расширенную).
- **Номер узла.** 8-разрядное число, идентифицирующее отдельный узел AppleTalk, подключенный к данной сети.
- **Номер сокета.** 8-разрядное число, которое идентифицирует сокет, принадлежащий данному узлу сети.

Адреса сетей AppleTalk обычно записываются в виде десятичных чисел, разделенных точками. Например, 10.1.50 означает сеть 10, узел 1 и сокет 50. Этот адрес может быть записан иным образом: 10.1, сокет 50. Формат сетевого адреса AppleTalk показан на рис. 38.7.

Назначение сетевого адреса

Одной из уникальных характеристик сетей AppleTalk является динамическая адресация устройств. Назначение устройству AppleTalk статического адреса не является обязательным. Адреса узлов AppleTalk назначаются динамически при первом подключении к сети.

При создании сетевой узел AppleTalk получает временный адрес сетевого уровня. Временный адрес сети (первые 16 разрядов) выбирается из начального, зарезер-

вированного, диапазона сетевых адресов (от 65280 до 65534). Временный адрес узла (следующие 8 разрядов) выбирается случайным образом.

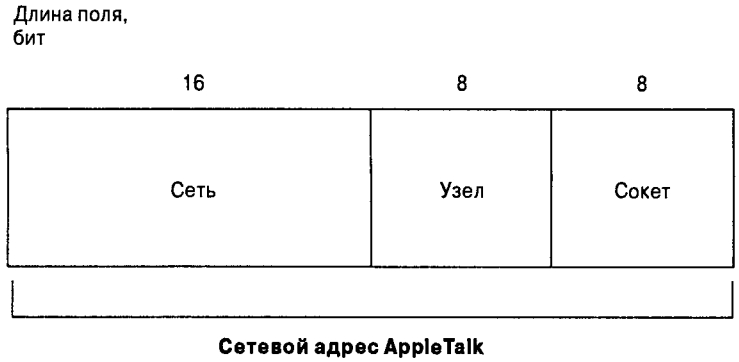


Рис. 38.7. Сетевой адрес AppleTalk

Используя протокол зонной информации (Zone Information Protocol — ZIP), узел связывается с подключенным к сети маршрутизатором. Маршрутизатор в ответ сообщает диапазон сетевого кабеля, к которому подключен узел. Затем узел выбирает правильный сетевой номер из известного кабельного диапазона, полученного от маршрутизатора, и случайный номер узла. Для проверки того, что выбранный адрес не используется другим узлом, рассылается широковещательное сообщение.

Если данный адрес еще не используется (т.е. ни один из узлов не ответил на широковещательное сообщение в течение определенного времени), узлу назначается этот адрес. Если же такой адрес уже используется другим узлом, последний отвечает на широковещательное сообщение, что свидетельствует о том, что адрес занят. Новый узел должен выбрать другой адрес и повторять процедуру до тех пор, пока не будет найден неиспользуемый адрес.

Протокол AARP

Протокол преобразования адреса в сетях AppleTalk (AppleTalk Address Resolution Protocol — AARP) представляет собой протокол сетевого уровня из набора AppleTalk, который соотносит сетевые адреса с адресами устройств. Службы протокола AARP используются другими протоколами AppleTalk. Например, если протоколу сети AppleTalk требуется передать данные, то он определяет сетевой адрес получателя. Задачей протокола AARP является определение адреса устройства, использующего данный сетевой адрес.

Для получения информации об адресе устройства или других узлов сети протокол AARP использует процесс "запрос-ответ". Поскольку AARP является протоколом, зависящим от среды передачи, методы, используемые для запроса узла об адресе устройства, изменяются в зависимости от реализации канального уровня. Как правило, посылается широковещательное сообщение всем узлам AppleTalk в сети.

Таблица соответствия адресов

Каждый узел в сети AppleTalk имеет *таблицу соответствия адресов* (Address Mapping Table — AMT), где адресам устройств соответствуют сетевые адреса. Каждый раз,

когда протокол AARP производит преобразование сетевого адреса в адрес устройства и наоборот, результат записывается в AMT.

Со временем вероятность недействительности записей в AMT возрастает. Поэтому у каждой записи AMT есть свой таймер. При получении AARP-пакета, проверяющего или изменяющего запись, таймер сбрасывается.

По истечении определенного времени по таймеру запись удаляется из AMT. Когда в следующий раз протоколу AppleTalk потребуется связаться с данным узлом, для получения адреса устройства потребуется передача нового AARP-запроса.

Сбор адресов

В некоторых реализациях происходит просмотр входящих DDP-пакетов для обнаружения сетевого адреса и адреса устройства того узла, откуда было отправлено данное сообщение, после чего DDP может поместить полученную информацию в AMT. Это один из способов, которым такие устройства, как маршрутизаторы, рабочие станции и серверы, могут обнаружить устройства, подключенные к сети AppleTalk.

Указанный процесс получения соответствий адресов путем просмотра входящих пакетов называют *сбором адресов* (Address Gleaning). Сбор адресов применяется не очень часто, но иногда он позволяет уменьшить количество передаваемых AARP-запросов.

Функционирование AARP

Протокол преобразования адреса в сетях AppleTalk (AppleTalk Address Resolution Protocol — AARP) устанавливает соответствие между аппаратными и сетевыми адресами устройств. Если у протокола AppleTalk имеются данные для передачи, то он передает протоколу AARP сетевой адрес узла-получателя. Задачей AARP является предоставление адреса устройства, ассоциированного с данным сетевым адресом.

Соответствие сетевого адреса адресу устройства AARP определяет по таблице AMT. Если такое соответствие уже установлено, то адрес устройства передается по запросу протоколу сети AppleTalk, который использует его для соединения с получателем. Если соответствие адресов еще не установлено, то AARP передает широковещательное сообщение с запросом, по которому узел с данным сетевым адресом должен сообщить свой адрес устройства.

Когда узел с данным сетевым адресом получает запрос, он передает обратно свой адрес устройства. Если узла с таким сетевым адресом не существует, ответ не посылается. После определенного количества попыток AARP рассматривает данный адрес как неиспользуемый и возвращает в ответ на запрос протокола AppleTalk сообщение об ошибке. Если ответ получен, адрес устройства и соответствующий ему сетевой адрес заносятся в AMT. Затем адрес устройства передается по запросу протоколу AppleTalk, который использует его для соединения с узлом-получателем.

Основные сведения о протоколе DDP

Протокол доставки дейтаграмм (Datagram Delivery Protocol — DDP) представляет собой главный протокол маршрутизации сетевого уровня в стеке протоколов AppleTalk, который обеспечивает передачу дейтаграмм между сокетами AppleTalk методом

негарантированной доставки, без подтверждения соединения. Как и в случае других протоколов, таких как TCP, между двумя устройствами не устанавливается виртуального канала или соединения. Доставку гарантируют протоколы верхних уровней набора AppleTalk, описанные далее в настоящей главе.

Протокол DDP выполняет следующие две основные функции.

- **Передача пакетов.** DDP получает данные от сокетов-клиентов, создает DDP-заголовок, используя соответствующий адрес получателя, и передает пакет протоколу канального уровня.
- **Получение пакетов.** DDP получает фреймы с канального уровня, извлекает из DDP-заголовка адрес получателя и передает пакет сокету-получателю.

Протокол DDP поддерживает кабельный диапазон локальной сети и сетевой адрес маршрутизатора, подключенного к локальной сети в каждом узле AppleTalk. Кроме этой информации, маршрутизаторы AppleTalk должны поддерживать таблицу маршрутизации, используя протокол поддержки таблицы маршрутизации (Routing Table Maintenance Protocol — RTMP).

Процесс передачи данных по протоколу DDP

Функционирование протокола DDP во многом аналогично функционированию других протоколов маршрутизации. Источник присваивает пакетам адрес, затем они передаются на канальный уровень и пересылаются в пункт назначения. При получении данных от протокола верхнего уровня протокол DDP путем проверки номера сети в адресе получателя определяет принадлежат ли источник и узел-получатель к одной и той же сети.

Если номер сети получателя принадлежит кабельному диапазону локальной сети, пакет инкапсулируется в заголовок DDP и передается на канальный уровень для передачи узлу-получателю, в противном случае пакет инкапсулируется в заголовок DDP и передается на канальный уровень для передачи маршрутизатору. Промежуточные маршрутизаторы, используя таблицы маршрутизации, направляют пакет в сеть-получатель. Когда пакет достигнет маршрутизатора, принадлежащего сети-получателю, он передается узлу-получателю.

Транспортный уровень AppleTalk

На транспортном уровне в сетях AppleTalk выполняется надежная, прозрачная для верхних уровней передача данных по объединенной сети. В задачи транспортного уровня обычно входит управление потоками, мультиплексирование, управление виртуальными каналами, а также проверка и исправление ошибок.

Существует пять основных протоколов AppleTalk транспортного уровня:

- протокол поддержки таблиц маршрутизации (Routing Table Maintenance Protocol — RTMP);
- протокол связывания имен (Name Binding Protocol — NBP);
- протокол маршрутизации в сетях AppleTalk с обновлением (AppleTalk Update-Based Routing Protocol — AURP);
- протокол транзакций в сетях AppleTalk (AppleTalk Transaction Protocol — ATP);
- протокол отклика в сетях AppleTalk (AppleTalk Echo Protocol — AEP).

Все эти протоколы описываются ниже.

Основные сведения о протоколе RTMP

Протокол поддержки таблиц маршрутизации (Routing Table Maintenance Protocol — RTMP) представляет собой протокол транспортного уровня из набора AppleTalk, который формирует и обновляет таблицы маршрутизации на маршрутизаторах сетей AppleTalk.

В основе RTMP лежит протокол информации о маршрутах (Routing Information Protocol — RIP). Подобно RIP, RTMP использует в качестве метрики маршрута количество пройденных узлов. Эта величина определяется как число маршрутизаторов или других промежуточных узлов, через которые должен пройти пакет от сети-источника до сети-получателя.

Таблицы маршрутизации протокола RTMP

Протокол RTMP отвечает за формирование и обновление таблиц маршрутизации для маршрутизаторов в сетях AppleTalk. Эти таблицы содержат записи для каждой сети, которой может достичь пакет.

Периодически маршрутизаторы обмениваются маршрутной информацией с целью ее обновления и согласованности в пределах всей объединенной сети. В таблице маршрутизации протокола RTMP содержится следующая информация о каждой сети-получателе, известной маршрутизатору:

- сетевой кабельный диапазон сети-получателя;
- расстояние (количество узлов) до сети-получателя;
- порт маршрутизатора, ведущего к сети-получателю;
- адрес маршрутизатора следующего пункта;
- текущее состояние данных таблицы маршрутизации (хорошее, сомнительное или плохое).

На рис. 38.8 показана типичная таблица маршрутизации протокола RTMP.

Основные сведения о протоколе NBP

Протокол связывания имен (Name Binding Protocol — NBP) представляет собой протокол транспортного уровня в наборе AppleTalk, который устанавливает соответствие между адресами, используемыми на нижних уровнях, и именами в сети AppleTalk. Сокеты-клиенты в пределах узлов сети AppleTalk называются также видимыми элементами сети или NVE-элементами (Network-Visible Entities — NVE). NVE-элементы представляют собой ресурсы, к которым можно обратиться по сети, такие, например, как служба печати, доступная через объединенную сеть. Обращение к NVE-элементу происходит по его имени, которое представляет собой строку символов. NVE-элементы также имеют зону и другие атрибуты, известные как ассоциированные типы элементов.

Существует две основных причины для использования на верхних уровнях имен записей вместо адресов. Во-первых, сетевые адреса назначаются узлам динамически и, следовательно, постоянно изменяются. Имена записей обеспечивают для пользователей единообразный способ обращения к сетевым ресурсам и службам, например, к файловому серверу. Во-вторых, использование имен вместо адресов для обращения к ресурсам и службам сохраняет для пользователей прозрачность операций нижних уровней.

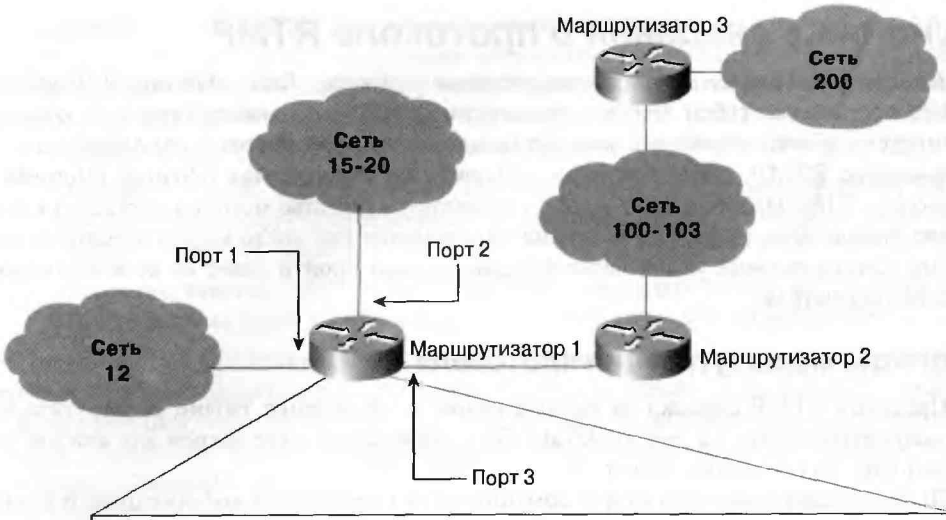


Таблица маршрутизации RTMP

Кабельный диапазон сети	Расстояние	Порт	Следующий узел	Запись Состояние
12	0	1	0	Норма
15-20	0	2	0	Норма
100-103	1	3	Маршрутизатор 2	Норма
200	2	3	Маршрутизатор 2	Норма

Рис. 38.8. В таблице маршрутизации RTMP содержится информация обо всех сетях-получателях, известных маршрутизатору

Связывание имен

Под *связыванием имен* понимается установка соответствия между именами NVE-элементов и их сетевыми адресами. Каждый узел в сети AppleTalk устанавливает соответствие между именами своих NVE-элементов и сетевыми адресами в таблице имен. Набор всех таблиц имен во всех узлах объединенной сети называется каталогом имен, который представляет собой распределенную базу данных, содержащую все соответствия имен и адресов. Связывание имен может иметь место при создании узла или происходить динамически, непосредственно перед получением доступа к элементу с данным именем.

Протокол NBP выполняет следующие четыре функции: поиск, распознавание, подтверждение и удаление имен. Результатом поиска по имени является сетевой адрес элемента NVE, который выясняется перед получением доступа к службам данного NVE. Для установления соответствия имен и адресов протокол NBP проверяет каталог имен. Регистрация имен позволяет узлу создать свою таблицу имен. NBP подтверждает,

что имя не используется, а затем добавляет в таблицу запись о соответствии имени и адреса. Подтверждение имени используется для проверки правильности соответствия имени и адреса, полученного при поиске по имени. Удаление имени применяется для удаления данных из таблицы имен в случае, например, отключения узла.

Протокол AURP

Протокол маршрутизации в сетях AppleTalk с обновлением (AppleTalk Update-Based Routing Protocol — AURP) представляет собой протокол транспортного уровня из набора AppleTalk, который позволяет объединить две и более объединенные сети AppleTalk с помощью сети TCP/IP, в результате чего образуется распределенная сеть AppleTalk. Протокол AURP инкапсулирует пакеты в заголовки протокола UDP, что обеспечивает их сквозную передачу по сети TCP/IP. AURP состоит из двух компонентов: внешних маршрутизаторов и туннелей AURP.

Внешние маршрутизаторы соединяют локальную объединенную сеть AppleTalk с туннелями AURP. Внешние маршрутизаторы преобразуют данные AppleTalk и маршрутную информацию в форму протокола AURP, а также выполняют инкапсуляцию и декапсуляцию потока данных AppleTalk. Внешние маршрутизаторы функционируют как маршрутизаторы сети AppleTalk в локальной сети и как конечные узлы в сети TCP/IP. При первом подключении внешнего маршрутизатора к туннелю AURP происходит обмен маршрутной информацией с другими внешними маршрутизаторами. С этого момента внешний маршрутизатор посылает маршрутную информацию только в следующих случаях:

- при добавлении или удалении сети из таблицы маршрутизации;
- при изменении расстояния до сети;
- если из-за изменения маршрута к сети внешний маршрутизатор должен получать доступ к этой сети через локальную объединенную сеть, а не через туннель, или наоборот.

Туннель AURP функционирует как отдельный виртуальный канал между удаленными объединенными сетями AppleTalk. На пути между внешними маршрутизаторами может находиться произвольное количество физических узлов, однако они являются прозрачными для сетей AppleTalk. Существует два вида туннелей AURP: туннели типа "точка-точка" и многоточечные. Туннели "точка-точка" AURP соединяют между собой два внешних маршрутизатора. Многоточечные туннели AURP осуществляют соединение между тремя и более внешними маршрутизаторами и, в свою очередь, делятся на два вида: полностью и частично подключенные. Полностью подключенный многоточечный туннель позволяет всем подключенным к нему внешним маршрутизаторам рассылать пакеты друг другу. Если многоточечный туннель является частично подключенным, то один или несколько внешних маршрутизаторов имеют информацию только о некоторых из оставшихся внешних маршрутизаторов. На рис. 38.9 показаны две LAN в сети AppleTalk, соединенных туннелем AURP типа "точка-точка".

Инкапсуляция протокола AURP

При обмене маршрутной информацией или данными через туннель AURP необходимо преобразовать пакеты AppleTalk из RTMP, ZIP и (в реализации Cisco) Enhanced IGRP в AURP. Затем пакеты инкапсулируются в заголовки протокола UDP для передачи

по сети TCP/IP. Преобразование и инкапсуляция выполняются внешними маршрутизаторами, получающими маршрутную информацию AppleTalk или пакеты данных для пересылки в удаленную объединенную сеть AppleTalk. Внешний маршрутизатор преобразует пакеты в формат AURP, инкапсулирует их в заголовки UDP и передает по туннелю (т.е. по сети TCP/IP).

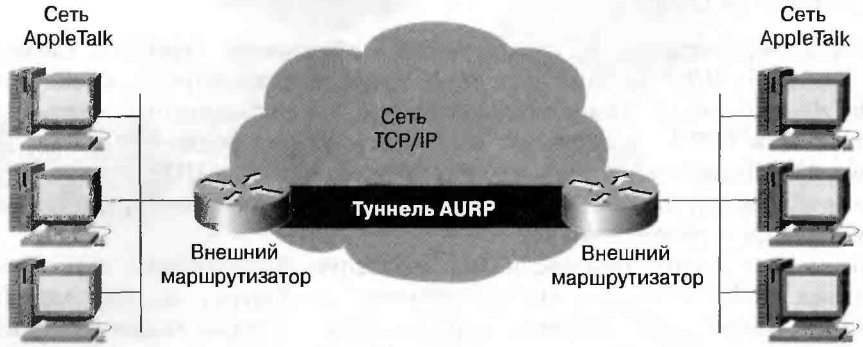


Рис. 38.9. Туннель AURP ведет себя как виртуальный канал между удаленными сетями

Сеть TCP/IP рассматривает пакеты как обычный поток данных UDP. Удаленный внешний маршрутизатор принимает пакеты UDP и удаляет из них заголовок UDP. Затем происходит преобразование пакетов AURP в исходный формат — в маршрутную информацию, или в пакет данных. Если пакеты AppleTalk содержат маршрутную информацию, то принимающий внешний маршрутизатор соответствующим образом обновляет свою таблицу маршрутизации. Если пакеты содержат данные для передачи узлу AppleTalk в локальной сети, то эти данные отсылаются в соответствующей форме.

Протокол ATP

Протокол транзакций в сетях AppleTalk (AppleTalk Transaction Protocol — ATP) представляет собой протокол транспортного уровня из набора AppleTalk, управляющий транзакциями между двумя сокетами сети AppleTalk. Транзакция состоит из запроса транзакции и ответа на него. Обмен этими сообщениями происходит между сокетами-клиентами.

Запрашивающий сокет-клиент посылает запрос транзакции с просьбой о выполнении каких-либо действий клиентом-получателем. Получив запрос, последний выполняет требуемые действия и возвращает соответствующую информацию в ответе транзакции. При передаче транзакционных запросов и ответов протокол ATP выполняет наиболее важные функции транспортного уровня, включая подтверждение и повторную передачу, упорядочение пакетов, сегментацию и повторную сборку пакетов.

Совместно с ATP работают несколько протоколов сеансового уровня, в том числе протоколы ASP и PAP. Подробнее эти два протокола верхнего уровня AppleTalk будут описаны ниже.

Устройства, посылающие ответ, реагируют на запрос по-разному, в зависимости от того, какой из двух типов служб транзакции используется: транзакции ALO (At-Least-Once, "хотя бы один раз") или XO (eXactly-Once, "ровно один раз"). Транзакции ALO используются, когда повторный запрос транзакции должен привести к тому же результату, что и первоначальный. Если ответ транзакции потерян,

источник повторяет запрос. Это не наносит ощутимого вреда протокольным операциям, поскольку повторение запроса не отличается от исходного. Транзакции XO используются в том случае, когда повторение запроса транзакции может коренным образом повлиять на протокольные операции. Принимающее устройство хранит список всех недавно полученных транзакций, поэтому повторные запросы выполняются лишь один раз.

Протокол AEP

Протокол отклика в сетях AppleTalk (AppleTalk Echo Protocol — AEP) представляет собой протокол транспортного уровня стека AppleTalk, который генерирует пакеты, проверяющие возможность достижения узлов сети. Протокол AEP может быть включен в любой узел сети AppleTalk и имеет статически присвоенный номер сокета 4 (сокет Echoer).

Для проверки доступности узла пакет запроса AEP передается протоколу DDP источника. DDP соответствующим образом адресует пакет, указывая в поле типа, что это запрос AEP. При получении пакета получателем протокол DDP просматривает поле типа и узнает оттуда, что это запрос протокола AEP. Пакет копируется, преобразуется в ответ AEP (путем изменением поля в пакете AEP) и возвращается пославшему его узлу.

Протоколы верхнего уровня в сетях AppleTalk

AppleTalk подерживает службы на сеансового уровня, уровней представления и приложений эталонной модели OSI. В стек протоколов AppleTalk входят четыре основных протокола сеансового уровня. (На сеансовом уровне устанавливаются, управляются и прерываются сеансы связи между элементами уровня представлений).

Сеанс обмена данными состоит из запросов и ответов службы, пересылаемых между приложениями, работающими на различных сетевых устройствах. Эти запросы и ответы координируются протоколами сеансового уровня.

В число протоколов сеансового уровня AppleTalk входят протоколы ADSP, ZIP, ASP и PAP.

Файловый протокол AppleTalk (AppleTalk Filing Protocol — AFP) стека AppleTalk реализован на уровнях представления и приложений. Уровень представлений обеспечивает главным образом разнообразные функции кодирования и преобразования, которые применяются к данным уровня приложений. Уровень приложений взаимодействует с прикладными программами (находящимися вне рамок модели OSI), имеющими коммуникационные компоненты. В задачи уровня приложений, как правило, входит идентификация партнеров по обмену данными, определение доступности ресурсов и синхронизация связи. На рис. 38.10 показано соответствие между верхними уровнями набора протоколов AppleTalk и уровнями модели OSI.

Протокол ADSP

Протокол потока данных в сетях AppleTalk (AppleTalk Data Stream Protocol — ADSP) представляет собой протокол сеансового уровня стека AppleTalk, который устанавливает и поддерживает двусторонний обмен данными между двумя сокетами AppleTalk. Протокол ADSP обеспечивает упорядочение данных и отсутствие дуб-

лированных пакетов. ADSP также использует механизм управления потоками, позволяющий пункту-получателю замедлять передачу данных от источника путем предоставления сведений об уменьшении размера окна приема. Протокол ADSP работает совместно с протоколом DDP.

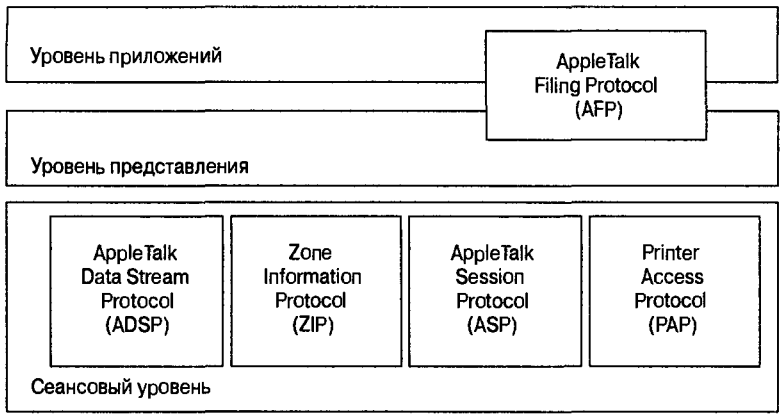


Рис. 38.10. Протоколы верхних уровней AppleTalk соответствуют трем уровням модели OSI

Протокол ZIP

Протокол информации о зоне (Zone Information Protocol — ZIP) представляет собой протокол сеансового уровня стека AppleTalk, который поддерживает соответствие между номером сети и именем зоны в маршрутизаторах сетей AppleTalk. Протокол ZIP используется преимущественно маршрутизаторами AppleTalk. Однако и другие вновь созданные узлы сети используют службы протокола ZIP для выбора зоны. В каждом маршрутизаторе ZIP ведет таблицу информации о зоне (zone information table — ZIT). Таблицы ZIT представляют собой списки, где каждому номеру сети соответствует одно или несколько имен зон. Каждая таблица ZIT содержит карту соответствий между номерами сетей и именами зон для каждой сети в объединенной сети. Пример простейшей ZIT представлен на рис. 38.11.

Протокол ASP

Сеансовый протокол сети AppleTalk (AppleTalk Session Protocol — ASP) представляет собой протокол сеансового уровня стека AppleTalk, который устанавливает и поддерживает сеансы обмена данными между клиентами и серверами сетей AppleTalk. ASP позволяет клиенту установить сеанс обмена данными с сервером и посылать команды на этот сервер, причем допускает одновременно несколько сеансов клиентов с одним сервером. Протокол ASP использует ряд служб, предоставляемых протоколами нижних уровней, такими как ATP и NBP.

Основные сведения о протоколе PAP

Протокол доступа к принтеру (Printer Access Protocol — PAP) представляет собой протокол сеансового уровня стека AppleTalk, который позволяет клиентским рабочим

станциям устанавливать соединение с серверами, в частности, с принтерами. Сеанс связи между клиентской рабочей станцией и сервером начинается с того, что рабочая станция направляет на сервер запрос такого сеанса. Протокол PAP получает сетевой адрес запрашиваемого сервера при помощи протокола NBP, а затем устанавливает соединение между клиентом и сервером. Обмен данными между клиентом и сервером происходит с использованием протокола ATP. При отсутствии дальнейшей необходимости в соединении PAP разрывает его. Серверы, использующие PAP, могут поддерживать сразу несколько соединений с клиентами. Это позволяет принтеру, например, одновременно выполнять задания, поступающие от нескольких рабочих станций.

Номер сети	Зоны
10	Отдел маркетинга
20-25	Отдел документации и обучения
50	Финансовый отдел
100-120	Технический отдел
100-120	Администрация

Рис. 38.11. Таблицы информации о зоне помогают идентифицировать зону

Протокол AFP

Файловый протокол AppleTalk (AppleTalk Filing Protocol — AFP) обеспечивает совместный доступ рабочих станций к файлам в сети AppleTalk. Протокол AFP выполняет функции на уровнях представлений и приложений AppleTalk. Этот протокол обеспечивает прозрачность сети, позволяя пользователям обращаться с удаленными файлами так же, как если бы эти файлы хранились на компьютере пользователя. Протокол AFP использует службы, предоставляемые протоколами ASP, ATP и AEP.

Стек протоколов AppleTalk

Полный набор (стек) протоколов AppleTalk и его соответствие эталонной модели OSI показан на рис. 38.12.

Формат DDP-пакетов

Существует два типа DDP-пакетов:

- **Короткие пакеты протокола DDP.** Используются для передачи данных между двумя узлами одного и того же сегмента сети (только в нерасширенных сетях). В современных сетях этот формат встречается редко.
- **Расширенные пакеты протокола DDP.** Используются для передачи данных между узлами с различными номерами сетей (в нерасширенной сети) и всегда — в расширенной сети.

Формат расширенного DDP-пакета показан на рис. 38.13.
Ниже описаны поля расширенного DDP-пакета, показанные на рис. 38.13.

- **Счетчик узлов.** В этом поле содержится количество промежуточных устройств, через которые прошел пакет. В источнике этому полю присваивается значение 0. В каждом промежуточном узле, через который передается пакет, это значение увеличивается на 1. Максимально допустимое количество узлов равно 15.
- **Длина.** Полная длина DDP-пакета в байтах.
- **Контрольная сумма.** Контрольная сумма для обнаружения ошибок. Если контрольная сумма не вычисляется, то все биты в этом поле равны 0.
- **Сеть-получатель.** 16-разрядный номер сети-получателя.
- **Сеть-источник.** 16-разрядный номер сети-источника.
- **ID узла-получателя.** 8-разрядный идентификатор узла-получателя.
- **ID узла-источника.** 8-разрядный идентификатор узла источника.
- **Сокет-получатель.** 8-разрядный номер сокета-получателя.
- **Сокет-источник.** 8-разрядный номер сокета источника.
- **Тип.** Протокол верхнего уровня, к которому относится информация, расположенная в поле данных.
- **Данные.** Данные, получаемые от протокола верхнего уровня.

Резюме

В настоящей главе приведены основные сведения о стеке протоколов AppleTalk. Протоколы AppleTalk используют зоны для объединения узлов или сетей в логические группы. В сетях AppleTalk адреса канального уровня присваиваются динамически.

В AppleTalk применяется метод преобразования адресов, аналогичный использованию протокола ARP в стеке протоколов TCP/IP. В AppleTalk этот метод называется протоколом AARP. Для получения информации об адресе устройства AARP использует широковещательные передачи.

Главным протоколом маршрутизации сетевого уровня в сетях AppleTalk является протокол доставки дейтаграмм (Datagram Delivery Protocol — DDP). Этот протокол обеспечивает передачу дейтаграмм методом негарантированной доставки без подтверждения соединения.

Существует пять основных реализаций транспортного уровня AppleTalk: RTMP, NBP, AURP, ATP и AEP.

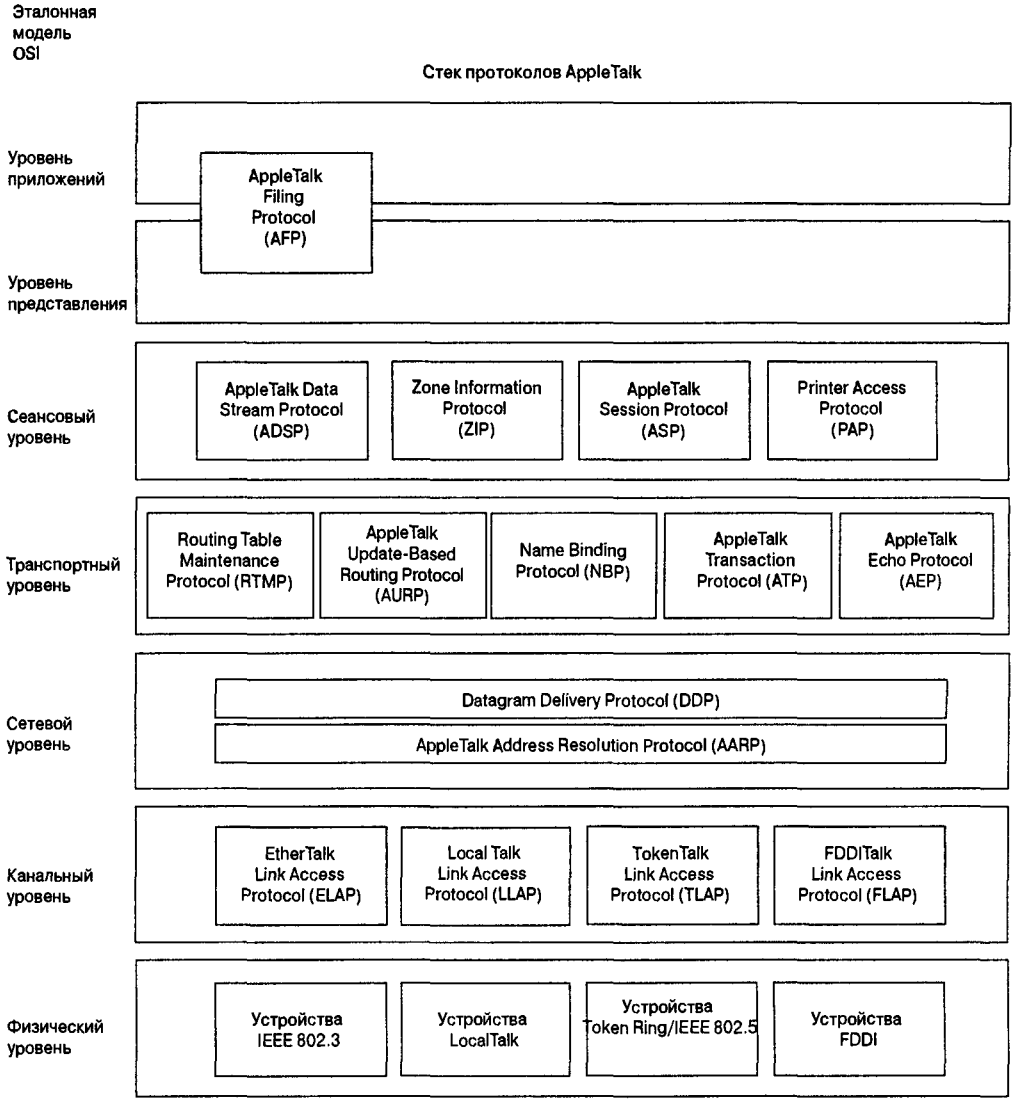


Рис. 38.12. Набор протоколов AppleTalk полностью соответствует эталонной модели OSI

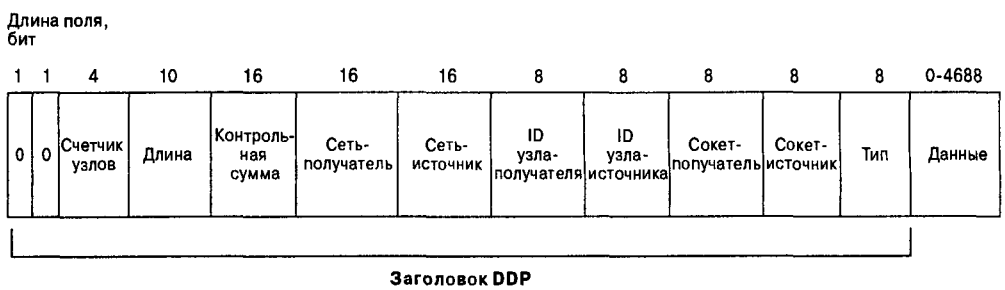


Рис. 38.13. Расширенный DDP-пакет

Контрольные вопросы

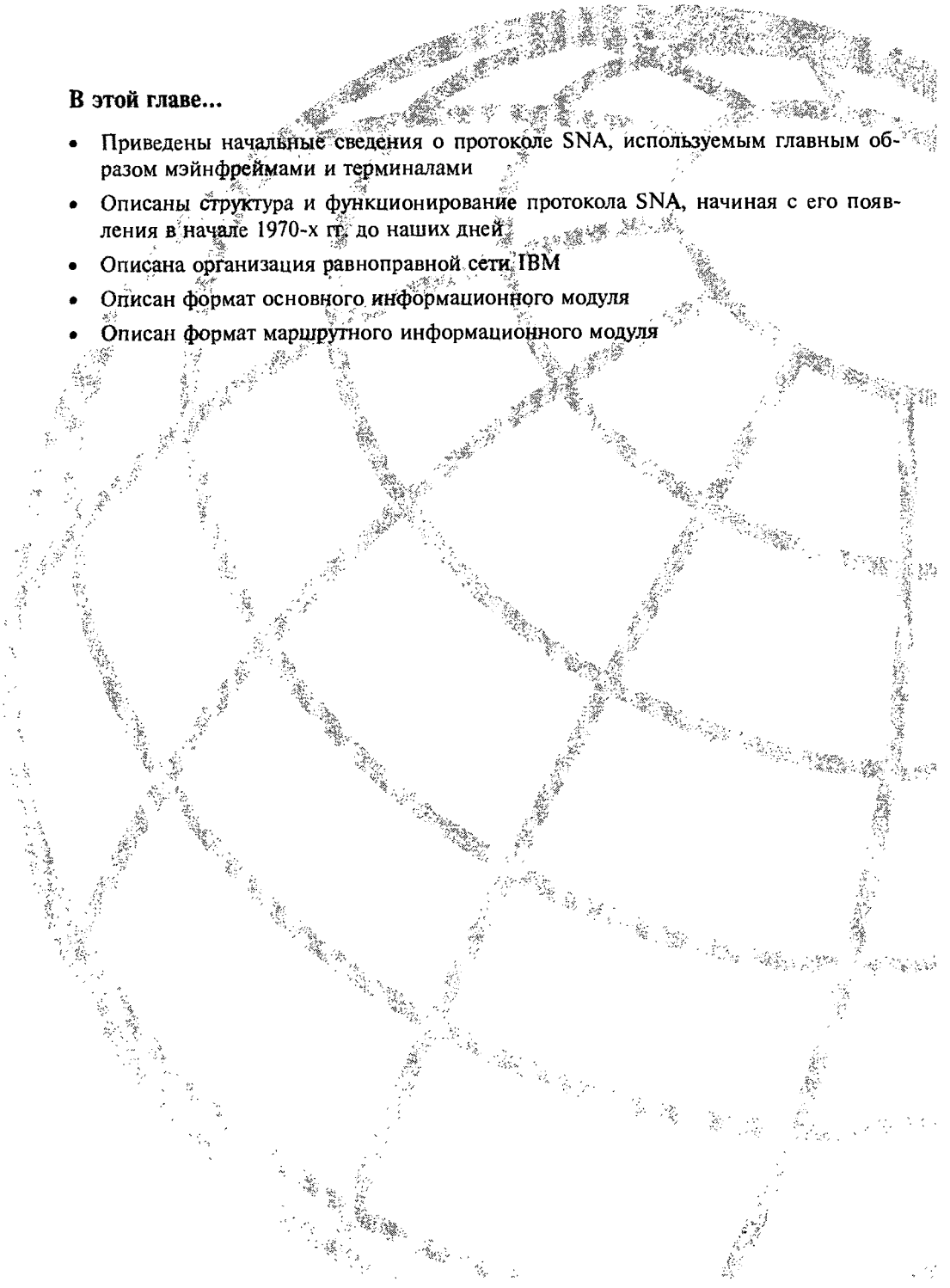
1. Что такое зона AppleTalk?
2. Назовите четыре основных средства реализации доступа к среде передачи для протоколов AppleTalk.
3. Как рабочим станциям назначаются адреса узлов?
4. Какой протокол маршрутизации сетевого уровня, используемый в сетях AppleTalk, является основным?
5. Назовите пять важнейших протоколов транспортного уровня в сетях AppleTalk.

Дополнительные источники

- http://www.apple.com
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/applet.htm

В этой главе...

- Приведены начальные сведения о протоколе SNA, используемым главным образом мэйнфреймами и терминалами
- Описаны структура и функционирование протокола SNA, начиная с его появления в начале 1970-х гг. до наших дней
- Описана организация равноправной сети IBM
- Описан формат основного информационного модуля
- Описан формат маршрутного информационного модуля



Глава 39

Протоколы сетевой архитектуры IBM

Введение

По существу, современные сети IBM состоят из двух отдельных архитектур, имеющих более или менее общую основу. До появления современных сетей сетевой ландшафт безраздельно принадлежал системной сетевой архитектуре (Systems Network Architecture — SNA) IBM, поэтому ее часто называют традиционной или унаследованной системной сетевой архитектурой.

С увеличением количества персональных компьютеров, рабочих станций и клиент-серверных вычислений IBM, отвечая на потребность в равноправной сетевой стратегии, разработала структуры улучшенного протокола одноранговых сетей (Advanced Peer-to-Peer Networking — APPN) и протокола улучшенных межпрограммных вычислений (Advanced Program-to-Program Computing — APPC).

Несмотря на то, что в сети APPN были перенесены многие старые технологии, связанные с мэйнфреймовой архитектурой SNA, между ними есть существенные отличия. В настоящей главе описываются все ветви сетевой среды IBM, начиная со старых систем SNA и заканчивая структурой APPN. В конце главы будут рассмотрены базовый и маршрутный информационные модули IBM.

Стратегии маршрутизации IBM описываются в отдельной главе. Подробнее протоколы маршрутизации рассматриваются в главе 43.

Традиционные среды SNA

Архитектура SNA была разработана в 70-х гг. XX века в виде всеобъемлющей структуры, соответствующей эталонной модели OSI. Роль концентратора в сети SNA играет мэйнфрейм, работающий под управлением ACF/VTAM (Advanced Communication Facility/Virtual Telecommunication Access Method). ACF/VTAM устанавливает сеансы связи, активирует и дезактивирует ресурсы. Ресурсы в этой среде явно определяются заранее, что исключает потребность в широковещательной рассылке служебных сообщений и сводит к минимуму размеры заголовков. Базовая архитектура и главные компоненты традиционной сети SNA описаны ниже.

Системная сетевая архитектура IBM

Компоненты модели IBM SNA близки к эталонной модели OSI. Ниже описывается роль каждого компонента SNA в соединении объектов системной сетевой архитектуры.

- **DLC Управление каналом (Data Link Control — DLC).** Несколько протоколов, среди которых протокол синхронного управления каналом (Synchronous Data Link Control — SDLC) и протокол обмена данными между равноправными узлами локальной сети Token Ring.
- **Управление маршрутом.** Множество функций сетевого уровня OSI, в том числе маршрутизация, сегментация и сборка дейтаграмм (SAR).
- **Управление передачей.** Надежное сквозное соединение с кодированием и декодированием данных.
- **Управление потоком.** Управление обработкой запросов и ответов, определение очередности обмена данными, группировка сообщений и прерывание потока данных по требованию.
- **Службы представления.** Определяют алгоритмы преобразования данных из одного формата в другой, координируют совместное использование ресурсов и синхронизируют транзакции.
- **Службы транзакций.** Службы приложений в виде программ, реализующих распределенную обработку и управление.

SNA не предусматривает специальных протоколов для управления физическим уровнем. Эта задача возлагается на другие стандарты.

Рис. 39.1. IBM SNA соответствует всем уровням модели OSI

Центральной конструкцией в сети SNA является сеть управления маршрутом, которая отвечает за перемещение информации между узлами SNA и организует обмен данными между узлами объединенной сети. Сеть управления маршрутом использует функции управления маршрутом и управления каналом (DLC). Сеть управления маршрутом является подсетью транспортной сети IBM.

Физические элементы IBM SNA

Традиционные физические элементы SNA принадлежат к одному из следующих четырех типов: узлы, коммуникационные контроллеры, контроллеры установки и терминалы.

Узлы SNA контролируют всю сеть или ее часть. На них выполняются вычисления, работают программы и службы каталогов, предоставляется доступ к базам данных и осуществляется управление сетью. (Примером узла в традиционной SNA может служить мэйнфрейм S/370.)

Коммуникационные контроллеры управляют физической сетью и каналами обмена данными. В частности, коммуникационные контроллеры, также называемые коммуникационными процессорами (Front-End Processors — FEP) выполняют основные задачи по маршрутизации данных в традиционной сети SNA. (Примером коммуникационного контроллера может служить 3745.)

Контроллеры установки часто называют кластерными контроллерами. Эти устройства управляют операциями ввода и вывода подключенных к ним устройств, таких как терминалы. (Примером контроллера установки может служить 3174.)

Терминалы, также называемые рабочими станциями, служат интерфейсом между пользователями и сетью. (Типичный пример терминала — 3270.) На рис. 39.2 показана обобщенная схема SNA со всеми описанными выше физическими элементами.

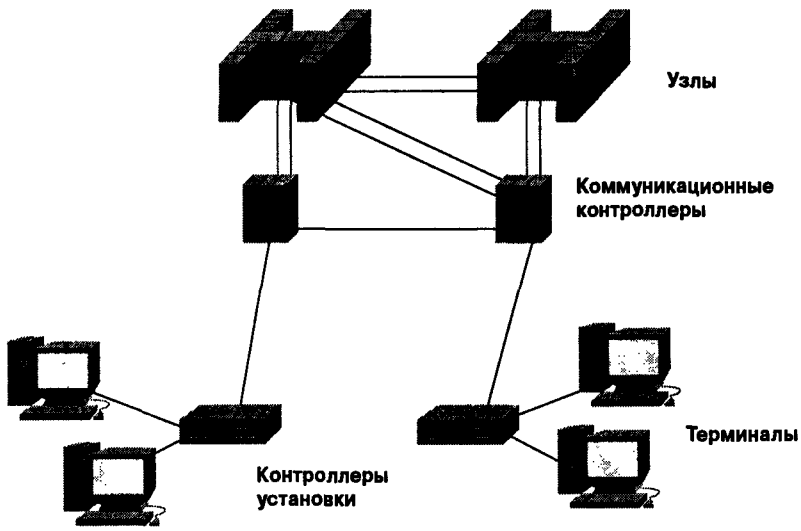


Рис. 39.2. Физические элементы SNA

Управление каналом в архитектуре IBM SNA

Уровень *управления каналом* (Data Link Control — DLC) SNA поддерживает несколько сред передачи, каждая из которых обеспечивает доступ к устройствам и пользователям с различными требованиями. В число сред передачи SNA входят мэйнфреймовые каналы, SDLC, X.25, Token Ring и др.

Стандартное подключение к мэйнфреймовому каналу представляет собой канал параллельной передачи данных с прямым доступом к памяти (Direct Memory Access — DMA). Мэйнфреймовые каналы соединяют многопроводными кабелями узлы IBM

между собой и с коммуникационными контроллерами. Длина каждого кабеля может составлять несколько сотен футов. Стандартный мэйнфреймовый канал может передавать данные со скоростью 3-4,5 Мбит/с.

Мэйнфреймовая среда IBM Enterprise Systems CONnection (ESCON) позволяет повысить пропускную способность канала и передавать данные на большие расстояния. Обычно ESCON передает данные со скоростью 18 Мбит/с и поддерживает соединение типа "точка-точка" в диапазоне нескольких километров. Для больших скоростей передачи данных и расстояний ESCON использует оптоволоконный кабель.

Протокол SDLC широко применяется в сетях SNA коммуникационными контроллерами и контроллерами установки, а также для передачи данных по телекоммуникационным каналам.

Сети X.25 долгое время использовались для передачи данных по WAN. Обычно сеть X.25 помещалась между двумя узлами SNA и рассматривалась как один канал. В SNA X.25 реализован как протокол доступа, а узлы SNA, соединенные сетью X.25, считаются смежными. Чтобы соединить узлы SNA по глобальной сети, основанной на X.25, необходим протокол DLC, так как он обладает некоторыми возможностями, которые X.25 не обеспечивает. Для восполнения этих пробелов применяются несколько специализированных протоколов DLC, такие как заголовок физических служб, ограниченный протокол управления логическим каналом (Qualified Logical Link Control — QLLC) и усовершенствованный протокол управления логическим каналом передачи (Enhanced Logical Link Control — ELLC).

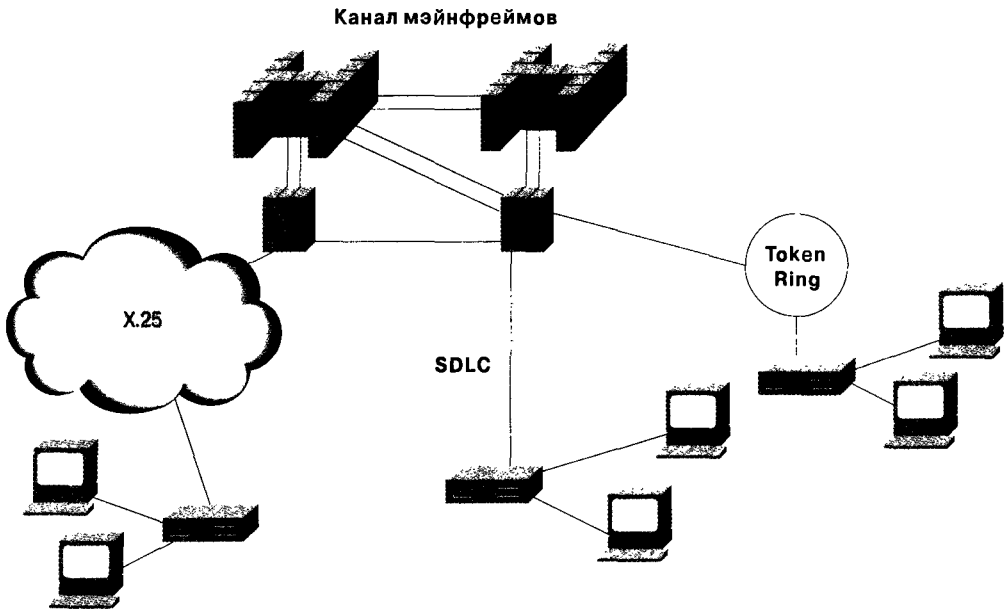


Рис. 39.3. SNA поддерживает различные среды передачи

Основным средством доступа SNA DLC к устройствам локальной сети является технология Token Ring. Token Ring, поддерживаемая IBM, в сущности, играет ту же роль, что и протокол доступа к каналу IEEE 802.5 под управлением IEEE 802.2 Logical Link Control Type 2 (LLC2).

Кроме основного набора сред передачи, IBM поддерживает несколько других широко распространенных сред, среди которых IEEE 802.3/Ethernet, FDDI и Frame Relay.

На рис. 39.3 показаны различные среды передачи, объединенные архитектурой SNA.

Адресуемые сетевые модули IBM

В SNA определены три основных адресуемых сетевых модуля (Network Addressable Units — NAU): логические модули, физические модули и контрольные точки. Каждый из них играет важную роль при установке соединений между системами в сети SNA.

Логические модули (Logical Units — LU) служат портами доступа пользователей к сети SNA. Логические элементы предоставляют пользователям доступ к сетевым ресурсам и управляют передачей информации между пользователями.

Физические модули (Physical Units — PU) используются для наблюдения и управления подключенными к ним сетевыми каналами и другими сетевыми ресурсами данного узла. PU реализуются на узлах в виде методов доступа SNA, таких как виртуальный телекоммуникационный метод доступа (Virtual Telecommunication Access Method — VTAM). Кроме того, физические модули реализуются на коммуникационных контроллерах при помощи программ управления сетью (Network Control Programs — NCP).

Контрольные точки (Control Points — CP) управляют узлами SNA и их ресурсами. Основное их отличие от физических модулей заключается в том, что контрольные точки CP определяют, какое действие должно быть выполнено, а физические модули PU дают компьютеру выполнить это действие. В качестве примера точек CP можно привести точки управления системными службами SNA (System Services Control Point — SSCP). Роль точки SSCP может играть контрольная точка, расположенная в узле PU 5; SSCP может также реализовываться совместно с методом доступа SNA, таким как VTAM.

Узлы IBM SNA

Традиционные узлы SNA делятся на две категории: подзональные и периферийные. Подзональные узлы SNA предоставляют все сетевые службы, в том числе промежуточную межузловую маршрутизацию и преобразование локальных и общесетевых адресов. Тип узлов SNA никак не связан с действительными физическими устройствами. Особый интерес представляют два подзональных узла: узел типа 4 и узел типа 5.

Узел типа 4 (T4) обычно принадлежит коммуникационному котроллеру, такому как 3745. Примером T4 может служить NCP, выполняющая маршрутизацию данных и управление потоком между коммуникационным процессором и другими сетевыми ресурсами.

Узел типа 5 (T5) обычно принадлежит узлу, такому как мэйнфрейм S/370. Примером T5 может служить VTAM, принадлежащий мэйнфрейму IBM. VTAM управляет логическим потоком данных в сети, служит интерфейсом между подсистемами приложений и сетью и защищает подсистемы приложений от несанкционированного доступа.

Периферийные узлы SNA используют только локальную адресацию и обмениваются данными с другими узлами через подзональные узлы. Среди периферийных узлов особый интерес представляет узел типа 2 (T2), хотя в SNA описан и периферийный узел типа 1. T2 обычно располагается в интеллектуальных терминалах (таких, как 3270) или контроллерах установки (типа 3174). Узел типа 1 (T1) в настоящее время устарел, но там, где еще используется, он располагается на неинтеллектуальных терминалах. На рис. 39.4 показаны различные типы узлов и их взаимосвязь.

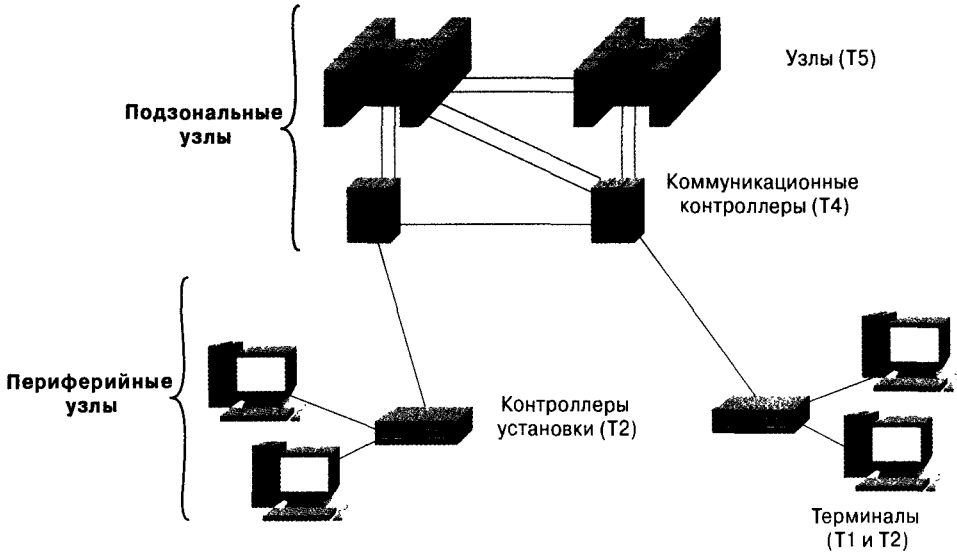


Рис. 39.4. Связь периферийных узлов с другими узлами через подзональные узлы

Равноправная сеть IBM

Изменения требований к организации сетей и обмену данными привели к тому, что IBM усовершенствовала и частично пересмотрела многие основные характеристики SNA. Потребность в равноправных сетевых объектах (таких как маршрутизаторы) привела к ряду серьезных изменений в системной сетевой архитектуре. Объединенная сеть с узлами SNA основана на нескольких сетевых компонентах IBM.

Улучшенный протокол равноправных сетей (Advanced Peer-to-Peer Networking — APPN) представляет собой IBM SNA второго поколения. Протокол APPN стал результатом перехода IBM SNA от иерархической среды, основанной на мэйнфреймах, к сети с равноправными узлами. Основой протокола APPN является архитектура IBM, поддерживающая обмен данными между равноправными узлами, службы каталогов и маршрутизацию между двумя и более системами APPN, не связанными непосредственно друг с другом.

Компоненты APPN

Кроме среды APPN, равноправная архитектура SNA определяет три дополнительные ключевые концепции: логические модули (LU), расширенные межпрограммные вычисления (Advanced Program-to-Program Computing — APPC), и узел типа 2.1. Каждая из них играет важную роль в установке соединений между узлами SNA в контексте равноправной объединенной сети SNA.

Логический модуль LU 6.2 управляет равноправным обменом данными в среде SNA. Кроме того, LU 6.2 поддерживает основной обмен данными между программами в среде распределенной обработки, а также между однотипными и разнотипными узлами. APPC позволяет приложениям SNA напрямую обмениваться

данными с другими приложениями SNA и обеспечивает набор программных соглашений и протоколов, используемых LU 6.2. Узлы типа 2.1 (T2.1) представляют собой логические объекты, обеспечивающие непосредственный обмен данными между периферийными узлами, поддерживающими T2.1. Объект T2.1 способствует обмену данными типа "точка-точка", обеспечивая передачу данных между равноправными узлами APPC. Кроме того, T2.1 содержит контрольную точку периферийного узла (PNCP), сочетающую традиционные функции физического модуля (PU) и контрольной точки (CP).

Типы узлов IBM APPN

APPN предусматривает равноправный обмен данными между несколькими хорошо известными типами узлов. Эти узлы делятся на три основных вида: низкоуровневые, конечные и сетевые.

Низкоуровневые узлы (Low-Entry Nodes — LEN) относятся к равноправным узлам, существовавшим до APPN. В APPN низкоуровневые узлы позволяют пользоваться преимуществами служб, предоставляемых смежными с ними сетевыми узлами (NN). Контрольная точка LEN-узла управляет локальными ресурсами, но не устанавливает сеанс связи с контрольной точкой смежного сетевого узла.

Конечный узел (End Node — EN) поддерживает часть функций APPN. Его доступ к сети и маршрутизация обеспечивается смежным сетевым узлом. Для соединения с сетью, регистрации ресурсов, направления запросов службе каталогов и системе маршрутизации информации EN использует сеанс CP-CP.

Сетевой узел (Network Node — NN) выполняет все функции APPN. Его контрольная точка управляет ресурсами сетевого узла, а также смежных конечных и низкоуровневых узлов. Кроме того, CP сетевого узла устанавливает сеанс связи CP-CP со смежными конечными и сетевыми узлами и поддерживает базы данных сетевой топологии и каталогов, формируемые и обновляемые на основе информации, динамически получаемой от смежных сетевых и конечных узлов.

На рис. 39.5 показано место этих равноправных типов узлов в обобщенной среде APPN.

Службы APPN IBM

Основные службы APPN делятся на четыре категории: конфигурация, каталоги, топология и службы маршрутизации и сеанса связи. Эти службы описаны ниже.

Службы конфигурации IBM APPN

Службы конфигурации отвечают за активацию соединений в сети APPN. Активация соединения включает в себя установку соединения, установку сеанса и выбор режима смежности.

На стадии соединения происходит начальная установка соединения между узлами. Сюда входит обмен характеристиками и распределение ролей, таких как первичный и вторичный узел. Установка соединения завершается идентификационным обменом фреймами 3-го типа между узлами XID3 (eXchange IDentification type 3).

На стадии установки сеанса между смежными конечными или сетевыми узлами устанавливаются сеансы связи CP-CP. Каждый узел должен установить как минимум одну пару сеансов со смежным узлом. Конечный узел может установить не более одной такой

пары сеансов, но он может быть подключен к нескольким сетевым узлам. Между сетевыми узлами могут быть установлены пары сеансов CP-CP со всеми смежными узлами или с некоторыми из них. Минимальное требование состоит в наличии хотя бы одной пары сеансов со смежным сетевым узлом для правильного обновления топологии.

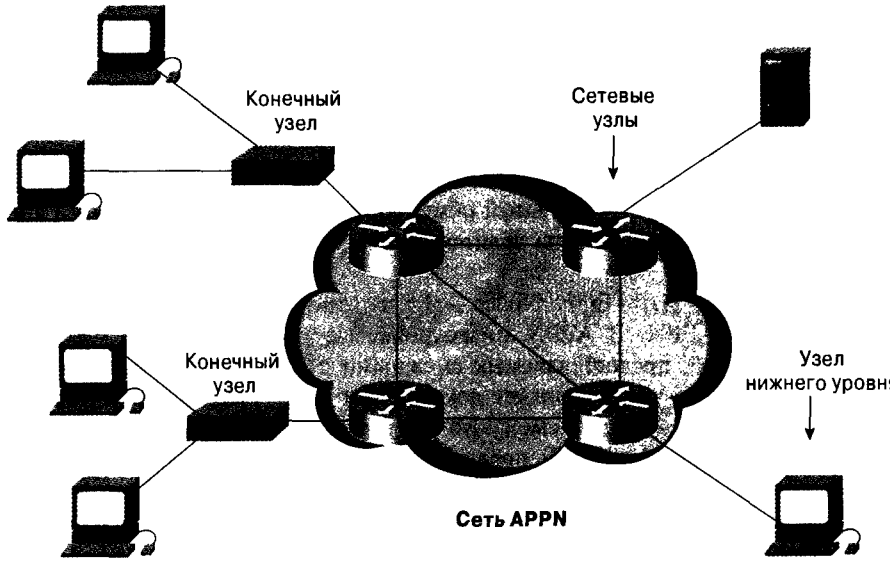


Рис. 39.5. APPN поддерживает несколько типов узлов

Смежность узлов APPN определяется сеансами CP-CP. Для определения смежности узлов применяются два настраиваемых параметра. Узел может быть смежным с одним узлом или логически смежным с любым возможным смежным узлом. Выбор режима смежности в конкретной ситуации зависит от требований сети. Сокращение количества сеансов CP-CP при одноузловой смежности может сократить нагрузки на сеть, связанные с обновлением топологии, а также количество необходимых для этого буферов. Однако сокращение количества смежных узлов увеличивает время, необходимое для синхронизации маршрутизаторов.

Службы каталогов IBM APPN

Службы каталогов помогают сетевым устройствам определять местонахождение провайдеров служб. Эти службы предназначены главным образом для создания сеанса между пользователями. В APPN службы каталогов обращаются к каждому сетевому узлу для формирования каталога локальных ресурсов и сетевого каталога, объединяющих пользователей и службы NN. Затем из отдельных сетевых каталогов NN формируется распределенная служба каталогов. В этом разделе описывается природа баз данных APPN, служба связи между узлами и каталогами, а также роль централизованной службы каталогов.

Локальные и сетевые базы данных каталогов поддерживают три типа записей: настраиваемые, зарегистрированные и кэшированные. Настраиваемые записи базы данных обычно являются локальными низкоуровневыми узлами, которые нуждаются в настройке из-за невозможности установить сеанс CP-CP для обмена информацией. Другие узлы также могут быть настроены для сокращения объема широковещательных

данных, который генерируется в процессе обнаружения. Зарегистрированные записи представляют собой записи локальных ресурсов, о которых конечный узел информирует смежный сервер сетевого узла во время установки сеанса CP-CP. Зарегистрированные записи вносятся сетевыми узлами в их локальный каталог. Кэшированные записи представляют собой записи каталогов, созданные в ответ на запрос сеанса и полученные сетевым узлом. Общее количество кэшированных записей может определяться пользователем для управления расходованием памяти.

Процесс согласования службы каталога конечного узла проходит в несколько этапов. Вначале EN посылает запрос LOCATE на NN, предоставляющий сетевые службы. Затем в базах данных локального и сетевого каталогов выполняется поиск пользователь-получатель. Если такой пользователь известен, посылается направленный запрос LOCATE, чтобы убедиться в доступности этого пользователя в данный момент. Если пользователь не найден в существующей базе данных, NN посылает запрос LOCATE смежным конечным узлам для определения, является ли пользователь локальным ресурсом. Если это не так, сетевой узел посылает широковещательный запрос LOCATE всем смежным сетевым узлам для распространения по сети. Когда NN, предоставляющий сетевые службы искомому пользователю, обнаружит его локальный ресурс, исходному NN будет отправлено сообщение о том, что пользователь-получатель найден. После этого NN-источник и NN-получатель кэшируют данную информацию.

Службы каталогов для узлов LEN управляются прокси-службами. В отличие от EN, посылающего запрос LOCATE, узел LEN сначала посылает запрос связанного сеанса (BIND) для присоединенного ресурса. Для получения LEN-узлом служб каталога NN должен обеспечить прокси-службы. Когда прокси-служба NN соединяется с LEN, NN отправляет широковещательный запрос LOCATED для LEN-узла.

Служба центрального каталога обычно находится в ACF/VTAM и предназначена для сокращения запросов LOCATE. Этот вид базы данных используется для обслуживания центрального каталога для всей сети, поскольку содержит настраиваемые, зарегистрированные и кэшированные записи. При обслуживании централизованным каталогом сетевой узел посылает широковещательный запрос LOCATE прямо на сервер центрального каталога, который затем при необходимости производит поиск в центральной базе данных и выполняет следующие широковещательные запросы.

Службы топологии и маршрутизации IBM APPN

В сетевой топологии APPN сетевые узлы связаны между собой трансмиссионными группами (Transmission Groups — TG). Каждая трансмиссионная группа состоит из отдельного канала, и все сетевые узлы поддерживают базу данных сетевой топологии, содержащую полную картину TT и TG в сети. Подробнее трансмиссионные группы описываются в главе 41.

База данных сетевой топологии обновляется посредством информации, получаемой из сообщений обновлений базы данных топологии (Topology Database Update — TDU). Эти TDU-сообщения передаются посредством сеансов CP-CP при любых изменениях в сети, таких как изменение активности узла или канала, затор в сети либо ограничение доступа к ресурсам.

База данных топологии содержит информацию, используемую при вычислении маршрутов для данного класса обслуживания (CoS). Эта информация включает данные о связности NN и TG, их состоянии и характеристиках, например пропускной способности.

Службы маршрутизации APPN использует информацию, получаемую из баз данных каталогов и топологии, чтобы определить маршрут для данного класса обслуживания. Определение маршрута начинается с получения конечным узлом запроса на сеанс от логического модуля. EN посылает запрос LOCATE на свой NN для получения информации о получателье, чтобы вычислить маршрут по сети. Сетевой узел определяет свойства, присущие запрашиваемому уровню обслуживания. Эти свойства сравниваются со свойствами каждой трансмиссионной группы и сетевого узла в сети, после чего все маршруты, удовлетворяющие данному критерию, признаются приемлемыми и кэшируются. Каждому EN, NN и TG в сети присваивается вес, исходя из свойств CoS: пропускная способность, стоимость, защищенность, задержка. Свойства также могут определяться пользователем. Наконец, путем сравнения весов всех маршрутов, удовлетворяющих критерию маршрутизации, выбирается маршрут с наименьшими затратами.

Службы сеансов IBM APPN

После выбора маршрута дальнейший процесс установки сеанса APPN зависит от типа узла. Если пользователь-источник соединен с конечным узлом, конечному узлу возвращается от NN, смежного с EN-получателем, ответ LOCATE, содержащий данные о расположении получателя и маршруте. Затем EN-источник посылает запрос BIND на маршрут сеанса. Если же пользователь подключен к LEN-узлу, то этот узел посылает запрос BIND на смежный NN. Смежный NN преобразует запрос LEN BIND в APPN BIND и отправляет его по маршруту сеанса.

BIND является особым типом сообщения-запроса, который посылается одним LU другому LU. В нем содержится маршрут, используемый для сеанса. В нем указываются NN и TG, приоритет передачи для сеанса и информация об окне для поддержки адаптивной установки скорости передачи с целью ограничения объема передаваемых данных.

Формат базового информационного модуля

Базовые информационные модули (Basic Information Unit — BIU) используются в IBM SNA для обмена запросами и ответами на них. Формат BIU показан на рис. 39.6.

Поля BIU

Ниже описаны поля BIU, определяющие его содержание и показанные на рис. 39.6.

- **Заголовок запроса.** Определяет тип данных в модуле запроса. Содержит информацию о формате данных и определяет протоколы для сеанса. Информация из заголовка запроса используется только NAU.
- **Модуль запроса.** Содержит либо данные пользователя, либо команды SNA. Команды SNA посылаются в модулях командных запросов, которые служат для управления сетью и содержат информацию, передаваемую между пользователями.
- **Заголовок ответа.** Определяет тип данных модуля ответа. Пакеты ответов от пакетов запросов отличаются битом-индикатором "запрос/ответ". NAU-получатель сообща-

ет, является ли ответ на запрос положительным или отрицательным при помощи индикатора типа ответа (Response Type Indicator — RTI) в заголовке ответа.

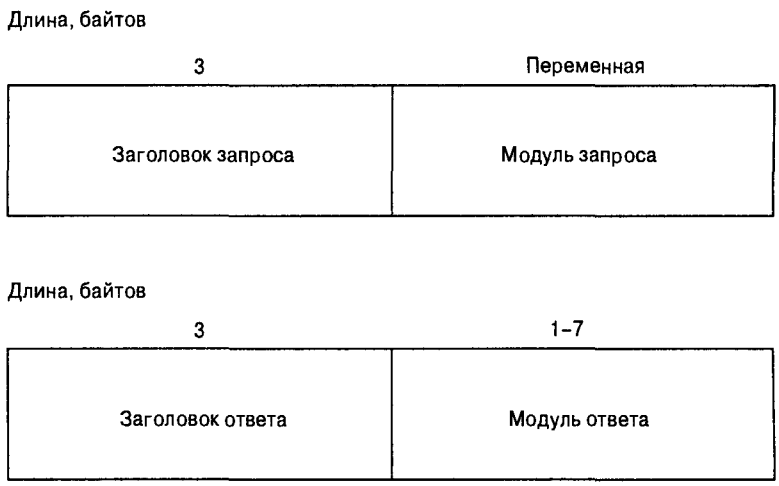


Рис. 39.6. Базовый информационный модуль может быть либо запросом, либо ответом

- **Модуль ответа.** Содержит информацию об ответе: положительный или отрицательный. Длина модуля положительного ответа на командный запрос обычно составляет 1-3 байта, идентифицирующих командный запрос. Положительные ответы на запросы данных содержат заголовки ответа, но не модуль ответа.

Длина модулей отрицательных ответов составляет 4-7 байтов. NAU-получатель возвращает отрицательный ответ запрашивающему NAU в одном из следующих случаев:

- отправитель нарушил протокол SNA;
- получатель не распознал переданные данные;
- возникла внештатная ситуация, например сбой маршрута.

При передаче отрицательного ответа первые четыре байта модуля ответа содержат данные о его причине. NAU-получатель может отправить до трех дополнительных байт, идентифицирующих отвергнутый запрос.

Формат маршрутного информационного модуля

Маршрутный информационный модуль (Path Information Unit — PIU) представляет собой модуль сообщения SNA, формируемый элементами управления маршрутом из заголовка передачи и базового информационного модуля. Формат PIU показан на рис. 39.7.

Поля PIU

Ниже описаны поля PIU, показанные на рис. 39.7.

Рис. 39.7. Маршрутный информационный модуль запроса и ответа

- **Заголовок передачи.** Передает сообщения по маршруту. Содержит маршрутную информацию для традиционной организации подсети SNA. Форматы заголовка передачи различаются по типу идентификации форматов (FID). При управлении маршрутом типы FID используются для маршрутизации данных по узлам SNA. В PIU существуют следующие три типа FID.
  - — **FID0** используется для маршрутизации данных между смежными узлами подзоны для устройств, не принадлежащих SNA. Сейчас на смену ему постепенно приходит FID4, определяющий, принадлежит ли устройство архитектуре SNA.
  - — **FID1** используется для маршрутизации данных между смежными узлами подзоны, если один или оба узла не поддерживают явный и виртуальный протоколы маршрутизации.
  - — **FID2** используется для маршрутизации данных между пограничным узлом подзоны и смежным периферийным узлом, или между смежными узлами типа 2.1. Обычно заголовок передачи используется для маршрутизации данных между смежными узлами подзоны, когда оба узла поддерживают явный и виртуальный протоколы маршрутизации.
- **Заголовок запроса.** Определяет тип данных в модуле запроса. Этот заголовок предоставляет информацию о формате данных и определяет протоколы для сеанса. Информацию заголовка запроса используют только NAU.
- **Модуль запроса.** Содержит данные пользователя или команды SNA. Данные пользователя отправляются в модулях ответа данных, а команды SNA — в командных модулях ответа. Они предназначены для управления сетью и обмена информацией между пользователями.

- **Заголовок ответа.** Определяет тип данных модуля ответа. Пакеты ответов от пакетов запросов отличаются битом-индикатором "запрос/ответ". NAU-получатель сообщает, является ли ответ на запрос положительным или отрицательным при помощи индикатора типа ответа (Response Type Indicator — RTI) в заголовке ответа.
- **Модуль ответа.** Содержит информацию об ответе: положительный или отрицательный. Модуль положительного ответа на командный запрос обычно состоит из 1-3 байтов, идентифицирующих командный запрос. Положительные ответы на запросы данных содержат заголовки ответа, но не модуль ответа.

Длина модулей отрицательных ответов составляет 4-7 байтов. NAU-получатель возвращает отрицательный ответ запрашивающему NAU в одном из следующих случаев: отправитель нарушил протокол SNA; получатель не распознал переданные данные; возникла внештатная ситуация, например сбой маршрута.

При передаче отрицательного ответа первые четыре байта модуля ответа содержат данные о его причине. NAU-получатель может отправить до трех дополнительных байтов, идентифицирующих отвергнутый запрос.

Резюме

Системная сетевая архитектура IBM является одним из первых сетевых протоколов. Несмотря на то, что в настоящее время она считается устаревшей, она по-прежнему широко распространена. В основе системной сетевой архитектуры лежит коммуникационная модель "узел-терминал", используемая мэйнфреймами IBM.

IBM расширила протокол SNA для поддержки одноранговой сети. Эти расширения получили названия: улучшенный протокол одноранговых сетей (Advanced Peer-to-Peer Networking — APPN) и протокол улучшенных межпрограммных вычислений (Advanced Program-to-Program Computing — APPC).

Контрольные вопросы

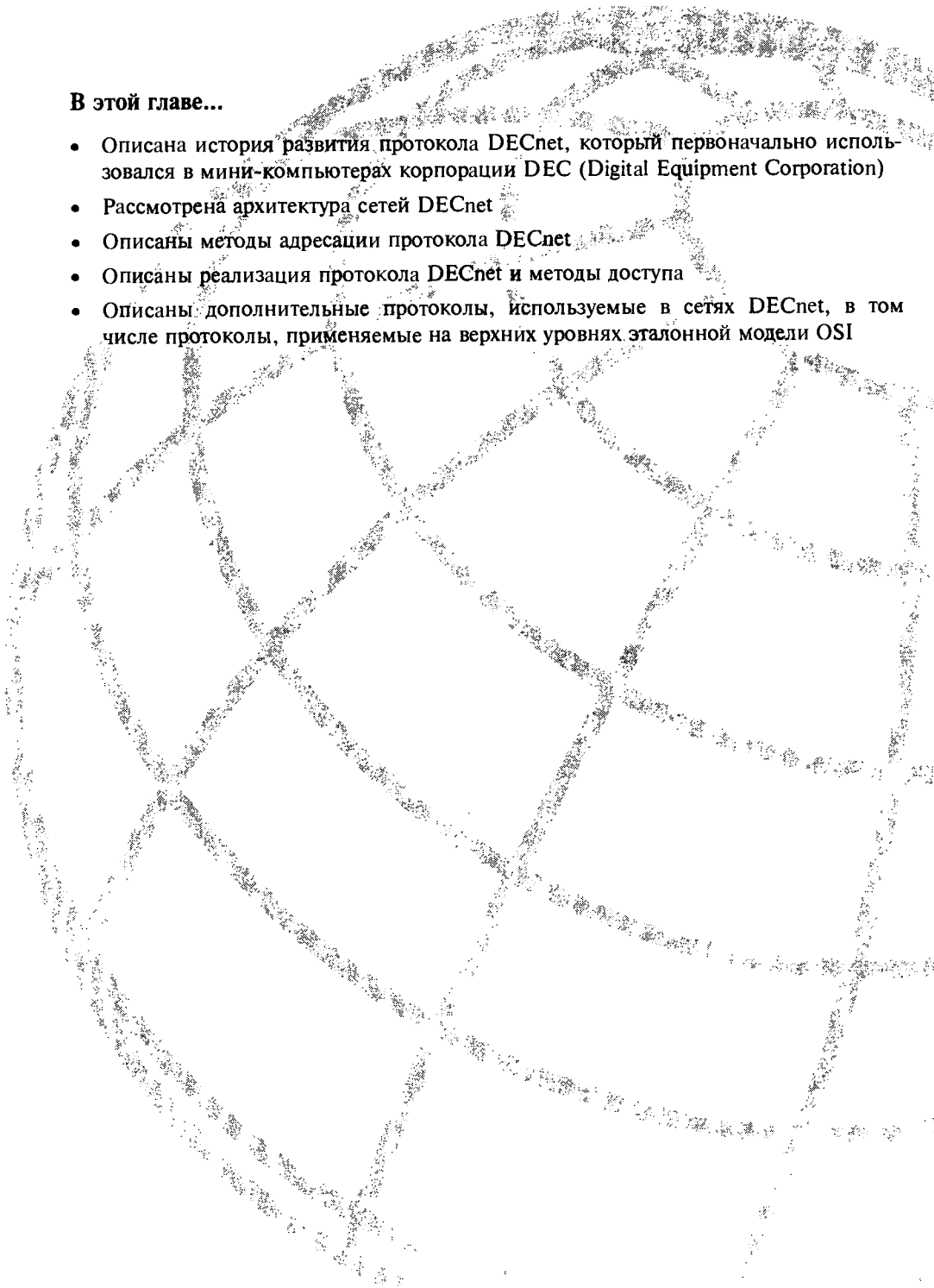
1. Что разработала IBM для того, чтобы приспособить свой протокол к одноранговой сети?
2. Какие типы физических устройств поддерживает SNA?
3. Какие три типа сетевых адресуемых модулей поддерживает SNA?
4. Каковы функции логического модуля?
5. Каковы функции физического модуля?
6. Каковы функции контрольной точки?
7. Назовите три типа хорошо известных узлов в APPN.
8. Назовите четыре основные категории служб в APPN.
9. Для чего предназначена база данных сетевой топологии?

Дополнительные источники

http://www.networking.ibm.com/app/aiwconf/cpic.htm

В этой главе...

- Описана история развития протокола DECnet, который первоначально использовался в мини-компьютерах корпорации DEC (Digital Equipment Corporation)
- Рассмотрена архитектура сетей DECnet
- Описаны методы адресации протокола DECnet
- Описаны реализация протокола DECnet и методы доступа
- Описаны дополнительные протоколы, используемые в сетях DECnet, в том числе протоколы, применяемые на верхних уровнях эталонной модели OSI



Глава 40

Протоколы DECnet

Введение

DECnet представляет собой группу продуктов для обмена данными, в которую входят набор протоколов, разработанных и поддерживаемых корпорацией Digital Equipment Corporation (Digital). Первая версия DECnet, появившаяся в 1975 г., обеспечивала связь между двумя непосредственно соединенными мини-компьютерами PDP-11. В последние годы Digital стала поддерживать протоколы других разработчиков, но DECnet остается главным сетевым продуктом Digital. В этой главе описываются набор протоколов DECnet, сетевые архитектуры Digital и основы управления потоками DECnet.

На рис. 40.1 приведена объединенная сеть DECnet с маршрутизаторами, соединяющими две локальных сети, содержащих рабочие станции и компьютеры VAX.

Было выпущено несколько версий DECnet. Первая обеспечивала обмен данными между двумя мини-компьютерами, соединенными напрямую.

В последующих версиях функциональность DECnet была расширена. Появилась поддержка дополнительных собственных и стандартных протоколов, но сохранилась совместимость с предшествующей версией. Таким образом, протоколы DECnet обратно совместимы. В настоящее время широко используются две версии DECnet: DECnet Phase IV и DECnet/OSI.

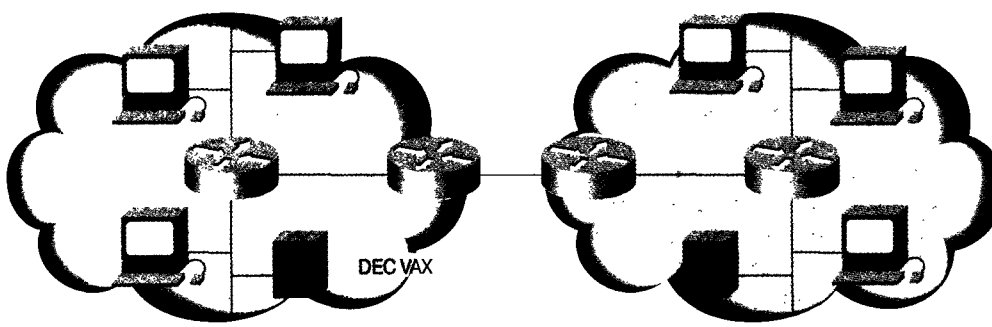


Рис. 40.1. В сети DECnet рабочие станции и VAX соединяются через маршрутизаторы

DECnet Phase IV является наиболее распространенной версией DECnet. Но последней версией является DECnet/OSI. Версия DECnet Phase IV основана на цифровой сетевой архитектуре (Digital Network Architecture — DNA) Phase IV и поддерживает фирменные протоколы Digital, фирменные протоколы других разработчиков и стандартные протоколы. DECnet Phase IV сохраняет обратную совместимость с предшествующей ей версией DECnet Phase III.

DECnet/OSI (также называемая DECnet Phase V) является последней версией DECnet и сохраняет обратную совместимость с DECnet Phase IV. Эта версия основана на DNA DECnet/OSI. Версия DECnet/OSI поддерживает некоторые из протоколов OSI, многие фирменные протоколы DECnet, фирменные протоколы других разработчиков и стандартные протоколы.

Архитектура DECnet Phase IV

Цифровая сетевая архитектура (Digital Network Architecture — DNA) представляет собой всеобъемлющую многоуровневую сетевую архитектуру, которая поддерживает большое количество фирменных и стандартных протоколов. Архитектура DNA Phase IV аналогична архитектуре, описанной в эталонной модели OSI. Как и в эталонной модели OSI, в DNA Phase IV используется многоуровневый подход, при котором функции данного уровня предоставляют службы для протоколов верхних уровней и, в свою очередь, зависят от протоколов нижних уровней. Но, в отличие от модели OSI, архитектура DNA Phase IV состоит из восьми уровней. На рис. 40.2 показано соответствие восьми уровней DNA Phase IV эталонной модели OSI.

В следующем разделе будут более подробно описаны функции и роль каждого из этих уровней, а также отмечены общие элементы архитектур DNA Phase IV и эталонной модели OSI.

Уровни DNA Phase IV

В DNA DECnet Phase IV определена восьмиуровневая модель, изображенная на рис. 40.2. Уровень пользователя представляет собой сетевой интерфейс пользователя, поддерживающий пользовательские службы и программы с коммуникационными компонентами. Уровень пользователя в целом соответствует уровню приложений OSI. Уровень управления сетью служит интерфейсом между пользователем и информацией по управлению сетью. Этот уровень взаимодействует со всеми нижними уровнями DNA и в целом соответствует уровню приложений OSI. Уровень сетевых приложений предоставляет различные сетевые приложения, такие как удаленный доступ к файлам и виртуальный терминальный доступ. Этот уровень примерно соответствует уровням OSI представлений и приложений.

Уровень управления сеансом управляет логическими канальными соединениями между конечными узлами и в целом соответствует сеансовому уровню OSI. Уровень конечных коммуникаций обеспечивает управление потоком, сегментацию и компоновку и соответствует транспортному уровню OSI. Уровень маршрутизации осуществляет маршрутизацию и другие действия и соответствует сетевому уровню OSI. Канальный уровень управляет каналами физической сети и соответствует канальному уровню OSI. Физический уровень управляет интерфейсами оборудования и определяет электрические и механические функции физических носителей; этот уровень соответствует физическому уровню OSI.

Рис. 40.2. Архитектура DNA DECnet Phase IV состоит из восьми уровней, соответствующих уровням эталонной модели OSI

Адресация протокола DECnet Phase IV

Адреса DECnet не связаны с физическими сетями, к которым подключены узлы. DECnet идентифицирует узлы адресными парами "зона/узел". Значения зон находятся в диапазоне от 1 до 63, а адрес узла — в диапазоне от 1 до 1023. Таким образом, в каждой зоне может быть до 1023 узлов, а всего сеть DECnet позволяет адресовать около 65000 узлов. Зоны могут охватывать несколько маршрутизаторов, а один кабель может поддерживать несколько зон. Поэтому, если у узла есть несколько сетевых интерфейсов, то он использует один и тот же адрес "зона/узел" для всех интерфейсов. На рис. 40.3 приведен пример сети DECnet с несколькими адресуемыми объектами.

Узелы DECnet не используют MAC-адреса, назначаемые производителем. Вместо этого адреса сетевого уровня встраиваются в MAC-адреса в соответствии с алгоритмом, который умножает номер зоны на 1024 и к результату добавляет номер узла. Полученный 16-разрядный десятичный адрес преобразуется в шестнадцатеричное число и присоединяется к адресу AA00.0400 с перестановкой байтов, для того, чтобы младшие байты передавались первыми. Например, адрес DECnet 12.75 превращается в десятичный 12363, который равен шестнадцатеричному 304B. После того как этот адрес с переставленными байтами присоединяется к стандартному префиксу MAC-адреса DECnet, получается адрес AA00.0400.4B30.

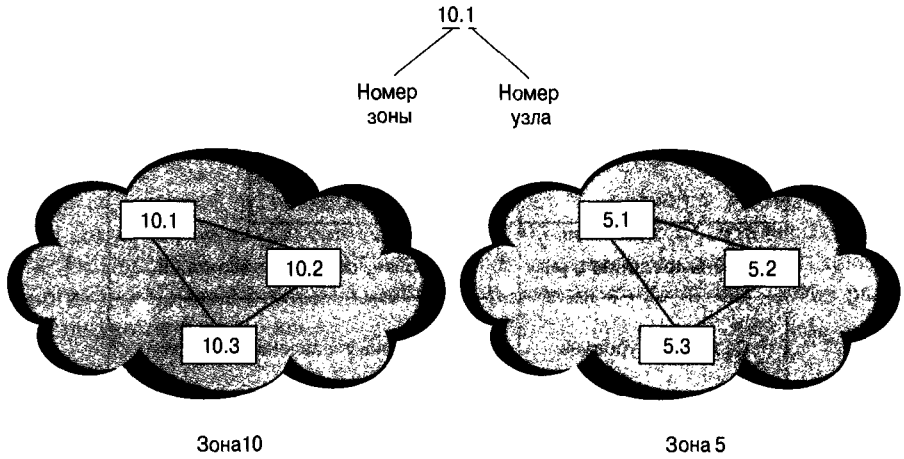


Рис. 40.3. Протокол DECnet идентифицирует узлы, используя адресные пары "зона/узел"

Архитектура DECnet/OSI

Архитектура DNA DECnet /OSI (DECnet Phase V) во многом аналогична архитектуре, описанной в эталонной модели OSI. В DECnet Phase V используется многоуровневый подход, обеспечивающий значительную гибкость в смысле поддержки набора протоколов верхних уровней. В следующем разделе будет показано, что DECnet OSI поддерживает несколько наборов протоколов.

Реализации DNA DECnet/OSI

Архитектура DNA DECnet/OSI определяет многоуровневую модель, в которой используются три набора протоколов: протоколы OSI, DECnet и протокол управления передачей/протокол Internet (Transmission Control Protocol/Internet Protocol — TCP/IP). OSI-реализация DECnet/OSI согласована с семиуровневой эталонной моделью OSI и поддерживает многие стандартные протоколы OSI. Digital-реализация DECnet/OSI обеспечивает обратную совместимость с DECnet Phase IV и поддерживает различные фирменные протоколы корпорации Digital. TCP/IP-реализация DECnet/OSI поддерживает протоколы TCP/IP нижних уровней и позволяет передавать потоки DECnet по транспортным протоколам TCP. На рис. 40.4 представлены три реализации DECnet/OSI.

Доступ DECnet к среде передачи

Версии DECnet Phase IV и DECnet/OSI поддерживают различные реализации доступа к среде передачи на физическом и канальном уровнях, благодаря чему протоколы DECnet получили довольно широкое распространение в индустрии компьютерных сетей. Ниже будет показано, что DECnet Phase IV и Phase V поддерживают многие основные современные физические и канальные технологии.

На физическом уровне версии DECnet Phase IV и DECnet/OSI поддерживают большинство распространенных физических реализаций, в том числе Ethernet/IEEE 802.3, То-

ken Ring/IEEE 802.5 и Fiber Distributed Data Interface (FDDI). Кроме того, DECnet/OSI поддерживает протоколы Frame Relay и X.21bis.

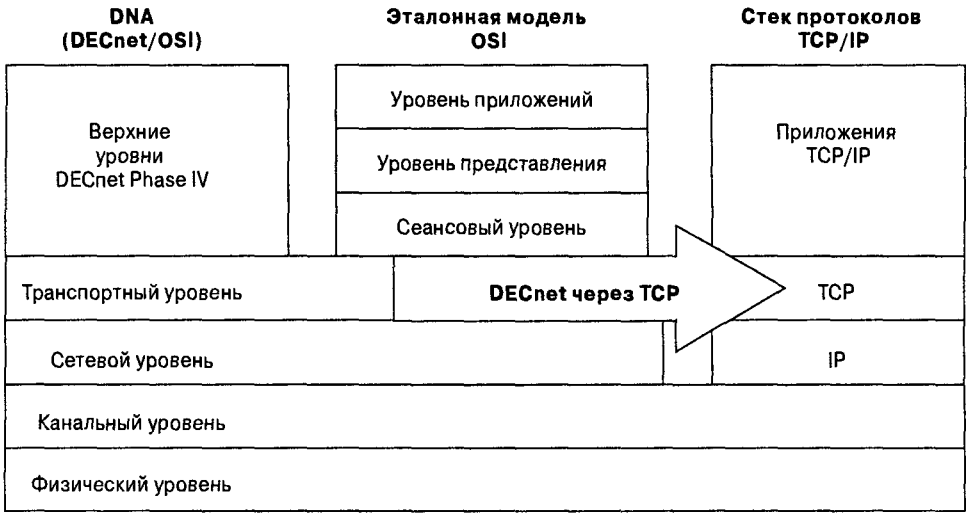


Рис. 40.4. Архитектура DECnet/OSI DNA поддерживает протоколы OSI, DECnet и TCP

На канальном уровне DECnet Phase IV и DECnet/OSI поддерживают протоколы IEEE 802.2 Logical Link Control (LLC), Link Access Procedure, Balanced (LAPB), Frame Relay (FR) и High-Level Data Link Control (HDLC). Кроме того, DECnet Phase IV и DECnet/OSI поддерживают фирменный канальный протокол корпорации Digital — Digital Data Communications Message Protocol (DDCMP), который обеспечивает многоточечные соединения и соединения "точка-точка", дуплексную и полудуплексную коммуникацию по синхронным и асинхронным каналам, коррекцию ошибок, упорядочение и управление.

Маршрутизация DECnet

Маршрутизация DECnet выполняется на уровне маршрутизации DNA в DECnet Phase IV и на сетевом уровне модели OSI в DECnet/OSI. Несмотря на это, маршрутизация в DECnet Phase IV во многом похожа на маршрутизацию в DECnet/OSI.

Маршрутизация DECnet Phase IV реализуется протоколом маршрутизации DECnet (DECnet Routing Protocol — DRP). Это относительно простой и эффективный протокол, основная задача которого состоит в определении оптимального пути по сети DECnet Phase IV. На рис. 40.5 приведен пример, иллюстрирующий маршрутизацию в сети DECnet Phase IV.

Маршрутизация DECnet основана на оценке (cost) — произвольной метрике, присваиваемой сетевым администратором различным маршрутам через объединенную сеть для их сравнения. Обычно оценка выражается в количестве узлов или пропускной способности среды передачи. Чем ниже оценка, тем лучше маршрут. При повреждении сети протокол DRP использует величину оценки для определения другого лучшего маршрута для каждого получателя.

Маршрутизация DECnet/OSI используется стандартными протоколами маршрутизации OSI (ISO 8473, ISO 9542 и ISO 10589) и DRP. Более подробно протоколы маршрутизации OSI описываются в главе 48 "Протоколы маршрутизации OSI".

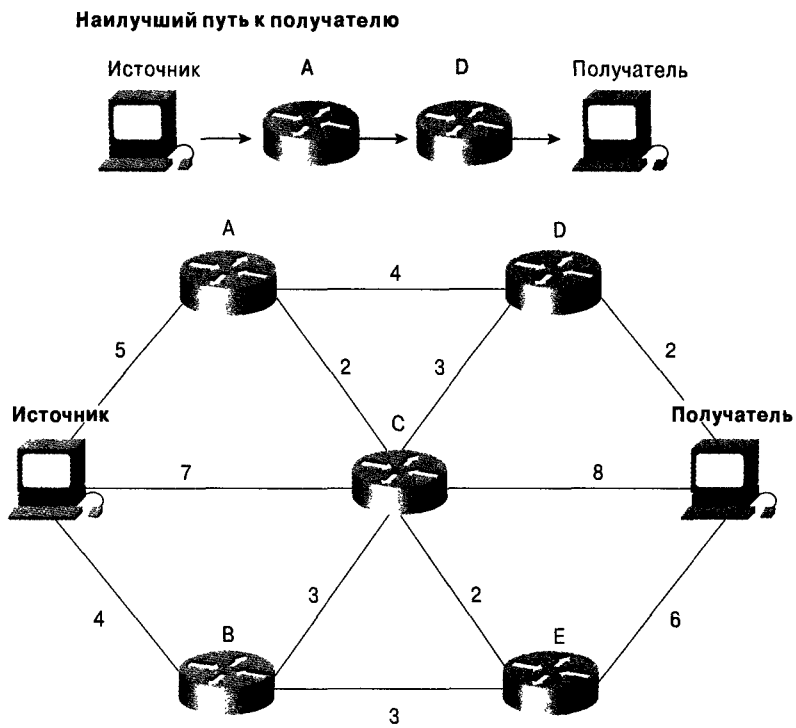


Рис. 40.5. Протокол DRP вычисляет оптимальный маршрут по сети DECnet Phase IV

Уровень конечных коммуникаций DECnet

DECnet Phase IV поддерживает на уровне конечных коммуникаций DNA один транспортный протокол — протокол сетевых служб (Network-Services Protocol — NSP).

Протокол NSP

Протокол сетевых служб (Network-Services Protocol — NSP) представляет собой фирменный, ориентированный на соединение протокол конечных коммуникаций, разработанный корпорацией Digital, который отвечает за установку и разрыв соединений между узлами, выполняет фрагментацию и компоновку сообщений и управление коррекцией ошибок.

Кроме того, NSP отвечает за два типа управления потоками: простой старт-стопный механизм — в этом случае получатель сообщает отправителю, когда прервать и когда продолжить передачу данных, и более сложную схему, при которой получатель сообщает отправителю, сколько сообщений он способен принять.

Транспортный уровень DECnet/OSI

DECnet/OSI поддерживает протокол NSP, три стандартных транспортных протокола OSI и протокол TCP.

DECnet/OSI поддерживает классы транспортных протоколов TP0, TP2 и TP4. TP0 представляет собой простейший транспортный протокол OSI, ориентированный на соединение. Из классических функций транспортного уровня он выполняет только сегментацию и компоновку. Это означает, что TP0 отмечает наименьший из модулей PDU максимального размера, поддерживаемых основными подсетями, и разбивает транспортный пакет на меньшие части, которые не будут слишком большими для передачи по сети. TP2 может мультиплексировать и демультиплексировать потоки данных, передаваемых по виртуальному каналу. Эта способность делает TP2 частично полезным в открытых сетях данных (PDN), где оплачивается каждый виртуальный канал. Как и TP0 и TP1, протокол TP2 также сегментирует и компонует модули PDU, в то время как протокол TP3 объединяет в себе функции протоколов TP1 и TP2. TP4, наиболее популярный транспортный протокол OSI, аналогичен протоколу TCP стека протоколов Internet. На самом деле он был основан на этой модели. Кроме функций TP3, TP4 обеспечивает службы надежной передачи данных и предполагает, что в сети не выполняется обнаружение ошибок.

Использование протоколов транспортного уровня OSI с TCP описано в RFC 1006 и RFC 1006. RFC 1006 определяет использование с TCP транспортного протокола OSI класса 0, а RFC 1006 — использование с TCP транспортного протокола класса 2.

Верхние уровни DECnet Phase IV

В DECnet Phase IV DNA определены четыре верхних уровня: взаимодействие с пользователями, управление сетью, передача файлов и управление сеансами. Соответственно, они называются уровнем пользователя, уровнем управления сетью, уровнем сетевых приложений и уровнем управления сеансом. Более подробно верхние уровни архитектуры DECnet Phase IV обсуждаются ниже.

Уровень пользователя

Уровень пользователя DNA поддерживает пользовательские службы и программы, которые взаимодействуют с пользовательскими приложениями. Пользователь взаимодействует с этими приложениями непосредственно, а приложения пользуются службами и программами, обеспечиваемыми уровнем пользователя.

Уровень управления сетью

Протокол управления сетью (Network Information and Control Exchange — NICE), широко используемый в сетях DECnet, является фирменным протоколом корпорации Digital. NICE представляет собой протокол, реагирующий на команды. Команды, запрашивающие какие-либо действия, посылаются управляемому узлу или процессу, а реакции, в форме действий, возвращаются этими узлами или процессами. NICE выполняет несколько функций, связанных с управлением сетью, и может быть использован для передачи операционной системы от локального устройства к удаленному, а также позволяет неиспользуемой удаленной системе передать содержимое своей памяти локальной системе. Протоколы, использующие NICE, могут тестировать или изменять некоторые параметры сети. NICE ведет журнал событий, куда автоматически заносятся такие важные сетевые события, как изменение состояний смежности или состояния каналов. Протокол NICE

поддерживает функции, позволяющие тестировать оборудование и обнаруживать межузловые петли.

Некоторые функции управления сетью могут использовать *протокол поддержки операций (Maintenance Operations Protocol — MOP)* — набор функций, не требующих уровней DNA между уровнем управления сетью и канальным уровнем. Это обеспечивает доступ к узлам, у которых работают только канальные службы.

Уровень сетевых приложений

Протокол доступа к данным (Data-Access Protocol — DAP) представляет собой фирменный протокол корпорации Digital, используемый DECnet Phase IV на уровне сетевых приложений. DAP обеспечивает удаленный доступ к файлам и удаленную пересылку файлов — службы, используемые приложениями на уровне управления сетью и на уровне пользователя. Кроме того, на уровне сетевых приложений работают следующие фирменные протоколы Digital: протокол MAIL, который обеспечивает обмен почтовыми сообщениями, и CTERM, обеспечивающий удаленный интерактивный доступ к терминалу.

Уровень управления сеансом

Протокол управления сеансом (Session Control Protocol — SCP) представляет собой протокол уровня управления сеансом DECnet Phase IV, выполняющий несколько функций. В частности, SCP запрашивает логическое соединение у конечных устройств, получает запросы логических соединений от конечных устройств, принимает или отвергает запросы логических соединений, преобразует имена в адреса и ликвидирует логическое соединение.

Верхние уровни DECnet/OSI

Архитектура DECnet/OSI DNA основана на эталонной модели OSI. На каждом из верхних уровней DECnet/OSI поддерживает два набора протоколов: протоколы OSI и протоколы DECnet Phase IV (для обратной совместимости). DECnet/OSI поддерживает функции уровней приложений, представления и сеансового уровня.

Уровень приложений

DECnet/OSI использует стандартные реализации уровня приложений OSI, а также такие стандартные процессы уровня приложений, как Common Management-Information Protocol (CMIP) и File Transfer, Access, and Management (FTAM). DECnet/OSI также поддерживает все протоколы, реализованные в DECnet Phase IV на уровне пользователя и на уровне управления сетью, в том числе протокол NICE.

Уровень приложений OSI содержит реальные приложения и элементы служб приложений (Application Service Elements — ASE). Элементы ASE облегчают обмен данными между уровнем приложений и нижними уровнями. Тремя наиболее важными элементами ASE являются Association Control Service Element (ACSE), Remote Operations Service Element (ROSE) и Reliable Transfer Service Element (RTSE).

ACSE логически связывает названия приложений друг с другом для подготовки к обмену данными между приложениями. ROSE реализует типичный механизм "запрос-

ответ", который позволяет работать в режиме удаленного доступа, подобно вызову удаленной процедуры (remote procedure call —RPC). RTSE обеспечивает надежность доставки, упрощая использование конструкций сеансового уровня.

Уровень представления

Протокол DECnet/OSI использует все стандартные реализации уровня представления OSI. Он также поддерживает все протоколы, реализованные в версии DECnet Phase IV на уровне сетевых приложений DNA. Наиболее важным из них является протокол доступа к данным (Data-Access Protocol — DAP).

Обычно уровень представления эталонной модели OSI представляет собой лишь промежуточный протокол для передачи информации смежных уровней. Хотя многие считают, что Abstract Syntax Notation 1 (ASN.1) является протоколом уровня представлений OSI, ASN.1 используется для преобразования форматов данных в машинонезависимые форматы. Это обеспечивает связь между приложениями на различных компьютерных системах (ES) способом, прозрачным для приложений.

Сеансовый уровень

Протокол DECnet/OSI использует все стандартные реализации сеансового уровня OSI. Он также поддерживает все протоколы, реализованные в DECnet Phase IV на уровне управления сеансом DNA. Первичным протоколом уровня управления сеансом является протокол управления сеансом (Session Control Protocol — SCP). Используя различные механизмы управления протокол уровня управления сеансом OSI преобразует потоки данных, предоставляемые нижними четырьмя уровнями, в сеансы. Эти механизмы включают в себя учет, управление обменом данными и согласование параметров сеанса. Управление обменом данными сеанса осуществляется с помощью маркера, наличие которого дает право на соединение. Маркер можно запросить, а компьютерная система ES может получить приоритет, обеспечивающий первоочередное использование маркера.

На рис. 40.6 полностью приведены стеки протоколов DECnet Phase IV и DECnet/OSI, включая использование протокола DECnet/OSI с TCP.

Резюме

Преимущества протокола DECnet проявляются в специализированных сетях, использующих оборудование корпорации Digital. В настоящее время этот протокол используется редко, однако все еще встречается в некоторых традиционных сетях.

Контрольные вопросы

1. Как узлы DECnet используют назначаемые производителем MAC-адреса?
2. Какой протокол в DECnet Phase IV отвечает за маршрутизацию?
3. Какие функции выполняет протокол NSP?
4. Какие функции выполняет протокол SCP?
5. Какие функции в DECnet выполняются на уровне пользователя?

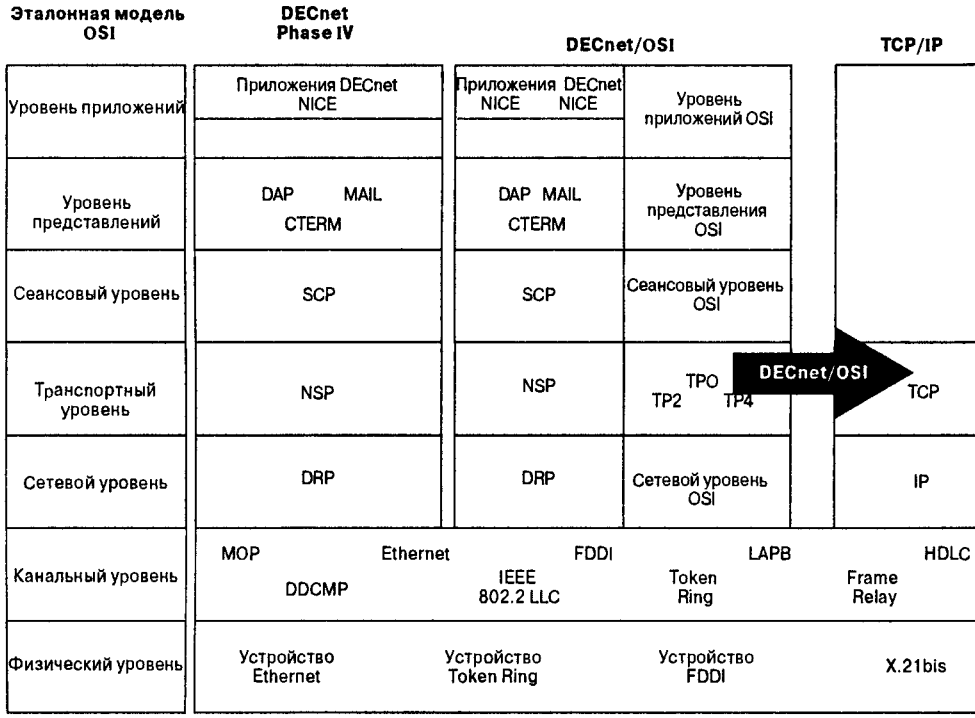
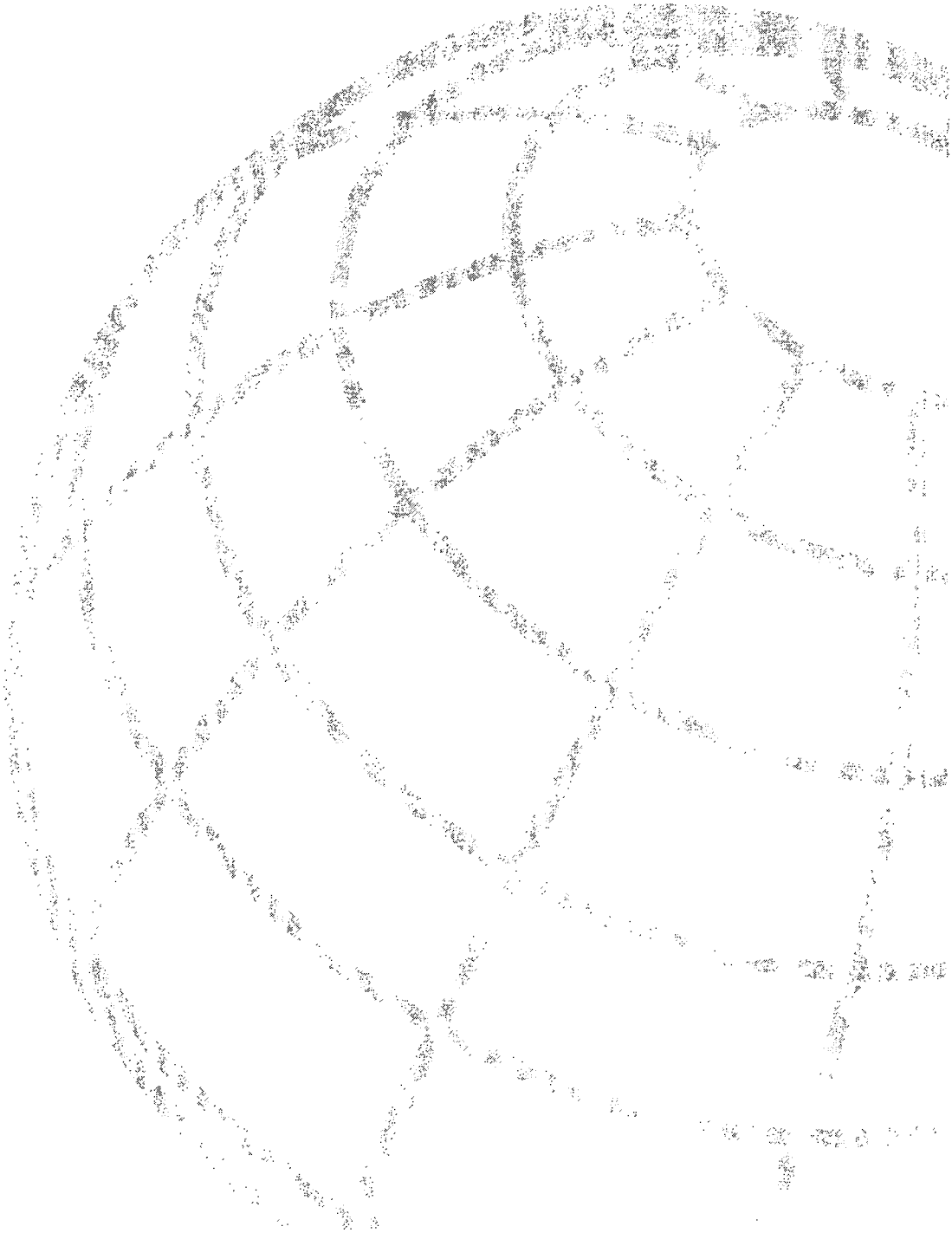


Рис. 40.6. DECnet Phase IV и DECnet/OSI поддерживают одни и те же спецификации физического и канального уровней



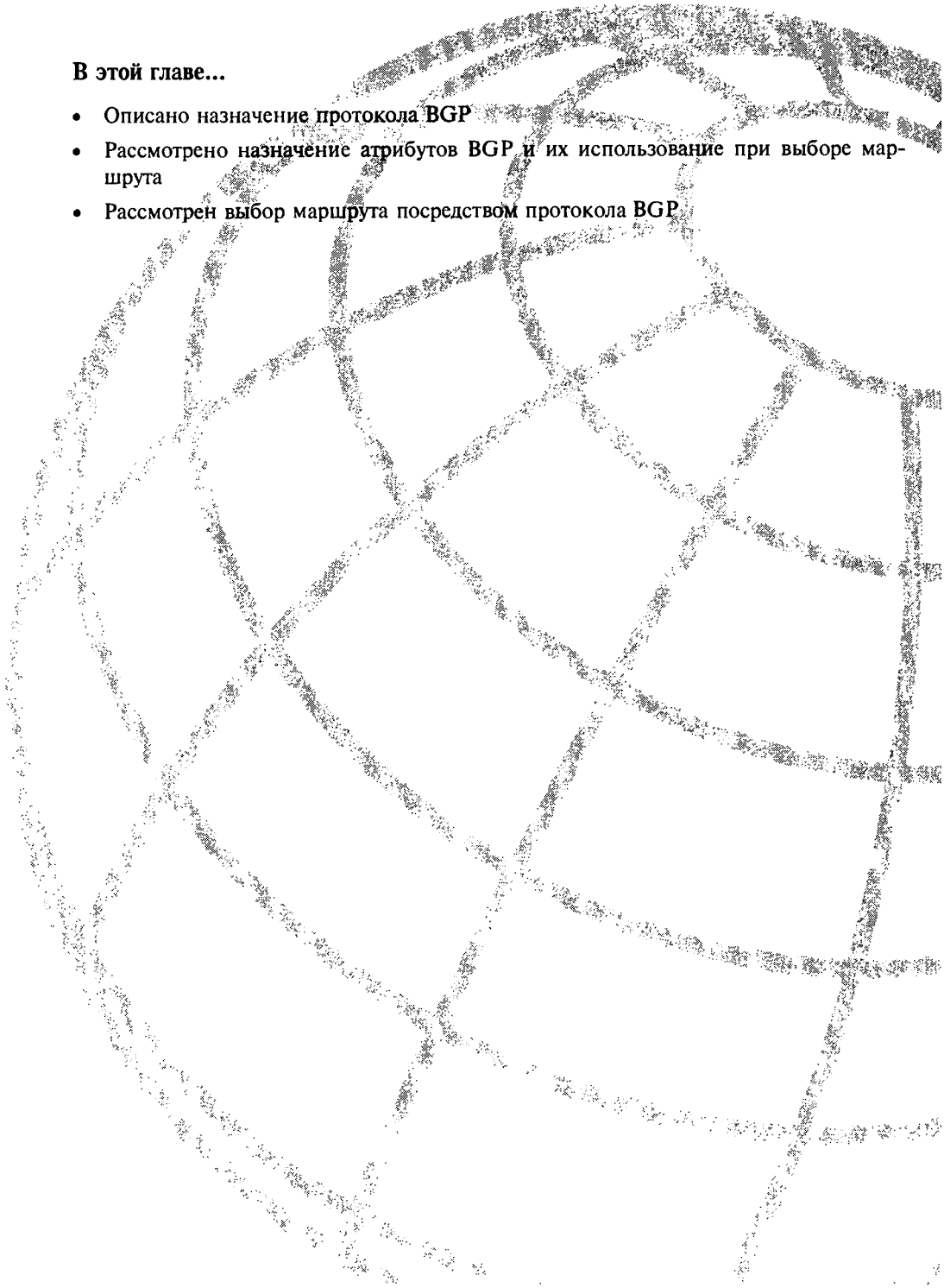
Часть VII

Протоколы маршрутизации

Глава 41. Протокол BGP
Глава 42. Протокол EIGRP
Глава 43. Маршрутизация в системной сетевой архитектуре IBM
Глава 44. Протокол IGRP
Глава 45. Многоадресатная рассылка
Глава 46. Протокол NSLP
Глава 47. Протокол OSPF
Глава 48. Протоколы маршрутизации OSI
Глава 49. Протокол RIP
Глава 50. Протокол RSVP
Глава 51. Протокол SMRP

В этой главе...

- Описано назначение протокола BGP
- Рассмотрено назначение атрибутов BGP и их использование при выборе маршрута
- Рассмотрен выбор маршрута посредством протокола BGP



Глава 41

Протокол BGP

Введение

Протокол граничного шлюза (Border Gateway Protocol — BGP) представляет собой протокол маршрутизации, который используется при передаче данных между автономными системами. Автономной системой называется сеть или группа сетей с общим администрированием и общей стратегией маршрутизации. Протокол BGP используется для обмена маршрутной информацией в сети Internet и является протоколом, используемым между провайдерами услуг Internet (Internet Service provider — ISP). В сетях пользователей, таких как университеты и корпорации, для обмена маршрутной информацией между сетями обычно применяются протоколы внутреннего шлюза (Interior Gateway Protocol — IGP), такие как RIP или OSPF. Пользователи подключаются к ISP-провайдерам, а последние используют BGP для обмена маршрутной информацией между пользователем и провайдером ISP. Когда протокол BGP используется для обмена между автономными системами (autonomous system — AS), он называется внешним BGP (External BGP — EBGP). Если провайдер служб Internet использует протокол BGP для обмена маршрутами внутри автономной системы AS, то этот протокол называется внутренним (Interior BGP — IBGP). Это различие проиллюстрировано на рис. 41.1.

BGP является очень устойчивым и легко масштабируемым протоколом маршрутизации. Об этом свидетельствует тот факт, что он применяется в сети Internet. На время написания этой книги таблицы маршрутизации протокола Internet BGP насчитывали более 90000 маршрутов. Для обеспечения такого уровня масштабируемости протокол BGP использует множество параметров маршрута, называемых атрибутами, которые определяют стратегию и поддерживают стабильную среду маршрутизации.

Для уменьшения размеров таблиц маршрутизации Internet протокол BGP, кроме атрибутов, использует бесклассовую междоменную маршрутизацию (Classless InterDomain Routing — CIDR). Предположим, например, что ISP-провайдер имеет блок IP-адресов 195.10.x.x из традиционного адресного пространства класса C. Этот блок состоит из 256 адресных блоков класса C, с адресами от 195.10.0.x по 195.10.255.x. Предположим, что ISP-провайдер выделяет блок адресов класса C каждому из своих клиентов. Без использования CIDR-маршрутизации провайдер ISP должен был бы выделить 256 блоков адресов класса C каждому из своих узлов BGP. С помощью маршрутизации CIDR протокол BGP может сконцентрировать сетевое адресное пространство и анонсировать только один блок — 195.10.x.x. Этот блок имеет такой же размер, как и традиционный адресный

блок класса B. Благодаря использованию CIDR-маршрутизации разграничение классов становится ненужным, что приводит к значительному сокращению размера таблиц маршрутизации протокола BGP.

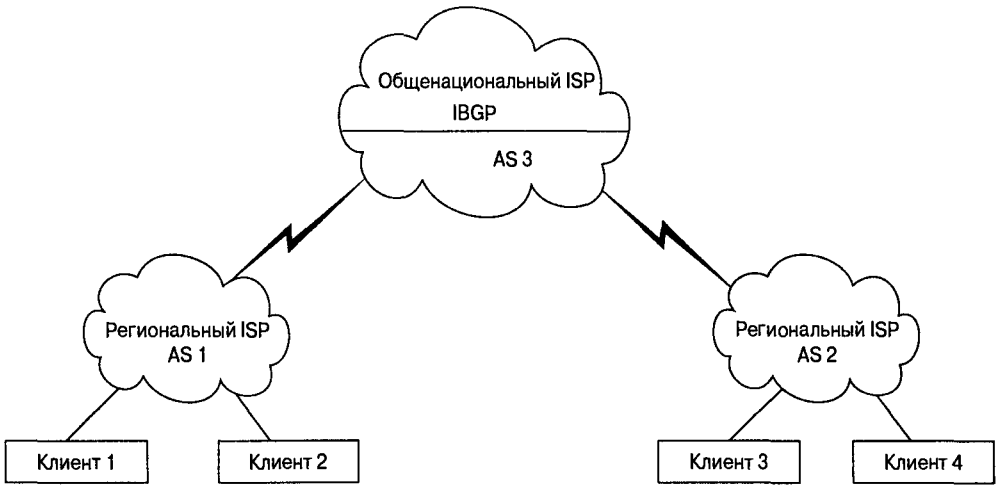


Рис. 41.1. Внешний и внутренний протоколы BGP

Соседние устройства протокола BGP обмениваются полной информацией о маршрутах при первом же установлении TCP-соединения между ними. Если в таблице маршрутизации обнаруживаются изменения, то BGP-маршрутизаторы пересылают своим соседям только те маршруты, которые претерпели изменения. Маршрутизаторы BGP не осуществляют периодической рассылки сообщений об изменениях маршрутов, а сообщают только оптимальный маршрут к сети-получателю.

Атрибуты протокола BGP

Маршруты, полученные с использованием протокола BGP, обладают некоторыми свойствами, которые используются для определения наилучшего маршрута в тех случаях, когда имеется несколько маршрутов к пункту назначения. Эти свойства называются атрибутами протокола BGP, и понимание их влияния на выбор маршрута необходимо для разработки устойчивой сети. В данном разделе описываются следующие атрибуты, которые BGP использует при выборе маршрута:

- Weight;
- Local preference;
- Multi-exit discriminator;
- Origin;
- AS_path;
- Next-hop;
- Community.

Атрибут Weight

Атрибут *Weight (вес)* представляет собой атрибут, введенный корпорацией Cisco и является локальным для конкретного маршрутизатора. Он не анонсируется соседним маршрутизаторам. Если маршрутизатор обнаруживает несколько маршрутов к пункту назначения, то выбирается маршрут с наибольшим весом. На рис. 41.2 маршрутизатор A получает от маршрутизаторов B и C извещение о маршруте к сети 172.16.1.0. Когда маршрутизатор A получает извещение от маршрутизатора B, соответствующему маршруту присваивается вес, равный 50. Когда маршрутизатор A получает извещение от маршрутизатора C, этому маршруту присваивается вес, равный 100. Оба пути для сети 172.16.1.10 будут храниться в таблице маршрутизации протокола BGP вместе со своими весами. В таблицу IP-маршрутизации будет помещен маршрут с наибольшим весом.

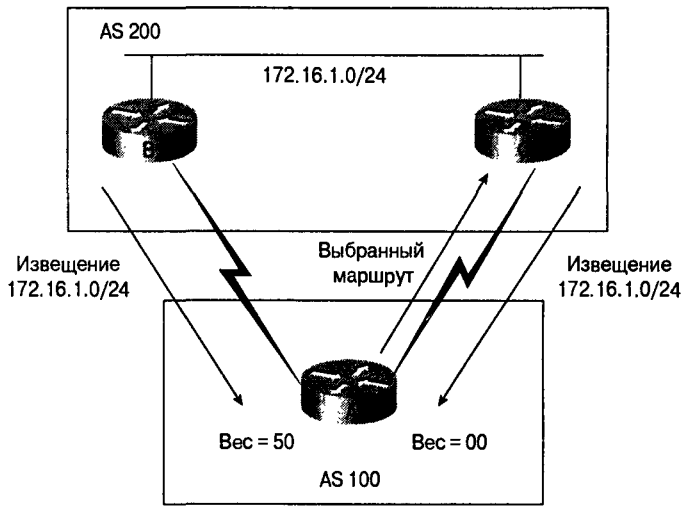


Рис. 41.2. Атрибут Weight

Атрибут Local Preference

Атрибут *Local Preference* используется для выбора точки выхода из локальной автономной системы (autonomous system — AS). В отличие от атрибута Weight, атрибут Local Preference анонсируется во всей локальной автономной системе AS. Если у системы AS есть несколько точек выхода, то этот атрибут используется при выборе точки выхода для определенного маршрута. На рис. 41.3 автономная система AS 100 получает от системы AS 200 два извещения о маршруте к сети 172.16.1.0. Когда маршрутизатор A получает извещение от сети 172.16.1.0, соответствующему атрибуту Local Preference присваивается значение 50. Когда маршрутизатор B получает извещение от сети 172.16.1.0, соответствующему атрибуту Local Preference присваивается значение 100. Маршрутизаторы A и B обмениваются этими значениями. Маршрутизатор B имеет большее значение атрибута, чем маршрутизатор A, поэтому он будет использован в качестве точки выхода из системы AS 100 для достижения сети 172.16.1.0 в системе AS 200.

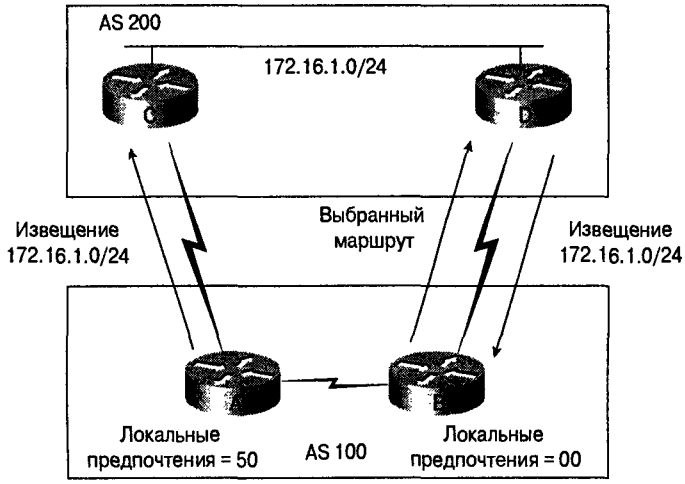


Рис. 41.3. Атрибут Local Preference

Атрибут Multi-exit Discriminator

Атрибут *Multi-Exit Discriminator* (MED), также называемый *атрибутом метрики (metric attribute),* используется как предложение внешней автоглмной системе AS выбрать маршрут к AS, которая анонсирует данную метрику.

Термин *"предложение"* применяется потому, что внешняя AS, которая получает атрибут MED, может использовать для выбора маршрута другие атрибуты протокола BGP. Правила выбора маршрута будут рассматрены в следующем разделе. На рис. 41.4 маршрутизатор C анонсирует маршрут 172.16.1.0 с метрикой 10, а маршрутизатор D анонсирует маршрут 172.16.1.0 с метрикой 5. Меньшая метрика предпочтительнее, поэтому система AS 100 выберет маршрут к сети 172.16.1.0 в системе AS 200 через маршрутизатор D. Атрибуты MED распространяются по локальной автономной системе.

Атрибут Origin

Атрибут *Origin* указывает, каким способом протокол BGP узнает о конкретном маршруте. Этот атрибут может принимать одно из следующих трех значений.

- **IGP.** Маршрут является внутренним по отношению к исходной автономной системе AS. Это значение устанавливается в тех случаях, когда для внедрения маршрута в протокол BGP используется команда конфигурирования сетевого маршрутизатора.
- **EGP.** О маршруте сообщается по протоколу внешнего граничного шлюза (Exterior Border Gateway Protocol — EBGP).
- **Incomplete (неполный).** Источник маршрута неизвестен или о нем сообщается каким-либо иным способом. Атрибут принимает это значение, когда маршрут перераспределяется в протокол BGP.

Использование атрибута *Origin* для выбора маршрута будет рассмотрено в следующем разделе.

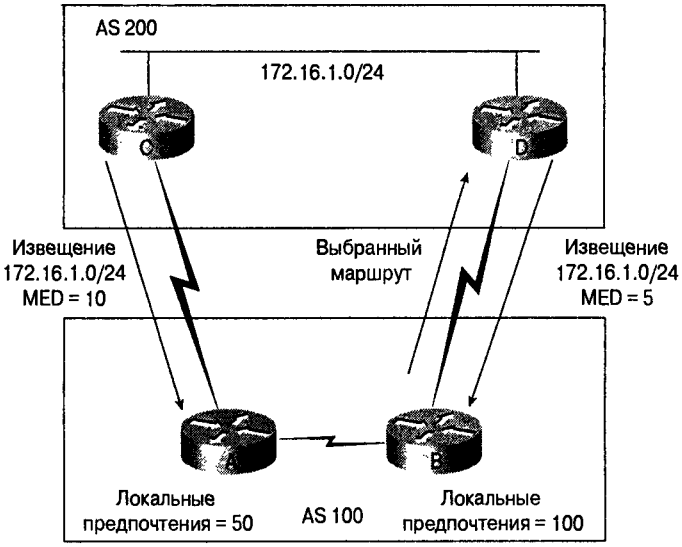


Рис. 41.4. Атрибут MED протокола BGP

Атрибут AS_path

Когда объявление маршрута проходит через автономную систему, ее номер заносится в упорядоченный список номеров автономных систем AS, пройденных этим маршрутным объявлением. На рис. 41.5 показана ситуация, когда маршрут проходит через три автономные системы.

Автономная система AS 1 создает маршрут к 170.16.1.0 и оповещает об этом системы AS 2 и AS 3 с атрибутом AS_path, равным {1}. Система AS 3 оповещает систему AS 1 в обратном направлении с атрибутом AS_path {3,1}, а AS 2 оповещает систему AS 1 в обратном направлении с атрибутом AS_path равным {2,1}. Когда система AS 1 обнаруживает в объявлении маршрута собственный номер, она отбрасывает эти маршруты. Этот механизм используется протоколом BGP для обнаружения маршрутных петель. Системы AS 2 и AS 3 передают друг другу маршрут со своими номерами, добавленными к атрибуту AS_path. Эти маршруты не будут занесены в таблицу IP-маршрутизации, поскольку системы AS 2 и AS 3 узнают о маршруте к 172.16.1.0 от AS 1 с более коротким списком AS_path.

Атрибут Next-Hop

Атрибут протокола EBGP *Next-Hop (узел следующего перехода)* представляет собой IP-адрес, который используется для достижения анонсирующего маршрут маршрутизатора. Для одноранговых устройств протокола EBGP адресом узла следующего перехода является IP-адрес соединения между одноранговыми узлами. В протоколе IBGP адрес узла следующего перехода протокола EBGP передается в локальную автономную систему AS, как показано на рис. 41.6.

Маршрутизатор C анонсирует сеть 172.16.1.0с адресом узла следующего перехода равным 10.1.1.1. Когда маршрутизатор A распространяет информацию об этом маршруте внутри своей автономной системы AS, информация об узле следующего перехода

протокола EBGP сохраняется. Если маршрутизатор B не имеет маршрутной информации об узле следующего перехода, то данный маршрут будет отброшен. Поэтому важно, чтобы в автономной системе AS функционировал протокол IGP для распространения маршрутной информации о следующем узле.

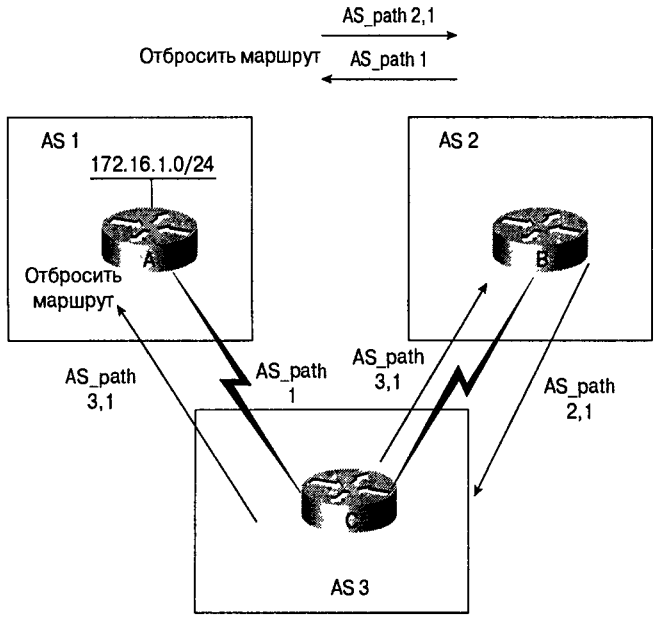


Рис. 41.5. Атрибут AS_path

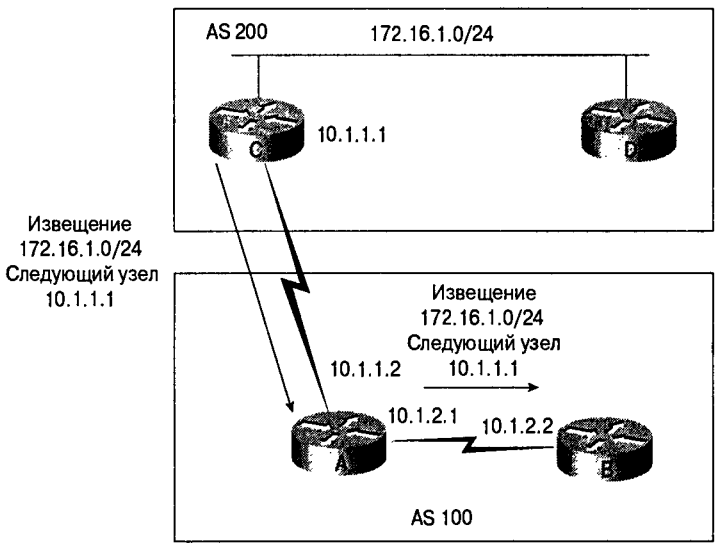


Рис. 41.6. Атрибут Next-Hop

Атрибут Community

Этот атрибут обеспечивает способ групповой адресации получателей, называемых сообществом (community), к которому могут относиться решения о выборе маршрута (такие, как принятие, предпочтение и перераспределение). Для установки данного атрибута используются преобразования маршрутов. Ниже перечислены стандартные значения атрибута Community.

- **no-export** (не экспортируется). Такой маршрут не анонсируется одноранговым узлам протокола EBGP.
- **no-advertise** (не анонсируется). Этот маршрут не анонсируется никаким одноранговым узлам.
- **Internet.** Об этом маршруте оповещается сообщество Internet; к этому сообществу принадлежат все маршрутизаторы сети.

На рис. 41.7 показано сообщество маршрутизаторов, имеющих значение атрибута Community равное **no-export**. Автономная система AS 1 анонсирует сеть 172.16.1.0 системе AS 2 о с атрибутом Community, имеющим значение no-export. Автономная система AS 2 распространит этот маршрут среди всех своих маршрутизаторов, однако не отправит его в AS 3 или любую другую внешнюю систему.

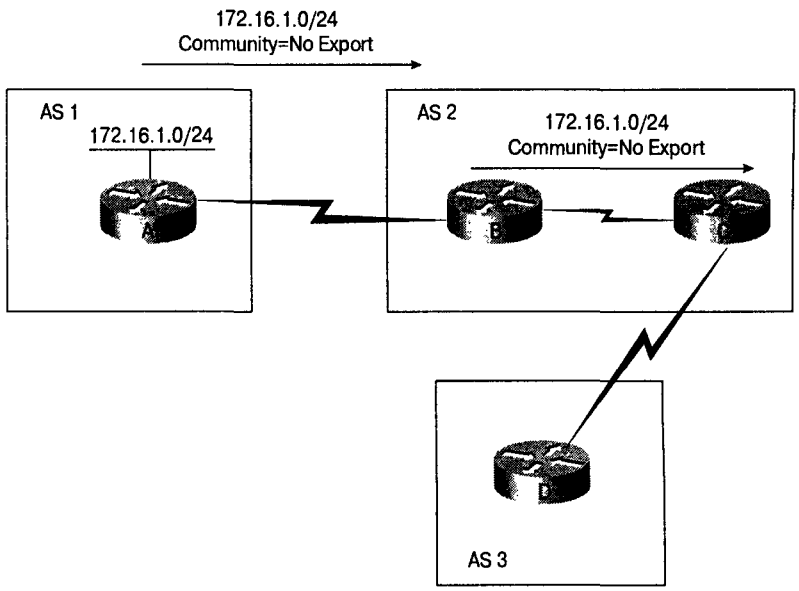


Рис. 41.7. Атрибут протокола BGP Community со значением no-export

На рис. 41.8 показано, как AS 1 анонсирует маршрут к 172.16.1.0 системе AS 2 с атрибутом Community, имеющим значение no-advertise. Маршрутизатор B в системе AS 2 не будет оповещать другие маршрутизаторы об этом маршруте.

На рис. 41.9 показан атрибут Community со значением Internet. Ограничения на область распространения оповещений о маршруте от системы AS 1 в данном случае отсутствуют.

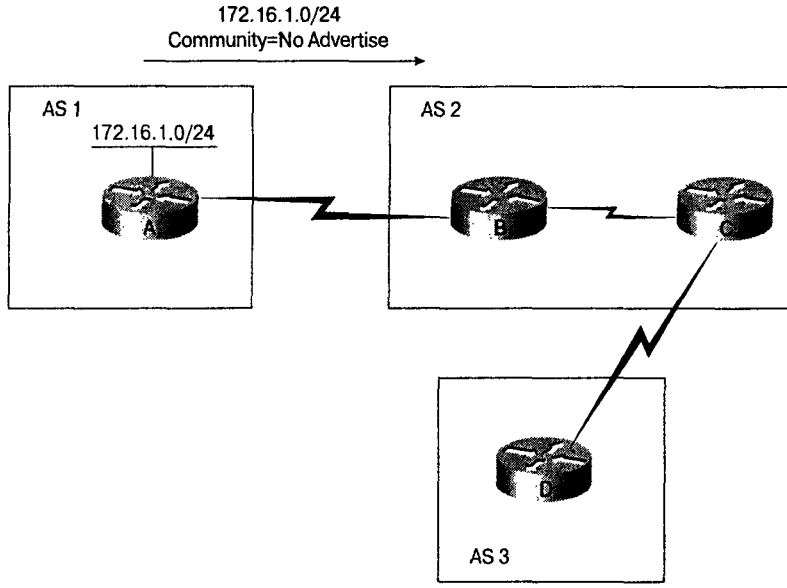


Рис. 41.8. Атрибут Community со значением no-advertise

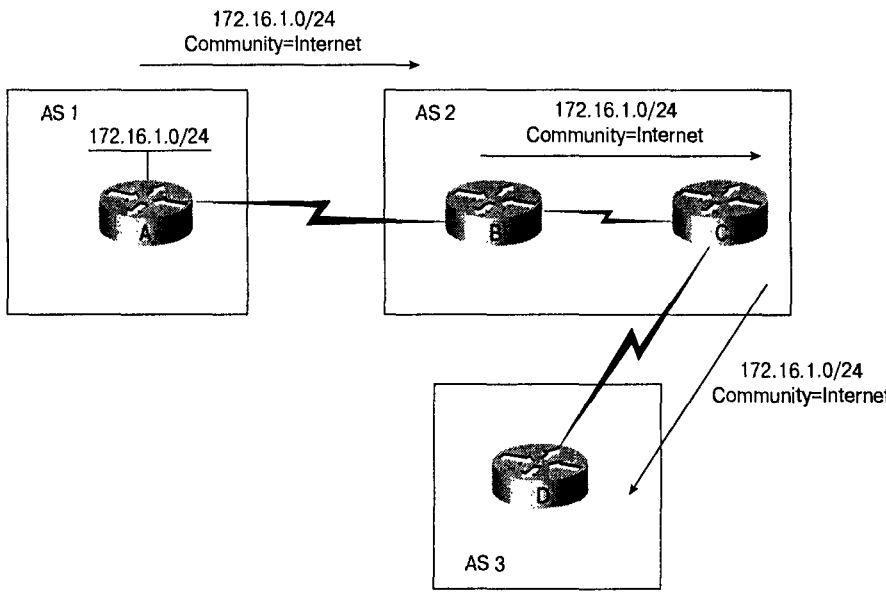


Рис. 41.9. Атрибут Community со значением Internet

Выбор маршрута по протоколу BGP

Протокол BGP может получить извещения об одном и том же маршруте из нескольких источников, однако выбирает только один, наилучший. BGP помещает выбранный маршрут в таблицу IP-маршрутизации и распространяет его среди своих

соседних маршрутизаторов. Для выбора маршрута к получателю протокол BGP использует приведенные ниже критерии в указанном порядке.

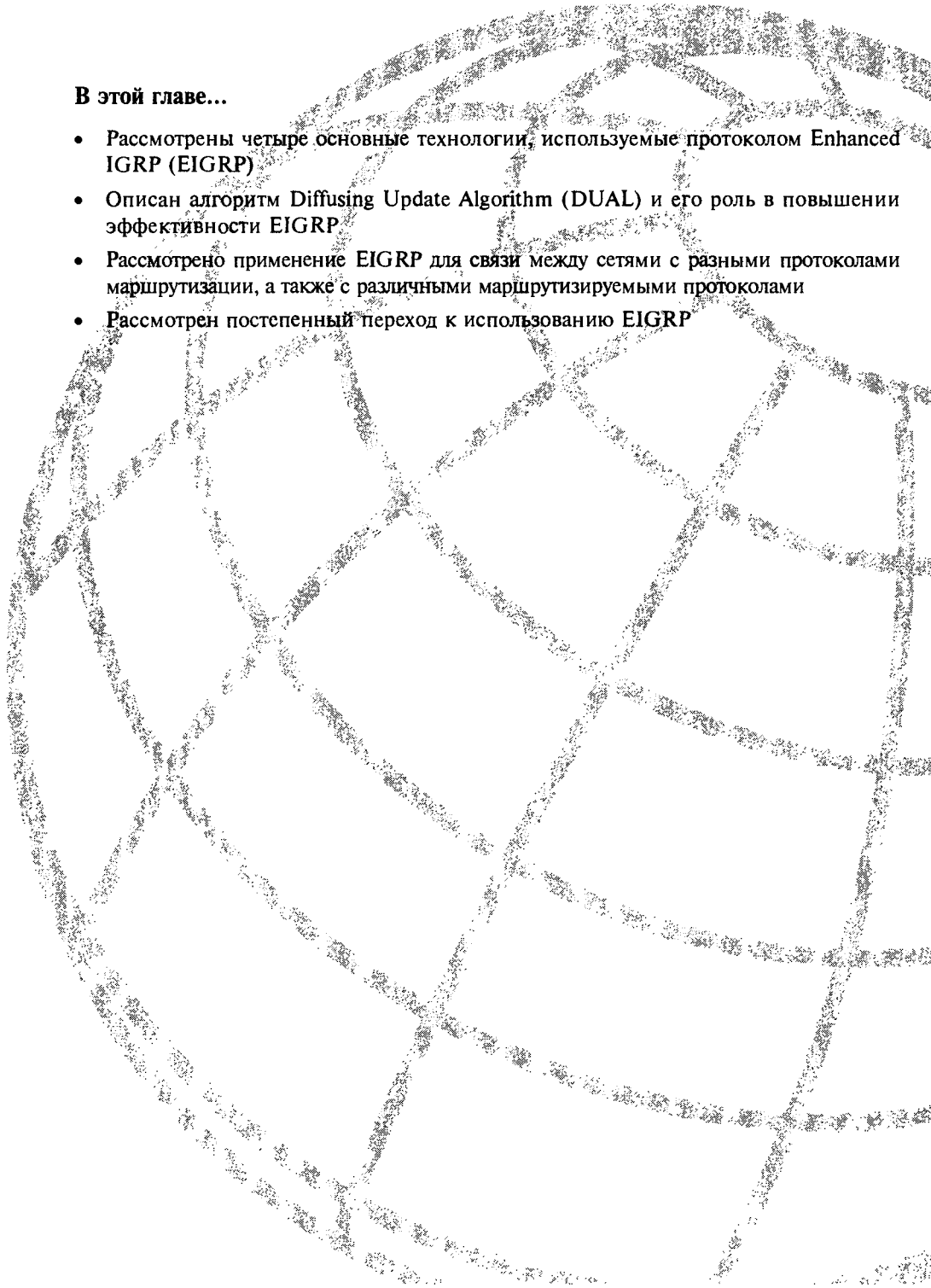
- Если узел следующего перехода недоступен, то сообщение об обновлении маршрута отбрасывается;
- Предпочтение отдается маршруту с наибольшим весом.
- Если веса одинаковы, то предпочтение отдается пути с наибольшим значением атрибута Local Preference.
- Если значения атрибутов Local Preference одинаковы, то предпочтение отдается пути, который был инициирован процессом протокола BGP, выполняющимся на этом маршрутизаторе.
- Если ни один маршрут не был инициирован протоколом BGP, выполняющимся на данном маршрутизаторе, то предпочтение отдается маршруту с самым коротким атрибутом AS_path.
- Если все маршруты имеют одинаковую длину атрибута AS_path, то предпочтение отдается маршруту с самым низким значением типа источника (считается, что IGP более низкий по сравнению с EGP, который, в свою очередь, ниже, чем неполный источник).
- При одинаковых типах источника предпочтение отдается маршруту с наименьшим значением атрибута MED.
- При равных значениях атрибута MED предпочтение отдается внешнему маршруту (по сравнению с внутренним).
- Если и эти характеристики совпадают, то предпочтение отдается маршруту через ближайшее соседнее IGP-устройство.
- Предпочтительным является маршрут с наименьшим IP-адресом, который определяется идентификатором (ID) BGP-маршрутизатора.

Контрольные вопросы

1. Может ли протокол IBGP использоваться вместо протокола IGP (RIP, IGRP, EIGRP, OSRF или ISIS)?
2. Предположим, что маршрутизатор BGP узнает об одинаковых маршрутах от двух разных узлов EBGP. Значение атрибута AS_path от узла 1 равно {2345,86,51}, а от узла 2 — {2346,51}. Какие атрибуты BGP могли бы быть скорректированы, чтобы принудить маршрутизатор предпочесть маршрут, о котором сообщил узел 1?
3. Справедливо ли утверждение, что протокол BGP может использоваться только провайдерами службы Internet?
4. Если непосредственно подключенный интерфейс перераспределяется в протокол BGP, то каково будет значение атрибута Origin для этого маршрута?

Дополнительные источники

- RFC 1771, "BGP4".
- Хелеби С., Мак-Ферсон Д. *Принципы маршрутизации в Internet*, 2-е издание. ИД "Вильямс", 2001.
- Baasam H. *Internet Routing Architectures.* Cisco Press: Indianapolis, 1997.
- Parkhurst W., Jackson D.R. *Practical BGP for Internet Routing.* Cisco Press: Indianapolis.
- BGP4 Case Studies/Tutorial Section 1, http://www.cisco.com/warp/customer/459/13.html
- BGP4 Case Studies/Tutorial Section 2, http://www.cisco.com/warp/customer/459/14.html
- BGP4 Case Studies/Tutorial Section 3, http://www.cisco.com/warp/customer/459/15.html
- BGP4 Case Studies/Tutorial Section 4, http://www.cisco.com/warp/customer/459/16.html
- BGP4 Case Studies/Tutorial Section 5, http://www.cisco.com/warp/customer/459/17.html



В этой главе...

- Рассмотрены четыре основные технологии, используемые протоколом Enhanced IGRP (EIGRP)
- Описан алгоритм Diffusing Update Algorithm (DUAL) и его роль в повышении эффективности EIGRP
- Рассмотрено применение EIGRP для связи между сетями с разными протоколами маршрутизации, а также с различными маршрутизируемыми протоколами
- Рассмотрен постепенный переход к использованию EIGRP

Глава 42

Протокол EIGRP

Усовершенствованный протокол маршрутизации внутреннего шлюза (Enhanced Internal Gateway Routing Protocol — EIGRP), представляет собой результат эволюции его предшественника, протокола IGRP (описанного в главе 44, "Протокол IGRP"). Эта эволюция стала результатом изменений в организации сетей и потребности в обмене данными между крупными сетями различной архитектуры. В протоколе EIGRP сочетаются возможности протоколов маршрутизации по состоянию канала и дистанционно-векторных протоколов. Кроме того, в состав EIGPR входят несколько важных протоколов, которые значительно увеличивают его эффективность по сравнению с другими протоколами маршрутизации. Одним из таких протоколов является диффузионный алгоритм обновления (Diffusing Update Algorithm — DUAL), разработанный доктором Дж. Дж. Гарсиа-Луна-Асивесом (J.J. Garcia-Luna-Aceves) в компании SRI International. Алгоритм DUAL позволяет маршрутизаторам EIGRP определять, является ли маршрут, сообщенный соседним узлом, петлей, и дает возможность маршрутизатору, на котором функционирует протокол EIGRP, находить альтернативные маршруты, не дожидаясь обновленной информации от других маршрутизаторов.

Усовершенствованный протокол EIGRP обеспечивает совместимость и гармоничное взаимодействие с маршрутизаторами IGRP. Механизм автоматического перераспределения позволяет импортировать маршруты IGRP в Enhanced IGRP и наоборот, что делает возможным постепенное внедрение протокола Enhanced IGRP в сети IGRP. Поскольку метрики обоих протоколов однозначно преобразуются друг в друга, они легко сопоставляются, как если бы маршруты были порождены в их собственных автономных системах. Enhanced IGRP интерпретирует маршруты IGRP как внешние и допускает их настройку сетевым администратором.

В настоящей главе описываются основные операции и характеристики протокола Enhanced IGRP.

Возможности и атрибуты протокола Enhanced IGRP

Основными свойствами, отличающими Enhanced IGRP от других протоколов маршрутизации, являются быстрая сходимость, поддержка маски подсети переменной длины, частичных обновлений и нескольких протоколов сетевого уровня.

Маршрутизатор, на котором выполняется протокол Enhanced IGRP, хранит все маршрутные таблицы соседних маршрутизаторов, что позволяет ему быстро адаптироваться к альтернативным маршрутам. Если подходящего маршрута нет, то Enhanced IGRP запрашивает альтернативный маршрут у соседних маршрутизаторов. Эти запросы передаются до тех пор, пока альтернативный маршрут не будет найден.

Протокол EIGRP поддерживает маски подсетей переменной длины, что позволяет автоматически обобщать маршруты в пределах сети с определенным номером. Кроме того, EIGRP можно настроить на обобщение маршрутов в любых битовых границах на любом интерфейсе.

Enhanced IGRP не выполняет периодических обновлений. Вместо этого он посылает обновленную информацию частями и только в случае изменения метрики маршрута. Распространение частично обновленной информации автоматически ограничивается таким образом, что ее получают только те маршрутизаторы, которым это необходимо. Благодаря этим двум свойствам протоколу Enhanced IGRP требуется значительно меньшая полоса пропускания, чем протоколу IGRP.

Enhanced IGRP поддерживает протоколы AppleTalk, IP и Novell NetWare. Реализация IGRP для AppleTalk перераспределяет маршруты, о которых известил протокол поддержки таблицы маршрутизации (Routing Table Maintenance Protocol — RTMP). Реализация для IP перераспределяет маршруты, о которых оповещают протоколы OSRF, RIP (Routing Information Protocol), IS-IS (Intermediate System-to-Intermediate System), EGP (Exterior Gateway Protocol) или BGP (Border Gateway Protocol). Реализация для Novell перераспределяет маршруты, о которых оповещает протокол RIP Novell или SAP (Service Advertisement Protocol — SAP).

Основные процессы и технологии

Для повышения эффективности в протоколе Enhanced IGRP используются четыре основные технологии, отличающие его от других технологий маршрутизации: обнаружение/восстановление соседних маршрутизаторов, транспортный протокол с достоверной передачей (reliable transport protocol, RTP), машина с конечным числом состояний алгоритма DUAL и модули, зависимые от протокола.

Механизм *обнаружения и восстановления соседних узлов* позволяет маршрутизаторам динамически обнаруживать другие маршрутизаторы в своей сети. Кроме того, маршрутизаторы должны определять состояние соседних маршрутизаторов в случаях, когда те становятся недоступными или неработоспособными. Этот процесс реализуется с небольшими затратами ресурсов с помощью периодической посылки небольших пакетов приветствия (hello packets). Пока маршрутизатор получает пакеты приветствия от соседнего маршрутизатора, он считает, что соседний маршрутизатор работоспособен и что они могут обмениваться между собой маршрутной информацией.

Транспортный протокол с достоверной передачей (Reliable Transport Protocol — RTP) обеспечивает гарантированную, упорядоченную доставку пакетов протокола EIGRP всем соседним маршрутизаторам. Он поддерживает смешанную передачу много- и одноадресатных пакетов. Для большей эффективности EIGRP с гарантией доставки передаются только некоторые пакеты. В сетях с множественным доступом и возможностями многоадресатной передачи, таких как Ethernet, нет необходимости посылать пакеты приветствия каждому соседнему маршрутизатору отдельно. Протокол EIGRP отправляет нескольким абонентам один пакет приветствия, ко-

торый содержит указатель, информирующий получателей о том, что пакет не нуждается в подтверждении. В пакетах других типов, таких как пакеты обновления, указывается, что подтверждение необходимо. В пользователе RTP есть средства более быстрой пересылки многоадресатных пакетов, в то время как отправка пакетов, не требующих подтверждения, задерживается. Это позволяет гарантировать быструю сходимость для скоростных соединений.

Машина с конечным числом состояний алгоритма DUAL реализует процесс принятия решений для всех маршрутных вычислений, анализируя и обобщая оповещения о маршрутах, поступающие от всех соседних маршрутизаторов. Для выбора эффективных маршрутов без петель DUAL использует информацию о расстоянии и отбирает маршруты для занесения в маршрутные таблицы, основываясь на допустимых маршрутизаторах. *Допустимым маршрутизатором* считается соседний маршрутизатор, используемый для пересылки пакетов к получателю с наименьшими затратами и гарантирующий отсутствие маршрутных петель. Если у соседнего маршрутизатора изменяется метрика или топология сети, то DUAL ищет в сети допустимые маршрутизаторы. Если будет найден хотя бы один, то DUAL использует его во избежание повторного вычисления маршрута. При отсутствии допустимых маршрутизаторов и повторных извещений о получателе от соседних маршрутизаторов повторное вычисление маршрута (называемое диффузным вычислением) все же выполняется, так как необходимо определить новый допустимый маршрутизатор. Хотя повторные вычисления не вызывают повышенной нагрузки процессора, они влияют на скорость сходимости, поэтому лучше их избегать.

Зависимые от протокола модули отвечают требованиям протокола сетевого уровня. Например, модуль IP-Enhanced IGRP отвечает за передачу и получение пакетов Enhanced IGRP, инкапсулированных в IP. IP-Enhanced IGRP отвечает также за анализ пакетов Enhanced IGRP и оповещение DUAL о новой полученной информации. IP-Enhanced IGRP запрашивает DUAL о выборе маршрута, который сохраняется в маршрутной таблице IP. IP-IGRP также отвечает за перераспределение маршрутов, о которых сообщили другие IP-протоколы.

Концепции маршрутизации

Протокол EIGRP опирается на четыре основные концепции: таблицы соседних маршрутизаторов, топологические таблицы, состояния маршрутов и маркировка маршрутов. Каждая из этих концепций рассматривается ниже.

Таблицы соседних маршрутизаторов

Когда маршрутизатор обнаруживает новый соседний маршрутизатор, он создает запись в таблице соседних маршрутизаторов и записывает в нее его адрес и интерфейс. Для каждого модуля, зависящего от протокола, существует по одной такой таблице. Соседний маршрутизатор посылает пакет приветствия, оповещающий о времени занятости, то есть о времени, в течение которого он считается доступным и работоспособным. Если пакет приветствия не получен в течение времени занятости, то DUAL оповещается об изменении топологии.

Кроме того, в таблице соседних маршрутизаторов содержится информация для протокола RTP. Для согласования пакетов данных и подтверждения их получения используются номера последовательностей. Последний порядковый номер, полученный

от соседнего маршрутизатора, фиксируется, что позволяет выявлять пакеты, выпавшие из последовательности. Для пересылки на соседний маршрутизатор используется очередь на основе списка передаваемых пакетов. Для оценки оптимального интервала повторной передачи используются записи в таблицах соседних маршрутизаторов, где хранятся значения таймеров передачи пакетов в прямом и обратном направлении.

Топологические таблицы

В *топологических таблицах* содержатся все адреса получателей, о которых оповещают соседние маршрутизаторы. Модули, зависящие от протокола, заполняют эти таблицы, которые обрабатываются машиной с конечным числом состояний DUAL. Каждая запись топологической таблицы содержит адрес получателя и список соседних маршрутизаторов, которые должны оповещать об этих адресах. Для каждого соседнего маршрутизатора существуют записи определенной метрики, которые хранятся соседними маршрутизаторами в их маршрутных таблицах. Протоколам маршрутизации по вектору расстояния необходимо придерживаться следующего правила: если соседний маршрутизатор сообщает о том, что получатель достигнут, то они должны использовать этот маршрут для передачи пакетов.

Метрика, используемая маршрутизатором для обращения к получателю, ассоциируется с получателем. Метрика, которую использует маршрутизатор в маршрутных таблицах и о которой он оповещает другие маршрутизаторы, является суммой наилучших метрик и канальных затрат лучшего из соседних маршрутизаторов.

Состояния маршрутов

Записи топологических таблиц, касающиеся получателей, существуют в двух состояниях: активном и пассивном. Получатель находится в *пассивном состоянии*, когда маршрутизатор не выполняет вычисления маршрута, и в *активном*, если такие вычисления выполняются. Если допустимые маршрутизаторы всегда доступны, то получатель никогда не перейдет в активное состояние, таким образом избегая повторных вычислений.

Повторные вычисления выполняются в том случае, когда получатель не имеет допустимых маршрутизаторов. Маршрутизатор инициирует повторные вычисления, посылая информационный пакет с запросом к каждому соседнему маршрутизатору. В свою очередь, соседний маршрутизатор может отправить ответный пакет, показывающий, что для получателя имеется допустимый маршрутизатор, или подтвердить, что он участвует в процессе повторных вычислений. Пока получатель находится в активном состоянии, маршрутизатор не может изменить информацию в маршрутной таблице. После того как маршрутизатор получит ответ от всех соседних маршрутизаторов, записи в топологической таблице для получателей вернутся в пассивное состояние и маршрутизатор может выбрать допустимый маршрутизатор для получателя.

Маркировка маршрута

Протокол EIGRP поддерживает внутренние и внешние маршруты. Внутренние маршруты порождаются автономной системой с Enhanced IGRP. Таким образом, непосредственно подключенная сеть, настроенная на использование EIGRP, рассчитана на внут-

реннюю маршрутизацию и распространяет эту информацию по автономным системам через протокол EIGRP. Информация о внешних маршрутах распространяется другим протоколом маршрутизации или хранится в маршрутной таблице как статические маршруты. Эти маршруты маркируются индивидуально в соответствии с источником.

Внешние маршруты маркируются следующей информацией:

- идентификатор (ID) маршрутизатора с протоколом Enhanced IGRP, который распространяет маршрут;
- номер AS-получателя;
- конфигурируемый маркер администратора;
- ID внешнего протокола;
- метрика внешнего протокола;
- битовые флаги стандартной маршрутизации.

Маркировка маршрута обеспечивает сетевому администратору настраиваемый процесс маршрутизации и гибкую стратегию управления. Маркировка маршрутов особенно полезна для транзитных AS, где Enhanced IGRP взаимодействует с междоменными протоколами маршрутизации, которые применяют более глобальные стратегии, реализующие масштабируемую, основанную на стратегии маршрутизацию.

Типы пакетов протокола Enhanced IGRP

В протоколе Enhanced IGRP используются следующие типы пакетов: приветствия, подтверждения, обновления, запросы и ответы.

Пакеты приветствия (hello packets) являются многоадресатными и предназначены для обнаружения и восстановления связи с соседними узлами. Эти пакеты не требуют подтверждения.

Пакеты подтверждения представляют собой пакеты приветствия, которые не содержат данных. Эти пакеты содержат ненулевые номера подтверждения и всегда являются одноадресатными.

Пакеты обновления используются для обеспечения достижимости получателя. Когда обнаруживается новый соседний маршрутизатор, ему отсылаются пакеты обновления для того, чтобы он смог построить свою топологическую таблицу. В других случаях, таких как изменение затрат на соединение, обновления являются многоадресатными. Пакеты обновления используют передачу с подтверждением.

Пакеты запросов и ответов отправляются, когда получатель не имеет допустимых маршрутизаторов. *Пакеты запросов* всегда являются многоадресатными. Пакеты ответов посылаются в ответ на пакеты запросов для того, чтобы сообщить источнику об отсутствии необходимости повторно вычислять маршрут, поскольку допустимый маршрутизатор существует. *Пакеты ответов* являются одноадресатными и предназначены только для источника запроса. Пакеты запросов и ответов используют передачу с подтверждением.

Резюме

Протокол EIGRP производства Cisco Systems является многофункциональным и устойчивым протоколом, вероятно, лучшим из всех, которые когда-либо разрабатыва-

лись. В нем уникально сочетаются лучшие свойства дистанционно-векторных протоколов маршрутизации и протоколов состояния канала. В результате получился гибридный протокол маршрутизации, который не поддается обычной классификации, применимой для традиционных протоколов.

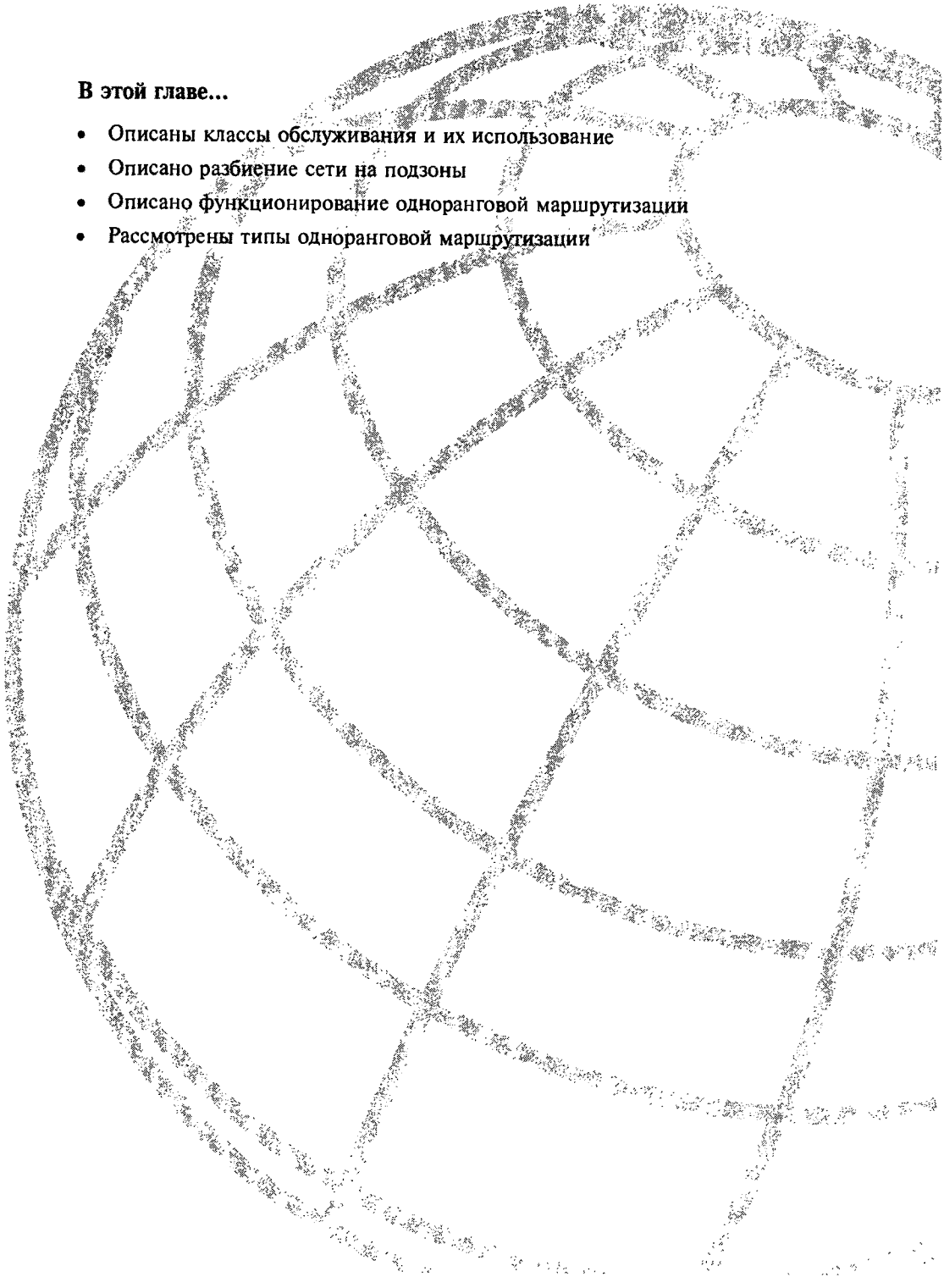
Протокол EIGRP удобно настраивать и использовать, он эффективен и безопасен; может быть использован совместно с IPv4, AppleTalk и IPX. Еще более важным является то, что его модульная архитектура легко позволит Cisco обеспечить поддержку других протоколов маршрутизации, которые могут быть разработаны в будущем.

Контрольные вопросы

1. Назовите четыре основные технологии, используемые протоколом EIGRP.
2. Почему EIGRP эффективнее, чем IGRP?
3. Каким образом RTP улучшает сходимость?
4. Зачем EIGRP маркирует определенные маршруты?

Дополнительные источники

- Pepelnjak I. EIGRP *Network Design Solutions.* Indianapolis: Cisco Press, 2000.
- Sportack M. A. *IP Routing Fundamentals.* Indianapolis: Cisco Press, 1999.
- http://www.cisco.com/cpress/cc/td/cpress/ccie/ndcs798/nd2017.htm



В этой главе...

- Описаны классы обслуживания и их использование
- Описано разбиение сети на подзоны
- Описано функционирование одноранговой маршрутизации
- Рассмотрены типы одноранговой маршрутизации

Глава 43

Маршрутизация в системной сетевой архитектуре IBM

Введение

В процессе перехода вычислительной техники от преобладания централизованных компьютерных решений к использованию одноранговых вычислительных устройств сетевая архитектура IBM претерпела значительные изменения. В настоящее время маршрутизация системной архитектуры IBM (Systems Network Architecture — SNA) может происходить в двух различных средах, хотя ряд ключевых концепций остается единым для всех типов маршрутизации SNA. В этой главе описываются функции и службы, которые делают возможными как подзональную маршрутизацию SNA, так и усовершенствованную маршрутизацию одноранговой сети (Advanced Peer-to-Peer Networking — APPN). В ней рассматриваются такие вопросы, как сеансовые соединения, группы передачи, явные и виртуальные маршруты, а также классы обслуживания (Class of Service — CoS). Общая информация о традиционных SNA и APPN приведена в главе 39 "Протоколы сетевой архитектуры IBM". На рис. 43.1 проиллюстрированы концепции, описываемые в данной главе, в контексте традиционной среды SNA.

Сеансовые соединители SNA

Сеансовые соединители SNA используются для того, чтобы связать адресные пространства, когда сеансы пересекают несколько адресных пространств. Существует три типа сеансовых соединителей: граничные функции, межсетевые шлюзы SNA (SNA Network Interconnection — SNI) и функции промежуточной маршрутизации APPN. Граничные функции находятся в подзональных узлах и устанавливают соответствие между подзоной и пространством периферийных адресов. Шлюзы SNI действуют как мосты между сетями SNA, получая данные из одной сети и передавая ее по назначению в другую сеть. Шлюзы SNI прозрачны для конечных устройств подключения к сети (Network Attachment Units — NAU). Промежуточные узлы APPN выполняют промежуточную маршрутизацию в сетях APPN. На рис. 43.1 показано место сеансового соединителя в традиционной среде SNA.

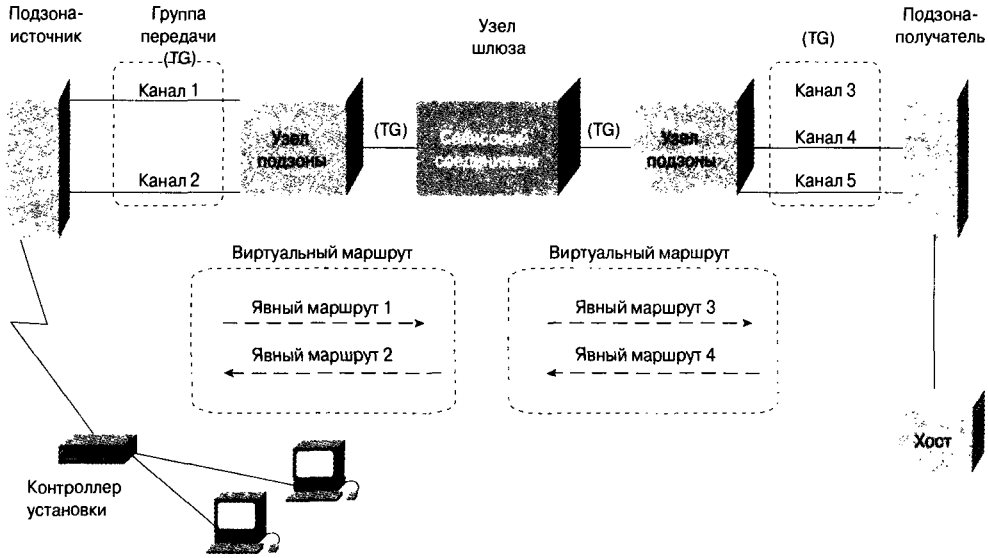


Рис. 43.1. Для связи между подзонами маршрутизация SNA базируется на группах передачи

Группы передачи SNA IBM

Группы передачи (Transmission Groups — TG) SNA IBM представляют собой логические соединения между смежными узлами SNA IBM, которые используются для прохождения сеансовых потоков данных SNA. Группы TG состоят из одного или нескольких каналов SNA с назначенными им приоритетами передачи. Многоканальные TG обеспечивают дополнительную надежность и расширенную полосу пропускания и используются для объединения нескольких физических каналов в один логический канал SNA. Многоканальные TG допускаются только между узлами T4. Для упорядочения нестандартных сообщений при каждой пересылке группам передачи присваиваются порядковые номера. В каждой группе поддерживается четыре приоритета передачи: низкий, средний, высокий и приоритет передачи данных сетевой службы (наивысший). На рис. 43.1 показаны взаимоотношения групп передачи с другими компонентами маршрутизации SNA при подзональной маршрутизации.

Явные и виртуальные маршруты SNA IBM

Маршруты между подзонами принимают одну из двух форм: явные или виртуальные. Явные маршруты представляют собой физические соединения между двумя узлами подзоны, выраженные в виде упорядоченных последовательностей подзон и связывающие между собой группы передачи. Явные маршруты являются однонаправленными, и для создания дуплексного канала необходимо два таких маршрута.

Виртуальные маршруты представляют собой двунаправленные логические соединения между двумя узлами подзоны. Виртуальный маршрут проходит по обоим одно-

направленным явным маршрутам — прямому и обратному, — принадлежащим одному физическому пути. Виртуальные маршруты не пересекают границ сети; вместо этого для связи между двумя виртуальными маршрутами используется сеансовый соединитель межсетевого соединения SNA. В состав виртуального маршрута входят параметры приоритета передачи и пошагового управления общим потоком, когда получатель с достаточным буфером предоставляет отправителю пошаговые окна. На рис. 43.1 показаны взаимоотношения между явными и виртуальными маршрутами, а также их место в подзональной маршрутизации SNA.

Класс обслуживания SNA IBM

Функция *класс обслуживания (Class of Service — CoS)* SNA IBM определяет транспортные характеристики сети для данного сеанса. В зависимости от требований пользователя, в сети SNA могут быть заданы разные классы CoS. Эти классы обеспечивают механизм определения всех маршрутов SNA и описывают приемлемые уровни обслуживания для данного сеанса. CoS также определяет ряд характеристик сеанса, в том числе время отклика, уровень безопасности и доступность. CoS может устанавливаться автоматически при входе в сеть или вручную (пользователем) при инициализации сеанса. Каждое имя CoS связано со списком виртуальных маршрутов, удовлетворяющих требованиям желаемого уровня обслуживания. Информация, относящаяся к данному сеансу, накапливается в подзоне CoS и хранится в таблицах APPN. Различия между реализацией CoS в подзоне и маршрутизацией APPN описываются в следующих разделах.

CoS при подзональной маршрутизации

При подзональной маршрутизации пользователь определяет CoS для данного соединения. Каждому виртуальному маршруту соответствуют определенные службы, и характеристики CoS связаны с соответствующими явными маршрутами. Точка управления системными службами (System Services Control Point — SSCP) использует таблицу CoS для предоставления функции управления маршрутом информации о виртуальном маршруте и приоритете передачи. Управление маршрутом, в свою очередь, выбирает виртуальный маршрут и приоритет передачи для данного сеанса. На рис. 43.2 показан формат записи таблицы CoS для подзональной маршрутизации.

Записи таблицы CoS для подзональной маршрутизации содержат имя CoS, номер виртуального маршрута (Virtual Route Number — VRN) и приоритет передачи подзоны (TRansmission PrIority — TRPI).

Имя CoS представляет собой стандартное имя, например, SEC3, удовлетворяющее соглашениям об именах.

VRN определяет отдельный маршрут между подзонами. Между двумя подзональными узлами может назначаться до восьми виртуальных маршрутов. Каждому виртуальному маршруту может присваиваться до трех приоритетов передачи, а между двумя подзонами возможно установление до 24 виртуальных маршрутов.

TRPI определяет приоритет потока сеансовой информации между логическими модулями (LU-LU) по явному маршруту. Пользователи могут присвоить каждому виртуальному маршруту одно из трех значений приоритета: 0 (самый низкий), 1 или 2 (самый высокий).

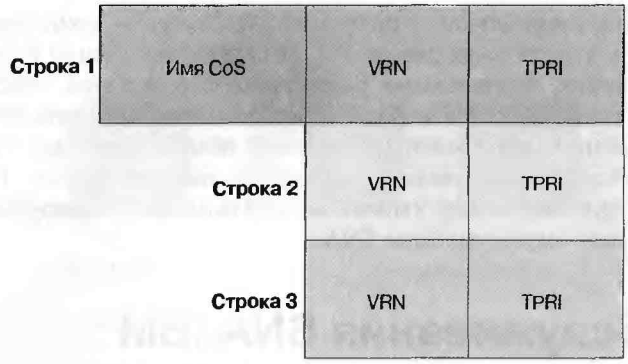


Рис. 43.2. В таблице CoS для подзональной маршрутизации хранятся виртуальные маршруты и приоритеты передачи

Механизм классов CoS при использовании маршрутизации APPN

CoS в APPN определяется явно, через параметры таблицы CoS. В APPN больше вариантов CoS, чем при подзональной маршрутизации SNA. В частности, CoS в APPN позволяет выбрать маршрут по пропускной способности, по оценке маршгрута, уровню безопасности, задержке распространения, а также по характеристикам, определенным пользователем. Класс обслуживания не ограничивается только коммуникационными контроллерами, как при подзональной маршрутизации SNA, а распространяется вплоть до конечных узлов (End Nodes — EN). В базе данных топологии CoS APPN каждому CoS соответствует древовидная структура, где отслеживаются все затраты и маршруты. CoS APPN также предусматривает параметры управления памятью, выделяемой для таких древовидных структур CoS. На рис. 43.3 показан формат записи таблицы CoS для маршрутизации APPN.

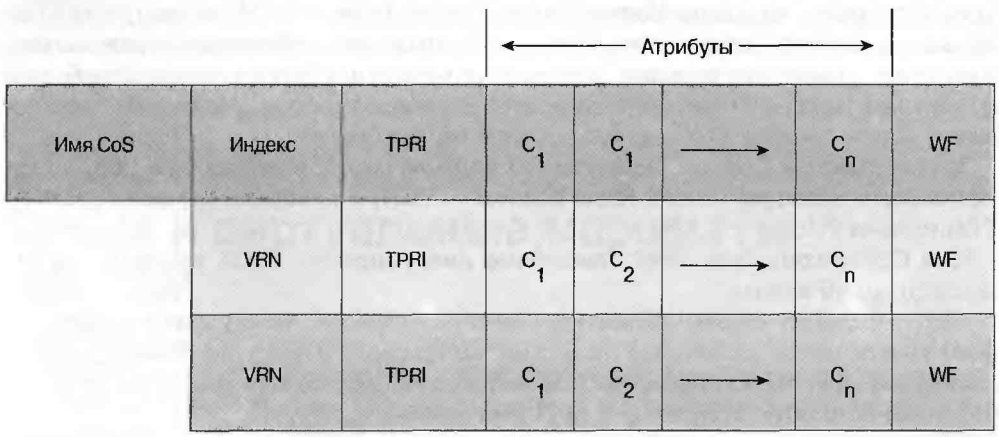


Рис. 43.3. В таблице CoS для маршрутизации APPN могут храниться специальные параметры возврата и информация о качестве маршрута

Записи таблицы CoS для маршрутизации APPN содержат имя CoS, индекс, характеристики приоритета передачи (TRPI) APPN и поле веса (Weighted Field — WF) CoS APPN.

Имя CoS представляет собой стандартное имя, например, SEC3, удовлетворяющее соглашениям об именах.

Данные в поле индекса позволяют сохранять в таблице и извлекать из нее веса маршрутных компонентов. Эта запись ссылается на запись в массиве весов CoS.

TRPI APPN определяет приоритет сеансового потока данных LU-LU по явному маршруту. Для каждой записи таблицы CoS определено только одно значение поля TRPI. TRPI APPN требует, чтобы поток конкретного сеанса с определенным CoS в данной сети APPN имел один и тот же приоритет передачи.

Характеристики узла и группы передачи представляют собой список определяемых пользователем характеристик, допустимых для данного CoS. В каждой строке определен набор характеристик узла или TG. Ими могут быть уровень безопасности, затраты на время соединения и доступная полоса пропускания. Поле характеристик содержит диапазон допустимых значений.

Поле WF CoS APPN позволяет службе выбора маршрута (Routes-Selection Service — RSS) назначать вес данному допустимому маршрутному компоненту (узлу или TG). RSS использует WF для определения относительной желательности маршрутного компонента. WF может содержать постоянную величину или имя функции, используемой RSS для определения веса.

Подзональная маршрутизация SNA IBM

Центральными компонентами традиционной маршрутизации в среде SNA являются логические области SNA и адресация узлов. В этом разделе они рассматриваются в контексте традиционной сети SNA.

Сети SNA делятся на логические области: подзоны и домены. Подзоны состоят из узла подзоны и его периферийных устройств. Домены состоят из точки управления системными службами (SSCP) и сетевых ресурсов, которыми она управляет. SSCP разных доменов могут взаимодействовать друг с другом с целью компенсации сбоев процессора узла. На рис. 43.4 показаны взаимоотношения между подзонами и доменами в контексте подзональной маршрутизации SNA.

Адреса узлов делятся на адреса подзональных и периферийных узлов. Адреса подзональных узлов являются глобальными и должны быть уникальными в пределах всей сети. Эти адреса присваиваются NAU при активации. Адреса подзональных узлов обычно состоят из двух частей: адреса подзоны и адреса элемента. Все NAU в пределах одной подзоны имеют одинаковый адрес подзоны, но разные адреса элементов.

Адреса периферийных узлов, которые считаются локальными адресами, отличаются в зависимости от типа узла: T2 или T2.1. Адреса T2 определяют NAU и являются статическими; адреса T2.1 назначаются динамически на время сеанса определяют сеанс, а не NAU. Адреса периферийных узлов называют локальными идентификаторами сеанса.

Маршрутизация IBM APPN

Маршрутизация усовершенствованной одноранговой сети (Advanced Peer-to-Peer Networking — APPN) IBM является динамической и основана на выборе маршрута с наи-

меньшим весом, вычисляемым по данным, полученным ото всех узлов сети APPN. Каждый узел сети APPN сообщает об изменениях в его локальной топологии (то есть в топологии самого узла и подключенных к нему каналов). Информация о топологии передается всем узлам APPN. Когда узел получает данные, которые ему уже известны, он прекращает их передачу другим узлам. Дублированная информация распознается путем проверки обновленных порядковых номеров. На рис. 43.5 показано место узлов сети APPN в общей схеме среды APPN с конечными (EN) и низкоуровневыми (LEN) узлами.

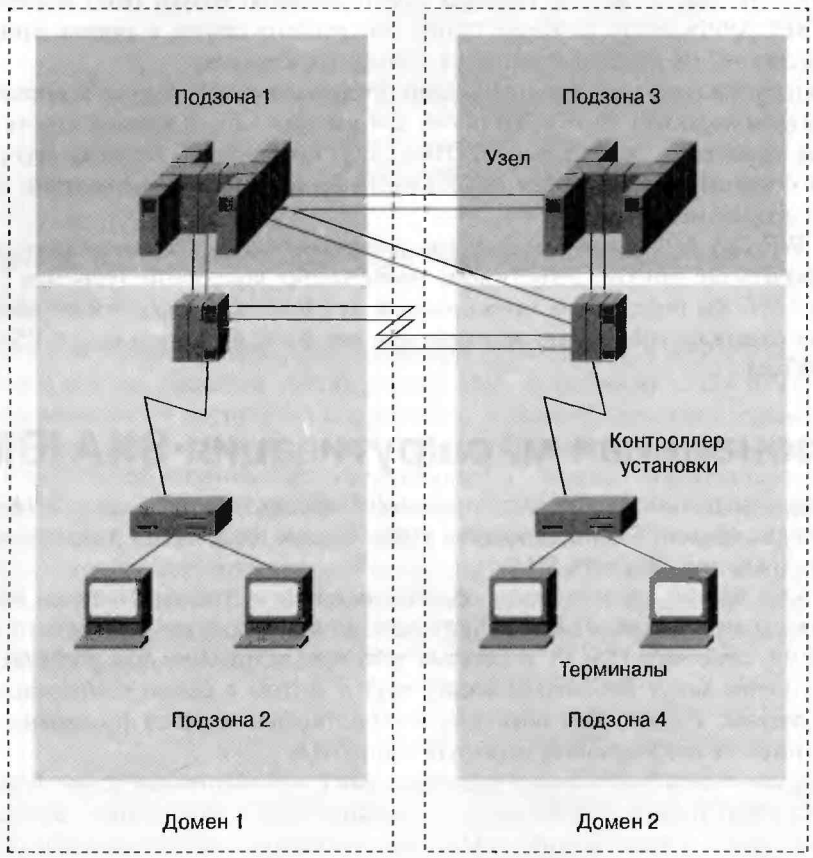


Рис. 43.4. При подзональной маршрутизации SNA подзоны принадлежат доменам

В основе маршрутизации APPN лежит несколько функций и свойств. Это маршрутизация узлов типа 2.1, маршрутизация зависимого логического запрашивающего узла/сервера (Dependent Logical-Unit Requester/Server — DLUR/S), сети соединений и граничные узлы.

Маршрутизация узлов типа 2.1 в APPN IBM

Узел типа 2.1 предполагает маршрутизацию потоков данных между одним или несколькими сетевыми узлами APPN. Поддерживаются два типа процессов маршрутизации узла типа 2.1: маршрутизация промежуточного сеанса (Intermediate Session Routing — ISR) и скоростная маршрутизация (High-Performance Routing — HPR).

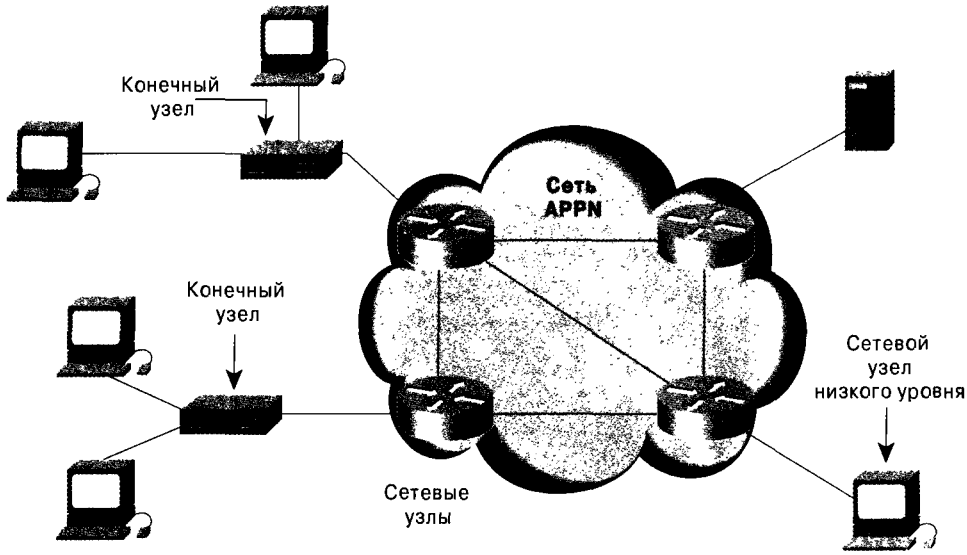


Рис. 43.5. Соединение сетевых узлов APPN с конечными, низкоуровневыми и другими сетевыми узлами APPN

Маршрутизация промежуточного сеанса

Маршрутизация промежуточного сеанса (Intermediate Session Routing — ISR) включает в себя логическое связывание запросов и ответов сеанса BIND, передаваемых с одного сетевого узла на другой. В этой среде вместо таблиц маршрутизации, применяемых в APPN, создаются и используются сеансовые соединители. В ISR устанавливается соответствие идентификатора сеанса и порта между одной стороной узла и другой. Уникальный идентификатор сеанса в заголовке сеансового соединителя меняется местами с исходящим идентификатором и затем отправляется из соответствующего порта.

ISR поддерживает такие свойства подзоны SNA, как межузловая ошибка и обработка данных управления потоком, а также переключение сеанса при сбоях сети. Обработка межузловых ошибок и данных управления потоком считаются излишними, поскольку снижают сквозную пропускную способность.

Скоростная маршрутизация

Протокол скоростной маршрутизации HPR (High-Performance Routing — HPR), являющийся альтернативой ISR, основан на двух основных компонентах: протоколе быстрой передачи (Rapid-Transport Protocol — RTP) и автоматической сетевой маршрутизации (Automatic Network Routing — ANR). RTP представляет собой надежный, ориентированный на соединение протокол, гарантирующий доставку и позволяющий регулировать ошибку сквозной сети и управлять передачей. Протокол RTP создает новые маршруты, регистрируя сбои в сети. ANR представляет собой межузловую службу маршрутизации от источника, не требующую подтверждения соединения.

Уровень RTP активизируется только на границах сетей APPN. В промежуточных узлах активизируется только уровень ANR. Узлы RTP устанавливают RTP-соединения для переноса данных сеанса. Весь поток данных отдельного сеанса про-

ходит через одно соединение RTP-RTP и мультиплексируется с потоками данных других сеансов, использующих это же соединение. На рис. 43.6 показана общая архитектура среды с HPR-маршрутизацией.

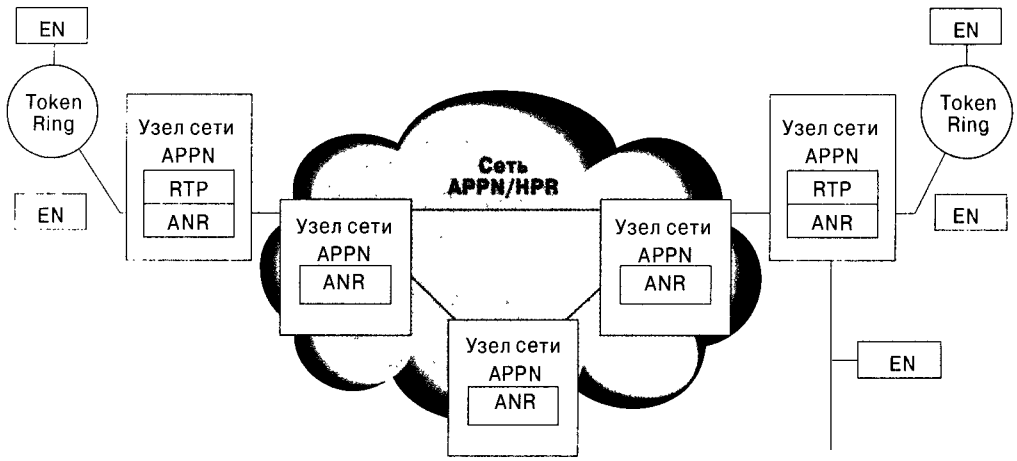


Рис. 43.6. Протокол RTP поддерживается только граничными сетевыми узлами APPN

Типичный процесс скоростной маршрутизации состоит из нескольких этапов. Вначале при помощи ISR выбирается маршрут. Для того, чтобы установить соединение между граничными RTP-узлами, используется либо уже существующее соединение RTP-RTP, либо посылается запрос служб маршрутизации (Route-Service Request — RSR). Полученный ответ службы маршрутизации (Route-Service Reply — RSP) содержит информацию о прямом и обратном сетевых маршрутах.

Маршруты представляют собой списки прямых и обратных портов и содержат идентификатор порта в каждом ANR-узле. Эти списки сопровождают каждое сообщение, устраняя необходимость в таблицах маршрутизации и сеансовых соединителях в узлах ANR.

Скоростная маршрутизация предусматривает восстановление после сбоев в результате обрыва соединения. Если соединение обрывается, но между конечными точками RTP существует другой маршрут с тем же CoS, то может быть выбрано новое соединение RTP-RTP, и сеанс продолжится без перерыва. Если же другого маршрута не существует, то посылаются сообщения RSR и RSP, чтобы получить новые списки портов. Отправка нового BIND не требуется, так как сеанс не был прерван.

Для управления потоком при скоростной маршрутизации применяется методика, называемая адаптивным скоростным (Adaptive Rate-Based — ARB) управлением потоком. ARB регистрирует объем данных, поступающего в сеть и управляет им. При таком управлении потоком отправляющие и получающие RTP-узлы обмениваются сообщениями через равные промежутки времени. Поток данных, поступающий в сеть, изменяется так, чтобы адаптироваться к ее условиям.

Маршрутизация DLUR/S APPN IBM

Зависимый логический запрашивающий узел/сервер (Dependent Logical-Unit Requester/Server — DLUR/S) представляет собой функцию APPN, позволяющую потокам данных SNA проходить по сети APPN.

При использовании DLUR/S между зависимым логическим сервером (Dependent Logical-Unit Server — DLUS) и зависимым логическим запрашивающим узлом (Dependent Logical-Unit Requester — DLUR) устанавливаются отношения "клиент-сервер". Обычно DLUS представляет собой элемент ACF/UTAM4.2, а DLUR — маршрутизатор. Между DLUS и DLUR устанавливается пара сеансов LU 6.2. Такие сеансы LU 6.2 передают управляющие сообщения SNA. Эти сообщения, не распознаваемые в среде APPN, инкапсулируются в сеансе LU 6.2. Потом они декапсулируются в DLUR и передаются в LU SNA. Затем инициация сеанса DLU передается DLUS и обрабатывается им как поток данных SNA. DLUS посылает сообщение узлу приложения, который посылает BIND. На последней стадии данные SNA передаются обычным способом, вместе с потоками данных APPN.

Сеть соединений APPN

Сеть соединений APPN представляет собой логическую структуру, обеспечивающую установку прямого соединения между конечными узлами APPN без затрат на настройку прямых соединений между каждой парой конечных узлов. Обычно создание сети соединений начинается с запроса LOCATE от конечного узла.

Затем сетевой узел (Network Node — NN) определяет получателя, указанного в запросе LOCATE. Если NN обнаруживает, что к одному транспортному носителю (например, Token Ring) подключены два EN (источник и получатель), то для соединения двух конечных точек и образования сети соединений используется виртуальный узел (Virtual Node — VN). Сетевой узел определяет маршрут сеанса как прямое соединение EN1-VN-EN2, после чего разрешается передача данных.

Граничный узел APPN IBM

Граничный узел представляет собой элемент APPN, обеспечивающий взаимодействие нескольких сетей APPN. В настоящее время граничные узлы существуют только в ACF/VTAM и OS/400. Граничные узлы связывают базы данных топологии и каталогов для связанных сетей, а также перестраивают запросы BIND, чтобы они показывали отдельные маршруты в каждой сети.

Граничные узлы позволяют сократить базы данных каталогов и топологии в сетевых узлах до размеров, необходимых для отдельных подсетей, а не всей сети. Кроме того, через граничные узлы проходят маршруты межсетевых сеансов. На рис. 43.7 показано место граничных узлов (устройств ACF/VTAM и OS/400) в среде APPN, включающей в себя несколько сетей.

Контрольные вопросы

1. Для чего предназначены сеансовые соединители SNA?
2. Что создается, когда сетевой узел посредством запроса LOCATE определяет, что два конечных узла подключены к общей среде передачи?
3. Верно ли утверждение, что все NAU в пределах подзоны имеют одинаковый адрес элемента?

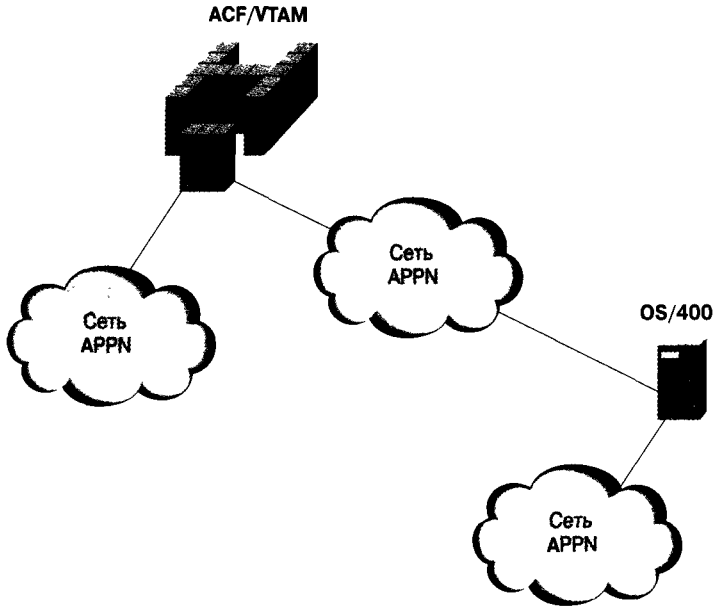


Рис. 43.7. Граничные узлы (устройства ACF/VTAM и OS/400) связывают между собой сети APPN

В этой главе...

- Рассмотрены метрики, используемые протоколом IGRP для сравнения маршрутов
- Описаны способы воздействия администратора на выбор маршрута
- Описана маршрутизация с использованием нескольких маршрутов
- Рассмотрены собственные функции поддержания стабильности протокола IGRP
- Рассмотрены механизмы синхронизации протокола IGRP и их назначение

Глава 44

Протокол IGRP

Протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP) представляет собой протокол маршрутизации, разработанный в середине 1980-х гг. корпорацией Cisco Systems. Главной целью создания протокола IGRP было обеспечение надежного протокола для маршрутизации в пределах автономной системы (AS). Такие протоколы называются протоколами маршрутизации внутреннего шлюза.

В середине 1980-х гг. самым популярным протоколом маршрутизации внутренних шлюзов был протокол маршрутной информации (Routing Information Protocol — RIP). Протокол RIP был вполне пригоден для маршрутизации в мелких и средних относительно однородных объединенных сетях, но по мере роста размеров сетей его ограничения становились все менее приемлемыми. В частности, небольшое количество допустимых переходов (16) RIP ограничивало размер сети, а его единственная метрика (счетчик пересылок), рассчитанная на распределение нагрузки на сеть только методом равных затрат (и только для сетей Cisco!), не обеспечивала достаточной гибкости в сложных средах.

Распространение маршрутизаторов Cisco и надежность IGRP побудили многие организации с крупными объединенными сетями перейти с протокола RIP на протокол IGRP.

Первоначальная реализация IGRP, разработанная корпорацией Cisco, работала в IP-сетях. Однако IGRP был предназначен для работы в любой сетевой среде, и Cisco вскоре перенесла его в сети CLNP (Connectionless-Network Protocol — CLNP) OSI. Для повышения эффективности протокола IGRP корпорация Cisco в начале 1990-х гг. XX в. разработала усовершенствованный протокол IGRP (Enhanced IGRP — EIGRP). В настоящей главе обсуждается базовая структура протокола IGRP и его реализация. Протокол Enhanced IGRP обсуждается в главе 42,"Протокол EIGRP".

Характеристики протокола IGRP

IGRP является *дистанционно-векторным* протоколом маршрутизации внутреннего шлюза (Interior Gateway Protocol — IGP). Дистанционно-векторные протоколы маршрутизации математически сравнивают маршруты используя какой-либо способ измерения расстояния. Полученная характеристика называется вектором расстояния. Маршрутизаторы, использующие протокол маршрутизации по вектору расстояния, должны регулярно посылать всем соседним маршрутизаторам всю или часть своей таблицы маршрутизации в виде сообщений о корректировке маршрута. По мере рас-

пространения маршрутной информации по сети маршрутизаторы узнают о новых узлах-получателях, подключаемых к сети, о сетевых сбоях и, что более важно, вычисляют расстояния до всех известных узлов-получателей.

Дистанционно-векторные протоколы маршрутизации часто противопоставляются протоколам маршрутизации по состоянию канала, которые отправляют информацию о локальном соединении всем узлам объединенной сети. Два распространенных протокола маршрутизации по состоянию канала: Open Shortest Path First (OSPF) и Intermediate System-to-Intermediate System (ISIS), описаны в главах 47 "Протокол OSPF" и 48 "Протоколы маршрутизации OSI".

В протоколе IGRP используется составная метрика, вычисляемая на основании взятых с определенным весом математических значений задержки в объединенной сети, полосы пропускания, надежности и нагрузки. У каждой из таких величин есть свой коэффициент (вес), который сетевой администратор может изменить, хотя делать это нужно очень осторожно. В протоколе IGRP предусмотрен широкий диапазон значений метрик. Например, надежность и загрузка могут изменяться от 1 до 255, полоса пропускания может принимать значения, соответствующие скоростям передачи от 1200 бит/с до 10 Гбит/с, а задержка может изменяться в пределах от 1 до 2^{24}. Эти широкие диапазоны значений метрик дополняются рядом констант, определяемых пользователем, что позволяет сетевому администратору влиять на выбор маршрута. Эти константы сравниваются с метриками и друг с другом в соответствии с алгоритмом, который и определяет единую, составную метрику. Такая гибкость позволяет сетевым администраторам выполнять тонкую настройку автоматического выбора маршрута по протоколу IGRP.

Для обеспечения дополнительной гибкости IGRP допускает маршрутизацию по нескольким маршрутам. Двойные каналы с одинаковой полосой пропускания могут циклически пропускать один поток данных, с автоматическим переключением на второй канал, если первый выйдет из строя. Маршруты могут иметь разные метрики и, вместе с тем, остаются действительными множественными маршрутами. Например, если один маршрут в три раза лучше другого (его метрика в три раза меньше), то лучший маршрут будет применяться втрое чаще. Для множественной маршрутизации могут использоваться только маршруты с метриками, отклонения которых от метрики наилучшего маршрута находятся в пределах определенного диапазона или дисперсии. Дисперсия является еще одной характеристикой, которая может быть устанавлена сетевым администратором.

Функции повышения стабильности

Протокол IGRP имеет ряд функций, предназначенных для повышения стабильности: удержания, расщепление горизонтов и обратные обновления.

Удержания (holddown) применяются во избежание восстановления в таблице маршрута, на котором, возможно, произошел сбой, в результате регулярных сообщений об обновлении. Если маршрутизатор выходит из строя, то соседние маршрутизаторы обнаруживают это по отсутствию регулярных сообщений обновления маршрутов. В этом случае маршрутизаторы вычисляют новые маршруты и отправляют сообщения об изменении маршрутизации, чтобы проинформировать своих соседей об изменении маршрута. Результатом этого является волна корректировок, которые фильтруются через сеть. Такие обновления поступают на сетевые устройства не одновременно. Устройство, еще не получившее сообщения о сбое в сети, может отправить регулярное сообщение обновления (согласно которому маршрут, где только что произошел сбой,

является действительным) другому устройству, только что получившему сообщение об этом сетевом сбое. В этом случае, на вышеупомянутом устройстве окажется (и, возможно, распространится дальше) неверная маршрутная информация.

Интервалы задержки изменений предписывают маршрутизаторам в течение некоторого периода времени не передавать дальше любые сообщения об изменениях, которые могут повлиять на маршруты. Интервал задержки изменений обычно выбирается таким образом, чтобы он несколько превышал время прохождения обновления маршрутизации во всей сети.

Метод *расщепления горизонта (split horizon)* опирается на предположение, что нецелесообразно посылать информацию о маршруте в том направлении, откуда она поступила. Для иллюстрации этого метода рассмотрим пример сети, показанной на рис. 44.1. Маршрутизатор 1 (R1) объявляет, что у него есть маршрут к Сети А. Маршрутизатору 2 (R2) нет оснований включать этот маршрут в свое сообщение обновления, которое он посылает R1, т.к. R1 ближе к Сети А. Согласно правилу расщепления горизонта маршрутизатор R2 должен исключить данный маршрут из всех сообщений обновления, посылаемых им маршрутизатору R1. Метод расщепления горизонта позволяет предотвращать маршрутные петли. Например, предположим, что интерфейс R1 с Сетью А вышел из строя. Без расщепления горизонтов маршрутизатор R2 продолжал бы информировать маршрутизатор R1 о том, что через него можно попасть в Сеть А (через R1). Если маршрутизатор R1 не располагает достаточными аналитическими ресурсами, то он действительно может выбрать маршрут, предлагаемый R2, в качестве альтернативы своему отказавшему прямому соединению, что приведет к образованию маршрутной петли. И хотя удержания должны помешать этому, в IGRP реализовано также расщепление горизонтов, что обеспечивает дополнительную стабильность алгоритма.

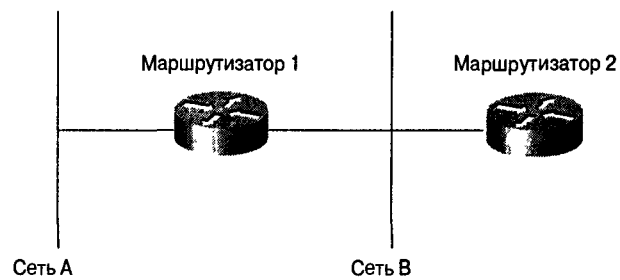


Рис. 44.1. Правило расщепления горизонта позволяет избежать маршрутных петель

Расщепление горизонта предотвращает образование маршрутных петель между смежными маршрутизаторами. Для ликвидации более крупных маршрутных петель применяются *обратные обновления (poison-reverse updates)*. Увеличение значений маршрутных метрик обычно указывает на появление маршрутных петель. В этом случае посылаются обратные обновления, чтобы удалить этот маршрут и перевести его в режим удержания. В реализации IGRP Cisco обратные обновления отправляются в том случае, если маршрутная метрика увеличивается в 1,1 и более раз.

Таймеры

Протокол IGRP предусматривает использование ряда таймеров и переменных, содержащих временные интервалы: таймер обновлений, таймер недействительных

маршрутов, период удержания и таймер исключения. *Таймер обновлений (update timer)* определяет, с какой частотой должны отправляться сообщения об обновлении маршрутов. Для протокола IGRP стандартное значение этой переменной равно 90 сек. *Таймер недействительных маршрутов (invalid timer)* определяет, в течение какого времени при отсутствии сообщений обновления маршрутизатор должен ожидать, прежде чем объявить этот маршрут недействительным. Стандартное значение IGRP для такой переменной составляет три периода обновления. *Период удержания (hold-time period)* определяет промежуток задержки внесения изменений в таблицу маршрутизации. Его стандартное значение в пользователе IGRP на 10 секунд больше тройного периода таймера обновления. Наконец, *таймер исключения (flush timer)* определяет, какое времени должно пройти до исключения маршрутизатора из таблицы маршрутизации. По умолчанию для протокола IGRP это время в семь раз превышает период рассылки обновления маршрутов.

Резюме

IGRP зарекомендовал себя как один из самых удачных из когда-либо существовавших протоколов маршрутизации. Этим он во многом обязан функциональному сходству с протоколом RIP — еще одним удачным и широко распространенным протоколом маршрутизации. Корпорация Cisco приложила все возможные усилия для того, чтобы сохранить многие эффективные функции RIP, одновременно значительно расширив его возможности. В настоящее время возраст IGRP начинает сказываться: ему недостает поддержки сетевых масок переменной длины (VLSM). Вместо того, чтобы разрабатывать версию IGRP 2, где можно было бы предусмотреть такую возможность, корпорация Cisco создала протокол Enhanced IGRP, унаследовавший все достоинства IGRP. Более подробная информация о протоколе Enhanced IGRP приведена в главе 42, "Протокол EIGRP".

Контрольные вопросы

1. Перечислите достоинства протокола IGRP, которые отсутствуют в протоколе RIP.
2. Как администратор может влиять на выбор маршрута?
3. Что такое дисперсия и как она влияет на множественную маршрутизацию?
4. Перечислите и опишите функции обеспечения стабильности IGRP.
5. Какие таймеры используются в IGRP и каковы выполняемые функции?

Дополнительные источники

- Sportack M. A. *IP Routing Fundamentals.* Indianapolis: Cisco Press, 1999.
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/np1_c/1cigrp.htm

В этой главе...

- Определено понятие многоадресатной рассылки
- Рассмотрены основы протокола IGMP
- Рассмотрены принципы групповой адресации при коммутации 2-го уровня
- Рассмотрены связующие деревья многоадресатной рассылки
- Рассмотрено функционирование многоадресатной пересылки
- Описаны основы протокола PIM
- Рассмотрен многопротокольный BGP
- Рассмотрены принципы работы протокола MSDP
- Рассмотрен протокол надежной многоадресатной рассылки PGM

Глава 45

Многоадресатная рассылка

Введение

Групповая IP-адресация представляет собой технологию экономии полосы пропускания, которая сокращает объем передачи за счет доставки одного потока информации сразу тысячам корпоративных и частных абонентов. Преимуществами групповой адресации пользуются такие приложения, как видеоконференции, корпоративная связь, дистанционное обучение, а также распространение программного обеспечения, котировок акций и новостей.

Многоадресатная рассылка доставляет данные от источника нескольким получателям без дополнительной нагрузки на источник и получателей, используя минимальную полосу пропускания по сравнению с другими подобными технологиями. Многоадресатные пакеты дублируются в сети маршрутизаторами Cisco, на которых установлен протокол многоадресатной рассылки, независимой от протокола (Protocol Independent Multicast — PIM) или другой протокол, поддерживающий групповую адресацию, что обеспечивает наиболее эффективную доставку данных нескольким получателям. Все прочие варианты требуют, чтобы источник посылал несколько копий данных каждому получателю в отдельности. Если получателей тысячи, то от применения технологии Cisco IP Multicast выиграют даже приложения, не очень требовательные к полосе пропускания. Один поток данных от приложения, нуждающегося в широкой полосе пропускания, например видео в формате MPEG, может занять значительную часть имеющейся полосы пропускания. Для таких приложений многоадресатная рассылка является единственным способом передачи данных сразу нескольким получателям. На рис. 45.1 показано, как данные из одного источника при помощи многоадресатной рассылки доставляются нескольким получателям.

Понятие группы многоадресатной рассылки

В основе групповой IP-адресации лежит понятие группы. Под группой многоадресатной рассылки понимается произвольно выбранная группа получателей, заинтересованная в получении определенного потока данных. У этой группы нет никаких

физических или географических ограничений: узлы могут находиться в любой точке Internet. Узлы, заинтересованные в получении данных для определенной группы, должны присоединиться к этой группе при помощи протокола IGMP. Для того чтобы получать поток данных, узел должен входить в группу.

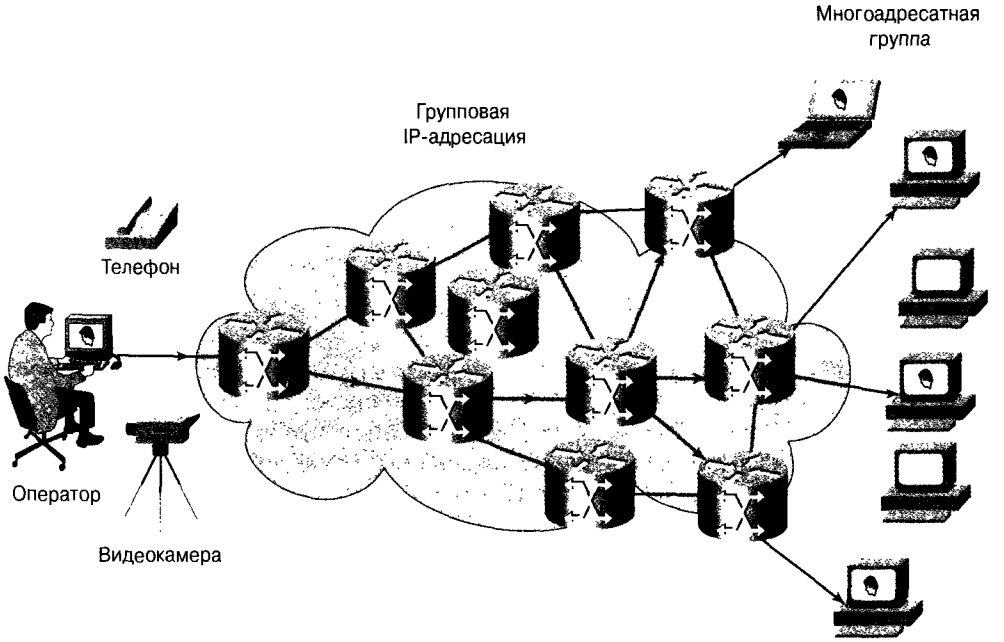


Рис. 45.1. Многоадресатная передача данных: все абоненты получают один пакет многоадресатной рассылки

IP-адреса многоадресатной рассылки

Групповые адреса определяют произвольную группу IP-узлов, присоединившихся к этой группе и желающих получать адресованные ей данные.

IP-адреса класса D

Назначением групповых IP-адресов управляет Агентство по выделению имен и уникальных параметров протоколов Internet (Internet Assigned Numbers Authority — IANA). Оно выделило для групповой IP-адресации часть адресов класса D. Это означает, что все групповые IP-адреса находятся в диапазоне от 224.0.0.0 до 239.255.255.255.

Примечание

Данный диапазон предназначен только для групповых адресов или адресов получателей многоадресатной IP-рассылки. Адреса источников многоадресатных дейтаграмм всегда являются адресами одноадресатной рассылки.

Зарезервированные локальные адреса

IANA зарезервировало адреса с 224.0.0.0 до 224.0.0.255 для сетевых протоколов локальных сетевых сегментов. Пакеты с такими адресами никогда не проходят через маршрутизатор. Они не выходят за пределы своего сегмента LAN. Их время существования всегда устанавливается равным 1.

Сетевые протоколы используют эти адреса для автоматического обнаружения маршрутизатора и для передачи важной маршрутной информации. Например, протокол OSPF использует адреса 224.0.0.5 и 224.0.0.6 для обмена информацией о состоянии канала. Некоторые хорошо известные адреса перечислены в табл. 45.1.

Таблица 45.1. Локальные адреса

Адрес	Использование
224.0.0.1	Все системы в подсети
224.0.0.2	Все маршрутизаторы в подсети
224.0.0.5	Маршрутизаторы OSPF
224.0.0.6	Назначенные маршрутизаторы протокола OSPF
224.0.0.12	DHCP сервер/агент передачи

Глобальные адреса

Адреса в диапазоне от 224.0.1.0 до 238.255.255.255 являются глобальными. Они могут использоваться для многоадресатной передачи данных между организациями и для передачи по сети Internet.

Некоторые из этих адресов зарезервированы IANA для многоадресатных приложений. Например, адрес 224.0.1.1 зарезервирован для протокола NTP.

Более подробные сведения о зарезервированных групповых адресах можно найти по адресу http://www.isi.edu/in-notes/iana/assignments/multicast-addresses.

Адреса ограниченного радиуса действия

В диапазоне от 239.0.0.0 до 239.255.255.255 содержатся адреса ограниченного радиуса действия, или административно ограниченные адреса. RFC 2365 ограничивает использование этих адресов локальной группой либо организацией. Маршрутизаторы обычно имеют фильтры, настроенные так, чтобы данные многоадресатной рассылки по этим адресам не выходили за пределы автономной системы (AS) или другой области, определенной пользователем. В пределах автономной системы или такой области адреса ограниченного действия можно также подразделить на группы, определив границы их влияния. Это позволяет использовать в полученных областях одни и те же адреса.

Статические адреса (GLOP-адресация)

RFC 2770 предлагает, чтобы диапазон адресов 233.0.0.0/8 был зарезервирован для статических адресов организациями, за которыми уже зарезервирован номер автономной системы AS. Номер AS в домене записывается во второй и третий октеты адреса из диапазона 233.0.0.0/8.

Например, номер AS 6200 в шестнадцатеричной системе записывается как F23A. Разделяя два октета F2 и 3A, получаем десятичные числа 242 и 58. Они указывают на подсеть 233.242.58.0, глобально зарезервированную для AS 6200.

Адреса многоадресатной рассылки 2-го уровня

Как правило, сетевые адаптеры в секторах локальных сетей получают только пакеты, соответствующие их MAC-адресам или пакеты с широковещательными MAC-адресами. Для того, чтобы несколько узлов многоадресатной группы могли получить один и тот же пакет и, вместе с тем, различали разные многоадресатные группы, были разработаны различные средства.

К счастью, в спецификации локальной сети IEEE предусмотрена передача широковещательных и многоадресатных пакетов. В стандарте 802.3 бит 0 первого октета используется для индикации широковещательных и многоадресатных фреймов. Расположение такого бита в фрейме Ethernet показано на рис. 45.2.

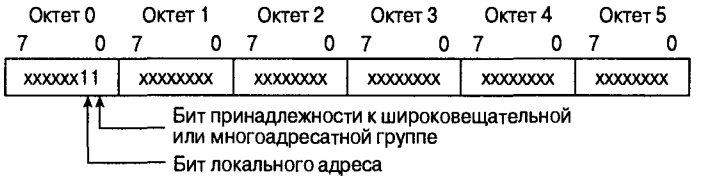


Рис. 45.2. MAC-адрес формата IEEE 802.3

Данный бит показывает, что фрейм предназначен для какой-либо группы узлов или для всех узлов сети (в случае если это широковещательный адрес 0xFFFF.FFFF.FFFF).

При многоадресатной рассылке эта возможность используется передачи IP-пакетов группе узлов локальной сети.

Преобразование MAC-адреса Ethernet

IANA владеет блоком MAC-адресов Ethernet, начиная с шестандатеричного адреса 01:00:5E. Половина этого блока предназначена для адресов многоадресатной рассылки. Таким образом образуется диапазон MAC-адресов Ethernet от 0100.5e00.0000 до 0100.5e7f.ffff.

Выделение этих адресов позволяет установить соответствие между 23 битами Ethernet-адреса и IP-адресами многоадресатной рассылки. При этом младшие 23 бита IP-адреса преобразуются в эти 23 бита адреса Ethernet (рис. 45.3).

Поскольку верхние 5 битов IP-адреса многоадресатной рассылки при преобразовании теряются, получившийся адрес не является уникальным. В действительности одному адресу Ethernet соответствуют 32 многоадресатные группы (рис. 45.4).

Протокол IGMP

Межсетевой протокол управления группами (Internet Group Management Protocol — IGMP) используется для динамической регистрации отдельных узлов в группе многоадресатной рассылки локальной сети. Узлы определяют принадлежность к группе, посылая IGMP-сообщения на свой локальный многоадресатный маршрутизатор.

По протоколу IGMP маршрутизаторы получают IGMP-сообщения и периодически посылают запросы, чтобы определить, какие группы активны или неактивны в данной сети.

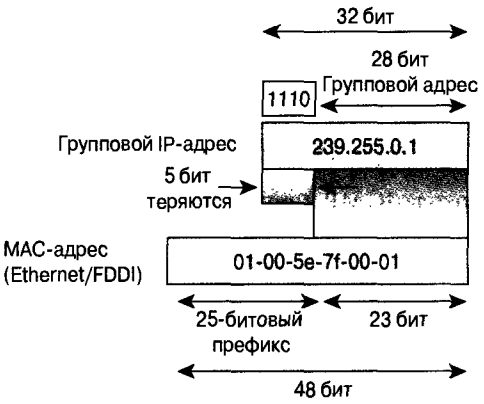


Рис. 45.3. Преобразование IP-адреса многоадресатной рассылки в адрес Ethernet

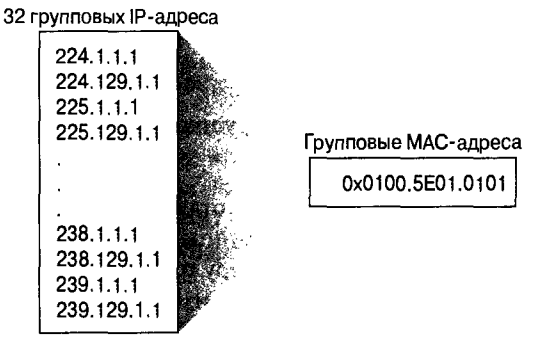


Рис. 45.4. Неоднозначность MAC-адреса

Протокол IGMP версии 1

Спецификация протокола IGMP 1 описана в RFC 1112. Формат пакета показан на рис. 45.5.

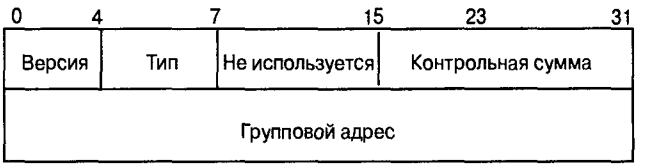


Рис. 45.5. Формат пакета IGMP 1

В протоколе IGMP 1 предусмотрено лишь два типа IGMP-сообщений:

- запрос о принадлежности к группе;
- ответ на запрос о принадлежности к группе.

Узлы отсылают IGMP-ответы, которые соответствуют определенной многоадресатной группе, для того, чтобы сообщить о своем желании присоединиться к этой группе. Маршрутизатор периодически отправляет IGMP-запрос, чтобы убедиться, что хотя бы один узел в подсети еще заинтересован в получении данных, предназначенных для данной группы. При отсутствии ответа на три последовательных IGMP-запроса маршрутизатор отключает группу и прекращает передавать адресованные ей данные.

Протокол IGMP версии 2

Спецификация протокола IGMP 2 описана в RFC 2236. Формат пакета показан на рис. 45.6.

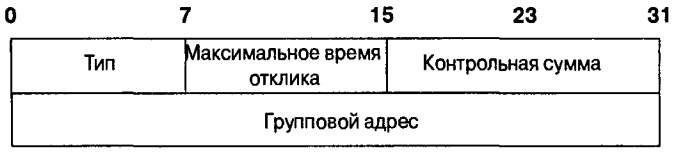


Рис. 45.6. Формат пакета IGMP 2

В IGMP 2 предусмотрено четыре типа IGMP-сообщений:

- запрос принадлежности к группе;
- ответ на запрос о принадлежности к группе по версии 1;
- ответ на запрос о принадлежности к группе по версии 2;
- сообщение о выходе из группы.

В основном работа протокола IGMP 2 не отличается от IGMP 1. Разница заключается в наличии сообщения о выходе из группы. Теперь узлы могут сами сообщить локальному многоадресатному маршрутизатору о намерении покинуть группу. В ответ маршрутизатор посылает группе специальный запрос, чтобы определить, остались ли в ней еще узлы, желающие получать данные. Если ответ не поступает, то маршрутизатор отключает группу и прекращает передачу данных. Это может значительно сократить задержки, связанные с прекращением членства в группе, по сравнению с IGMP 1. В этом случае передача нежелательных и ненужных данных может быть прекращена значительно быстрее.

Многоадресатная рассылка в среде коммутации на 2-м уровне

Стандартное поведение коммутатора 2-го уровня заключается в передаче всех данных многоадресатной рассылки на каждый порт, принадлежащий локальной сети-получателю на данном коммутаторе. Это противоречит основному назначению коммутатора, которое заключается в ограничении объема пересылки данных и доставке их только тем портам, для которых такие данные действительно предназначены.

Существует два метода эффективной многоадресатной рассылки на 2-м уровне в среде коммутации — использование протокола CGMP- и прослушивание по протоколу IGMP.

Протокол CGMP

Cisco-протокол управления группами CGMP (Cisco Group Management Protocol) представляет собой протокол Cisco, позволяющий коммутаторам Catalyst транслировать IGMP-информацию маршрутизаторам Cisco для принятия решений о пересылке на 2-м уровне. Протокол CGMP должен быть сконфигурирован как на многоадресатных маршрутизаторах, так и на коммутаторах 2-го уровня. В результате при использовании протокола CGMP данные многоадресатной рассылки протокола IP доставляются только на те порты коммутатора Catalyst, которые заинтересованы в получении этих данных. Остальные порты, которые явным образом не запрашивали эти данные, не получают их.

Основная концепция CGMP представлена на рис. 45.7. Когда узел присоединяется к группе многоадресатной рассылки (часть А), он отправляет этой группе (в данном примере по адресу 224.1.2.3) сообщение-отчет протокола IGMP о добровольном присоединении к группе. Этот отчет передается через коммутатор маршрутизатору для обычной IGMP-обработки. Маршрутизатор (интерфейс которого должен поддерживать CGMP) получает такой отчет IGMP и обрабатывает его как обычно, но в дополнение к этому создает CGMP-сообщение о присоединении и отправляет его коммутатору.

Коммутатор получает CGMP-сообщение о присоединении и заносит порт в свою таблицу ассоциативной памяти (content addressable memory — CAM) для этой группы многоадресатной рассылки. Теперь данные для данной многоадресатной группы будет направляться узлу через этот порт. Многоадреснатые маршрутизаторы должны прослушивать данные многоадресатной рассылки для всех групп, так как управляющие IGMP-сообщения также посылаются в виде многоадресатных данных. При использовании протокола CGMP коммутатор должен прослушивать только CGMP-сообщения о присоединении и выходе из группы, поступающие от маршрутизатора. Остальные данные многоадресатной рассылки передаются согласно таблице CAM обычным для коммутатора образом.

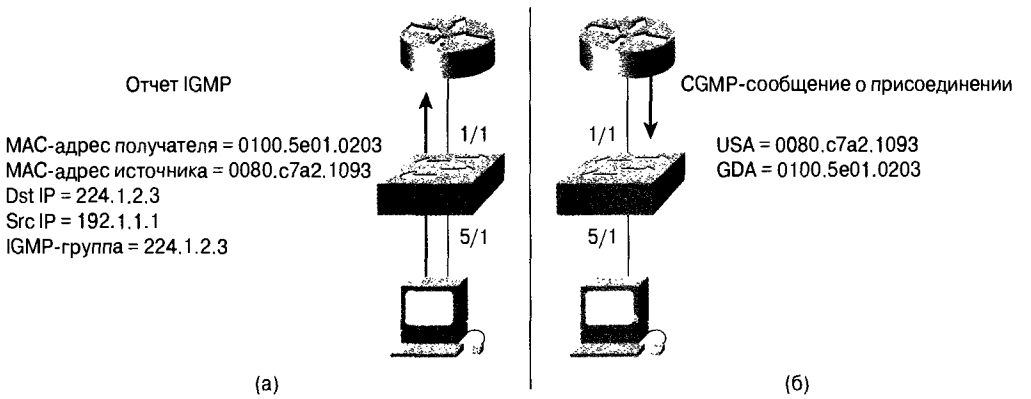


Рис. 45.7. Основные действия CGMP

IGMP-прослушивание

IGMP-прослушивание представляет собой проверку или прослушивание LAN на наличие в IGMP-пакетах, передаваемых между узлом и маршрутизатором, информа-

ции 3-го уровня. Если коммутатор обнаруживает в сообщении IGMP-отчет узла для группы многоадресатной рассылки, то он заносит номер порта узла в свою таблицу ассоциативной памяти для многоадресатной рассылки. Если же коммутатор обнаруживает IGMP-сообщение о выходе узла из группы, то он удаляет номер порта этого узла из своей таблицы.

Поскольку управляющие IGMP-сообщения передаются в виде многоадресатных пакетов, они неотличимы от многоадресатных данных 2-го уровня. Коммутатор, на котором осуществляется IGMP-прослушивание, проверяет все многоадресатные пакеты и ищет среди них те, которые содержат управляющую информацию. Если IGMP-прослушивание выполняется на маломощном коммутаторе с медленным процессором, то при передаче данных с высокой скоростью это может значительно повлиять на производительность. Поэтому для IGMP-прослушивания следует применять мощные коммутаторы со специализированными микросхемами для проверки IGMP-сообщений на аппаратном уровне. Для маломощных коммутаторов без специального оборудования оптимальным вариантом является использование протокола CGMP.

Связующие деревья многоадресатной рассылки

Маршрутизаторы многоадресатной рассылки создают связующие деревья, по которым определяется маршрут, которым должны проследовать по сети данные многоадресатной рассылки протокола IP, чтобы достичь всех получателей. Существует два основных типа многоадресатных связующих деревьев: деревья от источника и деревья общего доступа.

Дерево от источника

Простейшей формой многоадресатного связного дерева является *дерево от источника*. Его корнем служит источник многоадресатного дерева, а ветви образуют связующее дерево, соединяющее источник с получателями. Поскольку это дерево использует кратчайшие маршруты, его также называют деревом кратчайших маршрутов (shortest path tree — SPT).

На рис. 45.8 показано дерево SPT для группы 224.1.1.1 с корнем в источнике (узел A) и двумя получателями — узлами B и C.

Дерево SPT описывается в виде пары значений типа (S, G), где S — IP-адрес источника (Source), а G — групповой адрес получателей (Group). В частности, SPT-дерево на рис. 45.8 описывается как (192.1.1.1, 224.1.1.1).

Запись (S,G) подразумевает, что между каждым источником и каждой группой существует единственное и корректное SPT-дерево. Например, если узел B также отправляет данные группе 224.1.1.1, а получателями являются узлы A и C, то должно существовать отдельное дерево (192.2.2.2, 224.1.1.1).

Дерево общего доступа

В отличие от дерева источника, корень которого находится в источнике, *деревья общего доступа* имеют единый, общий корень в некоторой специально предназначенной для этого точке сети. Такой общий корень называется *точкой рандеву* (Rendezvous Point — RP).

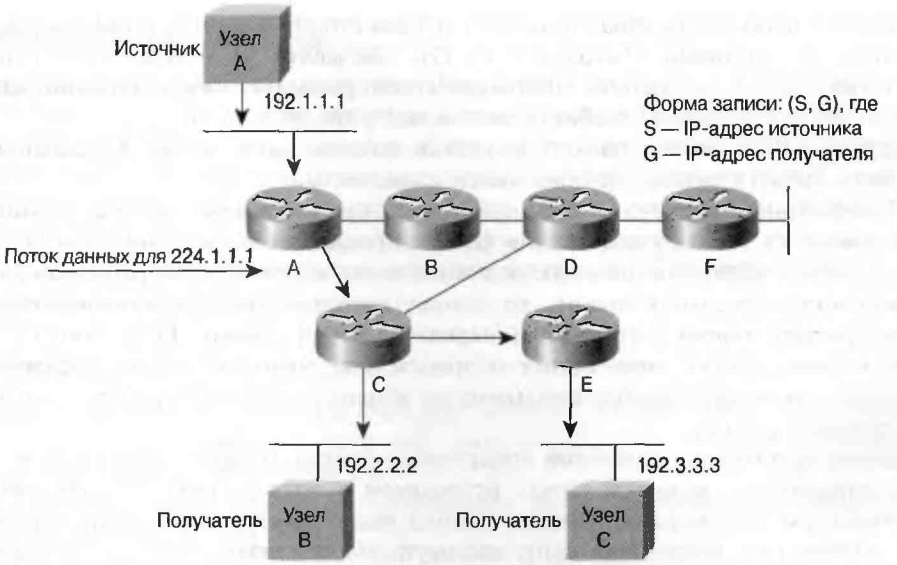


Рис. 45.8. Дерево кратчайших маршрутов для узла A

На рис. 45.9 показано дерево общего доступа для группы 224.2.2.2, корнем которого является маршрутизатор D. При использовании дерева общего доступа источники отправляют потоки данных корню, откуда он передается в нисходящем направлении по дереву общего доступа всем получателям.

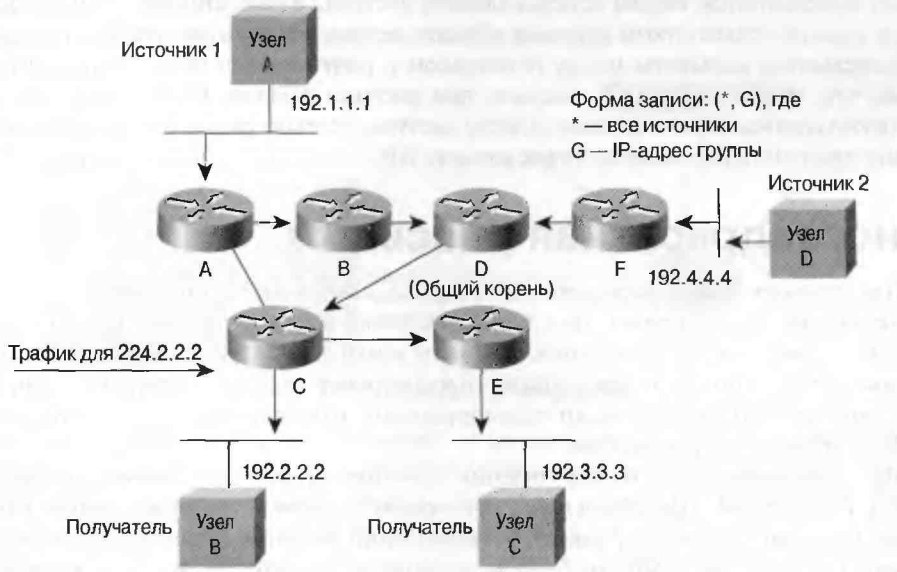


Рис. 45.9. Дерево общего доступа

В этом примере данные многоадресатной рассылки от источников — узлов A и D — передаются корню (маршрутизатор D), а оттуда по дереву общего доступа — двум получателям, узлам B и C. Поскольку все источники в многоадресатной группе

используют одно дерево общего доступа, то для его обозначения применяется форма записи с групповым символом *: (*, G). "Звездочка" в данном случае означает все источники, а G —группу многоадресатной рассылки. Соответственно, дерево общего доступа на рис. 45.9 обозначается как (*, 224.2.2.2).

Деревья SPT и деревья общего доступа не должны иметь петель. Сообщения дублируются только в точках, где появляются новые ветви.

Присоединиться к группе многоадресатной рассылки или покинуть ее можно в любой момент, поэтому связующие деревья нуждаются в динамическом обновлении. Если все активные получатели данной ветви перестанут запрашивать данные данной многоадресатной группы, то маршрутизаторы должны исключить эту ветвь из связующего дерева и прекратить передачу по ней данных. Если один из получателей данной ветви снова станет активным и запросит данные многоадресатной рассылки, то маршрутизатор динамически изменит связующее дерево и возобновит передачу данных.

Дерево кратчайших маршрутов имеет преимущество, которое заключается в создании оптимального маршрута между источником и получателями. Это обеспечивает минимальную задержку при передаче данных многоадресатной рассылки. Однако такая оптимизация имеет свою цену: маршрутизаторы должны собирать маршрутную информацию о каждом источнике. Если в сети тысячи источников и групп, то это может потребовать от маршрутизаторов значительных затрат ресурсов. Сетевым разработчикам следует принимать во внимание зависимость требуемых объемов памяти от размера многоадресатной таблицы маршрутизации.

Преимущество деревьев общего доступа заключается в том, что каждый маршрутизатор должен хранить лишь минимальный объем информации о состоянии сети. Если в сети используются только деревья общего доступа, то это снижает общие требования к памяти. Недостатком деревьев общего доступа является то, что в определенных обстоятельствах маршруты между источником и получателями не являются оптимальными, что, может привести к задержке при доставке пакетов. При реализации среды, где используются только деревья общего доступа, сетевые разработчики должны тщательно продумать размещение точек рандеву RP.

Многоадресатная рассылка

При одноадресатной маршрутизации данные направляются по одному маршруту — от источника к получателю. Для одноадресатного маршрутизатора адрес источника вообще не имеет особого значения. Для него важен только адрес получателя и то, как доставить туда данные. Маршрутизатор просматривает таблицу маршрутизации, после чего отправляет один экземпляр одноадресатного пакета через соответствующий интерфейс устройству-получателю.

При многоадресатной маршрутизации источник отправляет данные произвольной группе получателей, представленных групповым адресом. Многоадресатный маршрутизатор должен определить, какое из направлений является входящим (к источнику), а какое (какие) — исходящим. Если исходящих маршрутов много, то маршрутизатор копирует пакет и направляет его по соответствующим маршрутам, причем необязательно по всем. Принцип доставки данных многоадресатной рассылки не столько к получателю, сколько от источника называется *обратной передачей.*

Обратная передача

Пересылка по обратному маршруту (Reverse Path Forwarding — RPF) представляет собой фундаментальный принцип многоадресатной маршрутизации, позволяющий маршрутизаторам передавать данные многоадресатной рассылки по связующему дереву в правильном направлении. При использовании RPF соседние входящие и исходящие узлы определяются по таблице маршрутизации одноадресатной рассылки. Маршрутизатор отправляет многоадресатный пакет только в том случае, если этот пакет поступил на входной интерфейс. Это гарантирует отсутствие петель в связующем дереве.

RPF-проверка

Когда на вход маршрутизатора поступает многоадресатный пакет, маршрутизатор выполняет его RPF-проверку. Если она прошла успешно, то пакет отправляется, в противном случае он отбрасывается.

Для пакета, направляемого по связующему дереву, RPF-проверка заключается в следующем:

1. Маршрутизатор определяет по таблице одноадресатной маршрутизации адрес источника и проверяет, поступил ли пакет на интерфейс обратного маршрута и не направляется ли он обратно к источнику.
2. Если пакет поступил на интерфейс, ведущий обратно к источнику, то RPF-проверка считается успешно завершенной, и пакет отправляется.
3. Если RPF-проверка завершилась неудачно, то пакет отбрасывается.

Пример неудачной RPF-проверки показан на рис. 45.10.

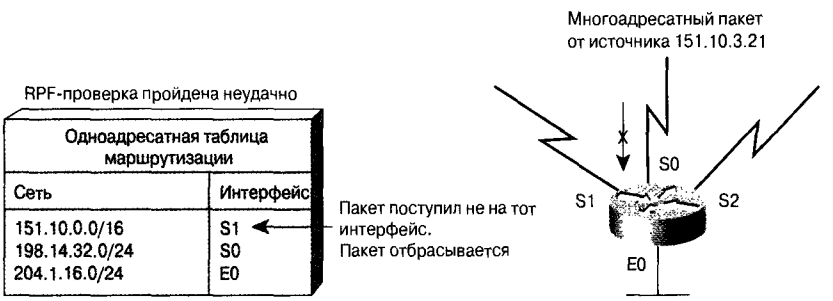


Рис. 45.10. Неудачная RPF-проверка

Многоадресатный пакет, поступивший от источника 151.10.3.21, получен на интерфейсе S0. Проверка таблицы одноадресатной маршрутизации показала, что этот маршрутизатор передает одноадресатные пакеты по адресу 151.10.3.21 через интерфейс S1. Поскольку пакет пришел на интерфейс S0, то он отбрасывается.

На рис. 45.11 показан пример успешно завершенной RPF-проверки.

На этот раз многоадресатный пакет пришел на интерфейс S1. По таблице одноадресатной маршрутизации маршрутизатор определил, что S1 является требуемым интерфейсом. RPF-проверка считается успешной и пакет пересылается получателю.

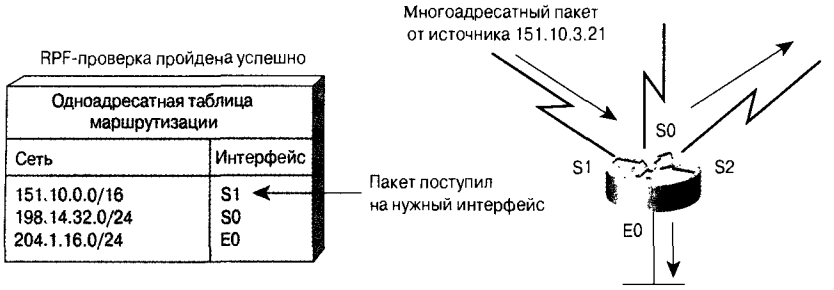


Рис. 45.11. RPF-проверка завершена успешно

Независимая от протокола многоадресатная рассылка

Независимая от протокола многоадресатная рассылка (Protocol-Independent Multicast — PIM) получила такое название, вследствие того, что она не зависит от IP-протокола маршрутизации. PIM может действовать независимо от того, какой протокол одноадресатной маршрутизации используется для заполнения таблиц маршрутизации — EIGRP, OSPF, BGP или статические маршруты. Протокол PIM использует для многоадресатной пересылки эту одноадресную маршрутную информацию и поэтому не зависит от IP-протокола. Несмотря на то, что PIM называют многоадресатным протоколом маршрутизации, на самом деле вместо построения полностью независимой таблицы многоадресатной маршрутизации он использует для обратной передачи таблицу одноадресатной маршрутизации. При использовании PIM, в отличие от других протоколов, маршрутизаторы не посылают и не принимают обновлений многоадресатных маршрутов.

Плотный режим протокола PIM

В *плотном режиме PIM (PIM Dense Mode — PIM-DM)* доставка данных многоадресатной рассылки по всей сети осуществляется методом выталкивания. Этот метод "грубой силы" по доставке данных получателям эффективен для некоторых приложений при условии, что активные получатели есть в каждой подсети.

Вначале протокол PIM-DM распространяет данные многоадресатной рассылки по всей сети. Маршрутизаторы, не имеющие соседей, расположенных в направлении передачи данных, отсекают эти нежелательные данные. Такой процесс повторяется каждые 3 минуты.

Механизм распространения и пресечения потоков данных является способом накопления маршрутизаторами информации о состоянии путем получения потока данных. Эти потоки данных содержат информацию об источнике и группе, так что маршрутизаторы, расположенные в направлении передачи данных, могут создавать собственные таблицы многоадресатной рассылки. Протокол PIM-DM поддерживает только деревья источника, т.е. структуры типа (S, G). Он не может быть использован для построения деревьев общего доступа.

Разреженный режим PIM

В *разреженном режиме PIM (PIM Sparse Mode — PIM-SM)* доставка данных многоадресатной рассылки осуществляется методом "втягивания". Данные передаются только в те сети, где есть активные источники, пославшие явный запрос на получение этих данных. Протокол PIM-SM описан в RFC 2362.

Для распространения информации об активных источниках в протоколе PIM-SM используется дерево общего доступа. В зависимости от конфигурации данные может оставаться в пределах дерева общего доступа или перейти на оптимизированное дерево источника. Последний из упомянутых вариантов работы протокола PIM-SM используется в маршрутизаторах Cisco по умолчанию. Данные начинают распространяться по дереву общего доступа, а потом маршрутизаторы, расположенные на его пути, определяют, есть ли лучший маршрут к источнику. Если существует лучший, более короткий маршрут, то выделенный (ближайший к получателю) маршрутизатор отправляет источнику сообщение о присоединении, и данные перенаправляются по этому маршруту.

Поскольку в протоколе PIM-SM, по крайней мере вначале, используется общее дерево доступа, в нем используются точки рандеву RP. Эти точки рандеву RP настраиваются администратором сети. Источники регистрируются в точке рандеву RP, после чего данные передаются получателям по дереву общего доступа. Если дерево общего доступа не является оптимальным маршрутом между источником и получателем, то маршрутизаторы динамически создают дерево от источника и прекращают передачу данных по дереву общего доступа. Таково стандартное поведение операционной системы IOS Cisco . Сетевые администраторы могут принудительно сохранить передачу данных по дереву общего доступа, используя опцию конфигурации (**`ip pim spt-threshold infinity`**).

Протокол PIM-SM легко масштабируется для сетей любого размера, в том числе и тех, где используются каналы WAN. Механизм явного присоединения предотвращает передачу нежелательных данных по глобальным каналам.

Разреженно-плотный режим

Корпорация Cisco разработала новый IP-интерфейс маршрутизатора, позволяющий выбирать между плотным и разреженным режимами. Такая необходимость возникла из-за изменения принципа передачи данных многоадресатной рассылки по протоколу PIM, которое стало очевидным в процессе развития этой технологии. Оказалось, что лучше выбирать режим — разреженный или плотный — для каждой группы, а не для каждого маршрутизатора. Такую возможность предоставляет разреженно-плотный режим.

Параметры разреженно-плотного режима настраиваются сетевым администратором. Он может назначить отдельным группам плотный или разреженный режим, в зависимости от того, доступна ли данной группе информация о точках рандеву RP. Если маршрутизатор имеет RP-информацию для группы, то для нее выбирается разреженный режим, в противном случае используется плотный режим.

Протокол MBGP

Протокол многопротокольного граничного шлюза (Multiprotocol Border Gateway Protocol — MBGP) позволяет провайдерам выбирать маршрутные префиксы для многоадресатных RPF-проверок. RPF-проверка является фундаментальным механизмом, используемым

маршрутизаторами для определения маршрутов, по которым деревья многоадресатной передачи доставляют многоадресатный контент от источников к получателям.

Протокол MBGP описан в RFC 2283, Multiprotocol Extensions for BGP4. Поскольку MBGP является расширением протокола BGP, он унаследовал от него весь административный аппарат, который провайдеры и пользователи привыкли использовать в среде внутридоменной маршрутизации, в том числе все средства фильтрации и управления маршрутизацией (в частности, маршрутные карты), применяемые при передаче данных между автономными системами AS. Поэтому при использовании MBGP любой внешний или внутренний сетевой протокол граничного шлюза BGP может применять различные BGP-расширения по управлению политиками для того, чтобы уточнить политику многоадресатной маршрутизации и пересылки.

В протоколе BGP4+ возникли два новых маршрутных атрибута — MP_REACH_NLRI и MP_UNREACH_NLRI. Благодаря им появился простой способ передачи двух вариантов маршрутной информации — одноадресатного и многоадресатного. Многоадресатные маршруты используются для построения многоадресатных связующих деревьев.

Главное преимущество протокола MBGP заключается в том, что объединенная сеть может поддерживать неконгруэнтные одно- и многоадресатные топологии. Если одно- и многоадресатные топологии конгруэнтны, то MBGP может поддерживать для каждой из них различные политики. Протокол MBGP представляет собой масштабируемый основанный на использовании политик протокол междоменной маршрутизации.

Протокол MSDP

В разреженном режиме модели PIM многоадресатные источники и получатели должны регистрироваться в своих локальных точках рандеву (Rendezvous Point — RP). В действительности в RP регистрируется ближайший к источникам и получателям маршрутизатор, однако точке рандеву RP известны все источники и получатели каждой конкретной группы. Однако точки рандеву RP не имеют информации об источниках, расположенных в других доменах. Изящным решением этой проблемы служит *протокол обнаружения многоадресатных источников (Multicast Source Discovery Protocol — MSDP)*. Протокол MSDP представляет собой механизм, который обеспечивает соединение между доменами PIM-SM и обмен информацией об активных источниках между точками рандеву RP. Когда RP в удаленном домене узнают об активных получателях, они могут передать эту информацию своим локальным получателям, что обеспечивает передачу многоадресатных данных между такими доменами. Привлекательным свойством MSDP является то, что он позволяет каждому домену иметь собственные точки рандеву RP, не зависящие от других доменов, но позволяющие передавать данные между доменами.

В каждом домене точка рандеву RP устанавливает сеанс одноранговой связи протокола MSDP с RP в других доменах или с граничными маршрутизаторами, ведущими к другим доменам, используя соединение TCP. Когда RP узнает о новом многоадресатном источнике в своем домене (путем обычного механизма регистрации протокола P M), она инкапсулирует первый пакет данных в сообщении об активности источника (Source Active — SA) и посылает SA всем одноранговым MSDP-партнерам. Каждый MSDP-партнер, получивший SA-сообщение, передает его дальше с использованием модифицированной RPF-проверки, пока это сообщение не будет получено всеми MSDP-маршрутизаторами объе-

диненной сети — теоретически всего многоадресатного Internet. Если MSDP-получателем является точка рандеву RP, у которой есть дерево (*, G) для группы, указанной в SA (то есть имеется получатель, заинтересованный в получении данной информации), то RP создает для источника дерево (S, G) и присоединяется к дереву кратчайших маршрутов для данного состояния источника. Инкапсулированные данные извлекаются и передаются по дереву общего доступа данной RP. Когда пакет будет получен последним маршрутизатором на пути к получателю, то последний узел также может присоединиться к дереву кратчайших маршрутов для данного источника. Точка рандеву RP источника периодически рассылает сообщения SA, куда входят все источники домена, к которому принадлежит RP. На рис. 45.12 показана передача данных между источником в домене A и получателем в домене E.

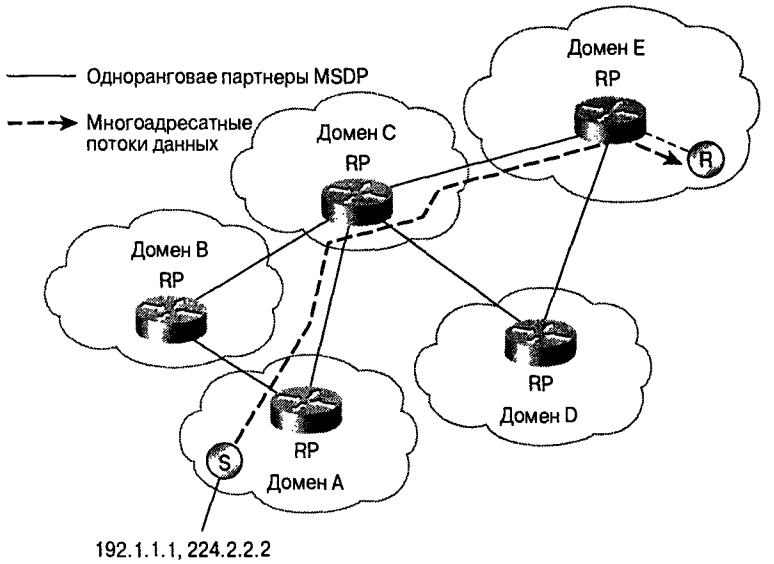


Рис. 45.12. Пример передачи данных по протоколу MSDP

Протокол MSDP был разработан для одноранговой обмена данными между провайдерами служб Internet (ISP). При обслуживании своих клиентов провайдерам ISP было желательно не зависеть от точек рандеву RP, поддерживаемых конкурирующими ISP. Протокол MSDP позволяет каждому ISP иметь собственную локальную точку рандеву RP, что не мешает ему посылать и получать данные многоадресатной рассылки по сети Internet.

Альтернативная и логическая точки рандеву

Использование альтернативных точек рандеву (anycast RP) представляет собой весьма полезное применение протокола MSDP. Конфигурирование альтернативных точек рандеву позволяет обеспечить отказоустойчивость и распределение нагрузки в пределах многоадресатного домена.

Для этого циклические интерфейсы двух или более RP конфигурируются с одним и тем же IP-адресом — например, 10.0.0.1 (рис. 45.13), длина которого должна составлять 32 бита. Все маршрутизаторы, расположенные в нисходящем направлении передачи

данных, должны быть сконфигурированы таким образом, чтобы адресом их локальной точки рандеву RP был адрес 10.0.0.1. При осуществлении IP-маршрутизации для каждого источника и получателя автоматически выбирается топологически ближайшая точка рандеву RP. Поскольку возможна ситуация, в которой источники используют одну RP, а получатели — другую, необходим способ обмена информацией об активных источниках между всеми точками рандеву. Для этого применяется протокол MSDP. Все RP конфигурируются таким образом, что они являются одноранговыми MSDP-устройствами. Каждая точка рандеву RP должна иметь информацию об активных источниках в области, принадлежащей другой RP. Если в одной из точек рандеву RP произойдет сбой, то произойдет конвергенция маршрутизации IP-адресов, и одна из оставшихся точек рандеву RP станет активной в обеих областях.

Примечание

В приведенном выше примере альтернативной RP используются IP-адреса из RFC 1918. Эти IP-адреса обычно блокируются на границах доменов и, следовательно, недоступны для других провайдеров Internet. Если нужно, чтобы эти RP были доступны из других доменов, то следует использовать другие IP-адреса.

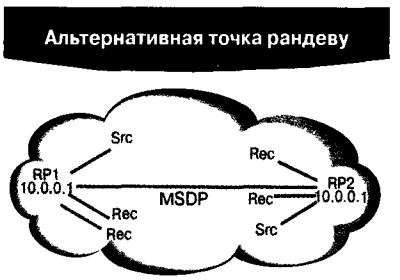


Рис. 45.13. Альтернативная точка рандеву

Примечание

Точки рандеву используются только для установки начального соединения между источником и получателями. После того как маршрутизаторы последнего перехода присоединятся к дереву кратчайших маршрутов, необходимость в этой RP отпадает.

Протокол MADCAP

Протокол динамического выделения клиентских групповых адресов (Multicast Address Dynamic Client Allocation Protocol — MADCAP) описан в RFC 2730 как протокол, позволяющий узлам динамически запрашивать выделение адресов многоадресатной рассылки у сервера MADCAP. Данная концепция во многом аналогична работе современного протокола DHCP и основана на модели "клиент/сервер".

Протокол MZAP

Протокол объявления границ многоадресатной зоны (Multicast-Scope Zone Announcement Protocol — MZAP) описан в RFC 2776 как протокол, который позволяет сетям автоматически обнаруживать административно выделенные зоны, относящиеся к определенной территории.

Протокол надежной многоадресатной рассылки

Протокол надежной многоадресатной рассылки (Pragmatic General Multicast — PGM) представляет собой надежный многоадресатный транспортный протокол для приложений, требующих упорядоченной, без дублирования, многоадресатной доставки данных от нескольких источников нескольким получателям. Протокол PGM гарантирует, что каждый получатель многоадресатной группы либо получит все пакеты данных путем передачи и повторной передачи, либо сможет определить потерю данных, не допускающую их восстановления.

Надежный транспортный протокол PGM должен быть сконфигурирован как у источников, так и у получателей. Источник поддерживает окно передачи исходящих пакетов данных и в случае получения отрицательного подтверждения (Negative AcKnowledgment — NAK) передает отдельные пакеты повторно. Элементы сети (маршрутизаторы) предотвращают взрывной рост передачи отрицательных подтверждений NAK в случае сбоя и способствуют эффективной повторной передаче данных соответствующим сетям.

Протокол PGM предназначен для многоадресатных приложений с повышенными требованиями к надежности передачи. Спецификация PGM не зависит от сетевого уровня. Разработанная корпорацией Cisco модификация Router Assist поддерживает PGM в IP.

Современная спецификация PGM представляет собой Internet-проект, представленный на Web-сайте IETF (http://www.ietf.org) под именем "PGM Reliable Transport Protocol".

Контрольные вопросы

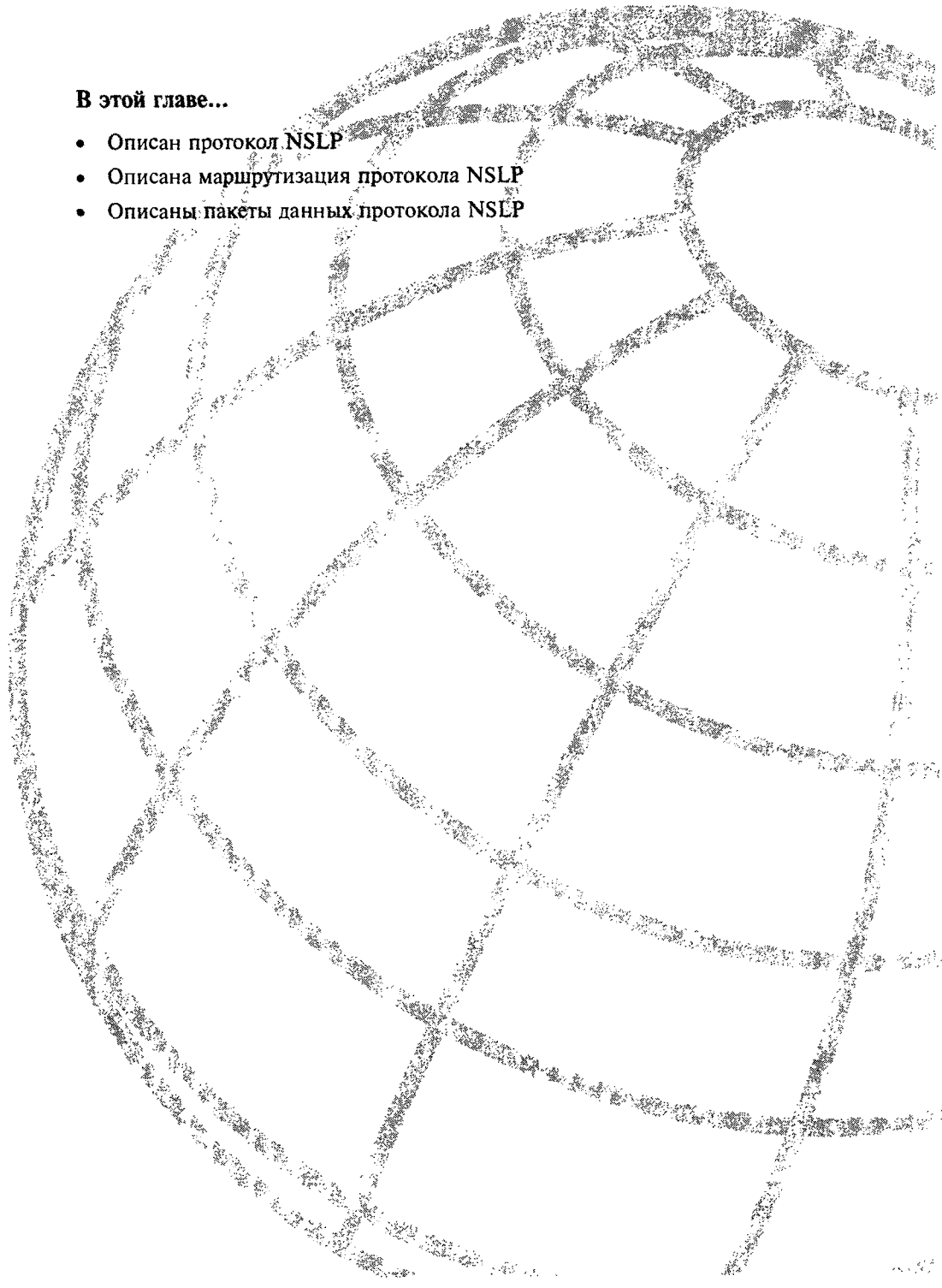
1. В каком диапазоне находятся доступные IP-адреса многоадресатной рассылки?
2. Каково назначение протокола IGMP?
3. Каковы преимущества протокола IGMP 2 по сравнению с IGMP 1?
4. Каковы возможные недостатки IGMP-прослушивания по сравнению с CGMP при использовании недорогих коммутаторов 2-го уровня ?
5. Каковы преимущества дерева кратчайших маршрутов (или дерева источника) по сравнению с деревом общего доступа?
6. Каковы преимущества дерева общего доступа?
7. Какую информацию использует маршрутизатор для RPF-проверки?
8. Почему независимая от протокола многоадресатная рассылка называется независимой?
9. В чем заключается основной недостаток протокола MBGP?
10. Как точки рандеву RP узнают об источниках от других RP при помощи MSDP?
11. Каково назначение альтернативных точек рандеву RP?

Дополнительные источники

- Williamson B. *Developing IP Multicast Networks.* Indianapolis: Cisco Press, 2000.
- http://www.cisco.com/warp/customer/105/48.html

В этой главе...

- Описан протокол NSLP
- Описана маршрутизация протокола NSLP
- Описаны пакеты данных протокола NSLP



Глава 46

Протокол NSLP

Введение

Протокол коммуникационных услуг в среде NetWare (NetWare Link-Services Protocol — NLSP) представляет собой протокол маршрутизации по состоянию канала, разработанный Novell для преодоления некоторых ограничений протокола маршрутной информации RIP (Routing Information Protocol — RIP) IPX и сопутствующего ему протокола анонсирования служб (Service Advertisement Protocol — SAP). Протокол NLSP основан на протоколе связи между промежуточными системами IS-IS (Intermediate System-to-Intermediate System — IS-IS) модели OSI и предназначен для замены протоколов RIP и SAP, первоначальных протоколов маршрутизации Novell, разработанных в те времена, когда объединенные сети были локальными и относительно небольшими. По существу, протокол RIP и SAP плохо приспособлены к современным глобальным объединенным сетям. В этой главе описывается маршрутизация и компоненты протокола NLSP.

По сравнению с RIP и SAP, протокол NLSP обеспечивает улучшенную маршрутизацию, эффективность и масштабируемость. Кроме того, NLSP-маршрутизаторы сохраняют обратную совместимость с RIP-маршрутизаторами. В NLSP-маршрутизаторах используется протокол надежной доставки, что делает ее гарантированной. Более того, NLSP облегчает принятие решения о выборе наилучшего маршрута, так как в NLSP-маршрутизаторах хранится полная карта сети, а не только информация о следующем узле, как в RIP-маршрутизаторах. Маршрутная информация передается только при изменении топологии, а не каждые 60 сек., независимо от того, изменялась топология или нет, как в RIP-маршрутизаторах. Кроме того, NLSP-маршрутизаторы посылают обновленную информацию о службах только тогда, когда эти службы изменяются, а не каждые 60 сек., как в протоколе SAP.

Протокол NLFS эффективен в нескольких областях. Особенно он полезен в глобальных сетях, благодаря сжатию заголовка IPX, за счет чего уменьшается размер пакетов. Кроме того, NLSP поддерживает многоадресатную рассылку и отправляет маршрутную информацию только другим NLSP-маршрутизаторам, а не всем устройствам, как RIP.

Кроме того, NLSP позволяет распределять нагрузку между параллельными маршрутами и обеспечивает улучшенную целостность соединений. Он периодически проверяет каналы на наличие связи и целостность маршрутной информации. При сбое канала NLSP переключается на альтернативный канал и обновляет базы данных топо-

логии сети в каждом узле после изменения связи между компонентами сети в любой зоне маршрутизации.

Что касается масштабируемости, то протокол NLSP поддерживает до 127 узлов (RIP — всего 15) и допускает иерархическую адресацию сетевых узлов, благодаря чему сеть может состоять из тысяч локальных сетей и серверов.

Иерархическая маршрутизация в NLSP

NLSP поддерживает иерархическую маршрутизацию для зоны, домена и глобальной объединенной сети. *Зона* представляет собой множество соединенных между собой сетей с одинаковым адресом зоны. *Домен* представляет собой множество зон, принадлежащих одной организации. *Глобальная объединенная сеть* представляет собой множество соседних доменов, принадлежащих, как правило, различным организациям. Зоны могут объединяться в домены маршрутизации, которые в свою очередь могут образовывать глобальную объединенную сеть.

NLSP поддерживает трехуровневую иерархическую маршрутизацию. Маршрутизатор 1-го уровня соединяет сетевые сегменты в пределах одной зоны маршрутизации. Маршрутизатор 2-го уровня соединяет зоны, а также служит маршрутизатором 1-го уровня в своей зоне. Маршрутизатор 3-го уровня соединяет домены и действует как маршрутизатор 2-го уровня в своем домене. На рис. 46.1 показаны три уровня маршрутизации NLSP.

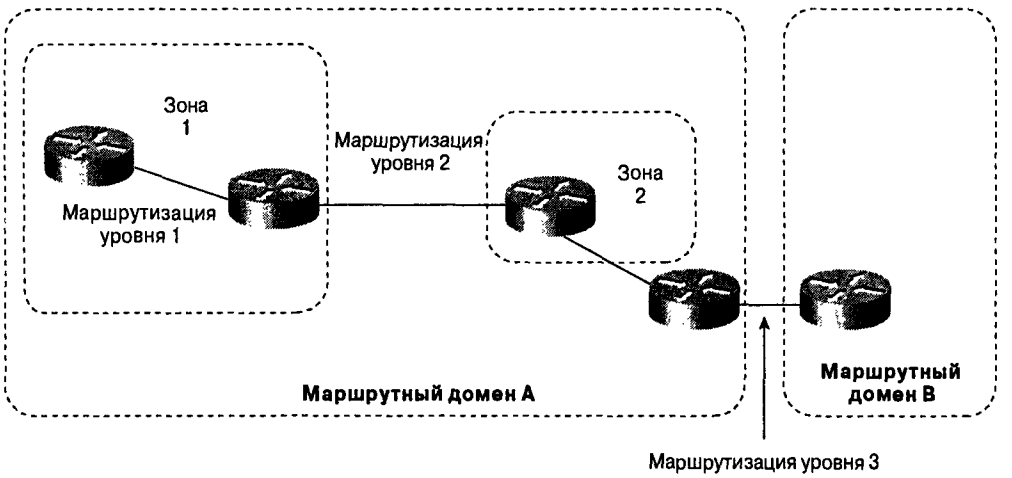


Рис. 46.1. NLSP определяет три уровня маршрутизации

Эффективность иерархической маршрутизации

Иерархическая маршрутизация упрощает процесс расширения сетей путем сокращения количества информации, которую каждый маршрутизатор должен хранить и обрабатывать для маршрутизации пакетов в домене. Маршрутизатор 1-го уровня должен хранить подробную информацию только о своей зоне и не должен запоминать информацию о состоянии каналов для каждого маршрутизатора и сегмента сети в домене. Для обмена данными с другими зонами маршрутизатор 1-го уровня обращается

к ближайшему маршрутизатору 2-го уровня. Для обмена информацией между зонами маршрутизаторы 2-го уровня рассылают оповещения о состоянии каналов только с адресами своих зон, а не со всей базой данных. Аналогичные действия выполняют маршрутизаторы 3-го уровня в отношении доменов.

Смежность в NLSP

Обмениваясь пакетами приветствия, маршрутизатор определяет доступность соседних маршрутизаторов и использует эту информацию для установки смежности. Смежность представляет собой запись о связи маршрутизатора с соседними маршрутизаторами и их атрибутах. Маршрутизатор хранит такие записи в своей базе данных смежности.

Процедура установки смежности зависит от того, в какой сети маршрутизатор устанавливает и поддерживает смежность — в глобальной или в локальной.

При установке смежности маршрутизатора в WAN прежде всего устанавливается соединение на канальном уровне (его особенности зависят от среды передачи). Затем маршрутизаторы обмениваются свойствами по протоколу IPX WAN 2 и определяют рабочие характеристики канала. После этого следует обмен пакетами приветствия, а затем маршрутизаторы обновляют свои базы данных смежности. Далее они обмениваются пакетами состояния канала (Link-State Packets — LSP), которые описывают состояние их каналов, и пакетами данных IPX по установленному каналу. Для обслуживания канала WAN в маршрутизаторе хранится переменная состояния, показывающая для каждой смежности, в каком состоянии находится канал — работает, не работает или инициализируется. Если маршрутизатор не получит отклика от соседнего маршрутизатора за период времени, определяемый таймером захвата, то он генерирует сообщение о том, что канал не работает, и удаляет смежность.

Пакеты приветствия WAN позволяют маршрутизаторам определить параметры друг друга, решить, принадлежат ли они к одной и той же зоне маршрутизации, и выяснить, работоспособны ли другие маршрутизаторы и каналы. Маршрутизатор посылает пакеты приветствия при начальной установке канала, по истечении времени, определяемого таймером или если содержание следующего пакета приветствия отличается от предыдущего, посланного этой системой (и если после отправки предыдущего пакета приветствия прошло не меньше одной секунды). Пакеты приветствия посылаются в течение всего времени, пока существует канал.

Установка новой смежности в глобальной сети

Типичная процедура создания глобального канала между двумя маршрутизаторами (A и B) начинается с того, что канал находится в нерабочем состоянии. Маршрутизатор A посылает по WAN пакет приветствия, где указывается, что канал с маршрутизатором B находится в нерабочем состоянии. Маршрутизатор B изменяет состояние соединения на инициализацию. Маршрутизатор B посылает маршрутизатору A по WAN пакет приветствия, где указывается, что канал находится в состоянии инициализации. Маршрутизатор A изменяет свое состояние канала на состояние инициализации и посылает маршрутизатору B по сети WAN пакет приветствия, где сообщается об этом. Маршрутизатор B изменяет свое состояние канала на рабочее и посылает по сети WAN пакет приветствия, отражающий это новое состояние. Наконец, маршрутизатор A изменяет свое состояние канала на рабочее.

Поддержка смежности в LAN

Если маршрутизатор поддерживает широковещательный канал, такой как 802.3 Ethernet или 802.5 Token Ring, то он начинает посылать сам и подтверждать получение пакетов приветствия от других маршрутизаторов LAN, а также начинает процесс выбора назначенного маршрутизатора.

Назначенный маршрутизатор хранит базу данных состояний каналов всей LAN, принимает решения о маршрутизации и генерирует пакеты LSP для всей LAN. Это обеспечивает сохранение разумных размеров базы данных состояний каналов, которую создает и поддерживает каждый маршрутизатор.

Периодически маршрутизатор посылает в LAN многоадресатный пакет приветствия. Маршрутизатор с наивысшим приоритетом (настраиваемый параметр) становится назначенным маршрутизатором 1-го уровня в LAN. В случае совпадения приоритетов предпочтение оказывается маршрутизатору с более высоким MAC-адресом.

Отправка пакетов приветствия в LAN

Пакеты приветствия позволяют маршрутизаторам на широковещательных каналах идентифицировать другие маршрутизаторы 1-го уровня на этих каналах в той же зоне маршрутизации. Пакеты посылаются сразу после установки канала по специальному групповому адресу. Маршрутизаторы "прослушивают" этот адрес для выявления поступающих пакетов приветствия.

Функционирование NLSP

Маршрутизатор NLSP извлекает информацию из базы данных смежности и добавляет к ней информацию, полученную локально. С помощью этой информации маршрутизатор конструирует пакет состояния канала (Link-State Packet — LSP), где описываются его ближайшие соседи. Все пакеты LSP, построенные всеми маршрутизаторами в данной зоне маршрутизации, образуют базу данных состояния каналов этой зоны.

Спецификация NLSP предусматривает наличие на маршрутизаторах синхронизированных копий базы данных состояний каналов. База данных состояний каналов синхронизируется путем надежного распространения LSP-пакетов в зоне маршрутизации, когда маршрутизатор замечает изменение топологии. Есть два метода распространения точной информации об изменении топологии: лавинное распространение и подтверждение получения.

Лавинное распространение начинается в том случае, если маршрутизатор обнаруживает изменения в топологии. Маршрутизатор конструирует новый LSP-пакет и передает его всем соседним маршрутизаторам. Такие пакеты являются направленными пакетами в WAN и многоадресатными в LAN. Получив LSP-пакет, маршрутизатор по его порядковому номеру определяет, новее ли данный пакет копии, хранящейся в базе данных маршрутизатора. Если это так, то маршрутизатор передает пакет дальше своим соседям (за исключением того канала, откуда был получен LSP).

Процесс подтверждения приема различен для LAN и WAN. В WAN маршрутизатор получает LSP-ответы с подтверждением. В LAN явного подтверждения не происходит, но назначенный маршрутизатор периодически осуществляет многоадресатную рассылку пакета, называемого полным пакетом порядковых номеров (Complete Sequence Number Packet — CSNP), где содержатся все идентификаторы и порядковые

номера пакетов LSP, содержащихся в базе данных зоны. Это позволяет остальным маршрутизаторам определить, не нарушилась ли синхронизация их копии базы данных с назначенным маршрутизатором.

Иерархическая адресация протокола NLSP

NLSP поддерживает схему иерархической адресации. Каждая зона маршрутизации идентифицируется двумя 32-разрядными величинами: сетевым адресом и маской. Эта пара чисел называется адресом зоны. Ниже приведен пример шестнадцатеричного адреса зоны:

- **01234500** — сетевой адрес данной зоны маршрутизации. Каждый номер сети в этой зоне начинается с идентификационного кода 012345.
- **FFFFFF00** — маска, которая определяет, сколько сетевых адресов ссылаются на саму зону и сколько — на отдельные сети, принадлежащие этой зоне.

В данном примере адреса зоны первые 24 бита (012345) определяют зону маршрутизации, а оставшиеся 8 битов — номера отдельных сетей в этой зоне (например 012345AB, 012345C1, 01234511). Данная концепция адресации отображена на рис. 46.2, где представлены три сети, принадлежащие одной зоне.

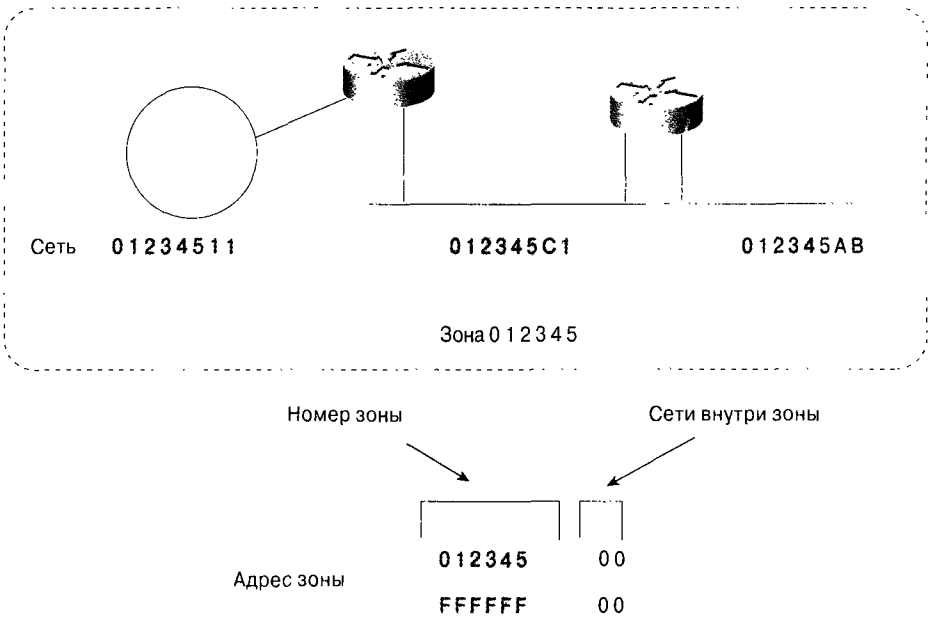


Рис. 46.2. Адреса NLSP состоят из адреса сети и маски

Зона маршрутизации может иметь столько же адресов, что и три зоны с разными масками. Обладание несколькими адресами позволяет реорганизовывать зону маршрутизации без перерывов в работе. В домене может использоваться любая комбинация адресов зон.

Пакеты приветствия NLSP

Существует два типа пакетов приветствия NLSP: пакеты приветствия WAN и пакеты приветствия LAN 1-го уровня.

Пакет приветствия WAN

Поля пакета приветствия WAN показаны на рис. 46.3.

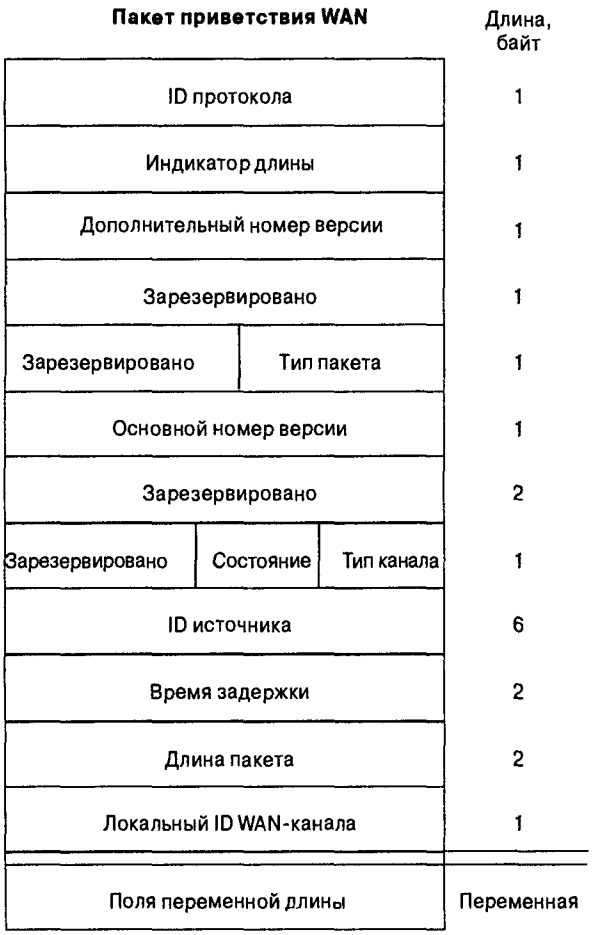


Рис. 46.3. Пакет приветствия WAN

Поля пакета приветствия WAN

Ниже описаны поля пакета приветствия WAN, показанные на рис. 46.3.

- **ID протокола.** Уровень маршрутизации NLSP, шестнадцатеричное число 0x83.
- **Индикатор длины.** Количество байтов в фиксированной части заголовка.

- **Дополнительный номер версии.** Одно из возможных десятичных значений. При приеме игнорируется.
- **Зарезервировано.** Не содержит десятичных значений. При приеме игнорируется.
- **Тип пакета.** Длина поля — 5 битов. 17 возможных десятичных значений.
- **Основной номер версии.** Единственное возможное десятичное значение.
- **Состояние.** Длина поля — 2 бита. Состояние маршрутизатора (0 — работает, 1 — инициализируется, 2 — не работает).
- **Тип канала** (Cct type). Длина поля — 2 бита. Это поле может принимать одно из следующих значений.
  - — **0** — зарезервированное значение; весь пакет игнорируется.
  - — **1** — только маршрутизация 1-го уровня.
  - — **2** — только маршрутизация 2-го уровня. (Отправитель использует этот канал для маршрутизации 2-го уровня.)
  - — **3** — уровни 1 и 2. (Отправитель является маршрутизатором 2-го уровня и использует данное соединение для передачи данных уровней 1 и 2.)
- **ID источника.** Идентификатор маршрутизатора-отправителя.
- **Таймер.** Значение таймера занятости в секундах, которое используется для маршрутизатора-отправителя.
- **Длина пакета.** Полная длина пакета в байтах, включая заголовок NLSP.
- **Локальный ID WAN-канала.** Уникальный идентификатор, присваиваемый каналу, создаваемому маршрутизатором.
- **Поля переменной длины.** Несколько дополнительных полей.

Пакеты приветствия NLSP LAN

Поля пакета приветствия 1-го уровня для LAN показаны на рис. 46.4.

Поля пакета приветствия 1-го уровня LAN

Ниже описаны поля пакета приветствия 1-го уровня LAN, показанные на рис. 46.4.

- **ID протокола.** Уровень маршрутизации NLSP, шестнадцатеричное число 0x83.
- **Индикатор длины.** Количество байтов в фиксированной части заголовка (до поля LAN ID включительно).
- **Дополнительный номер версии.** Одно из возможных десятичных значений. При приеме игнорируется.
- **Зарезервировано.** Не содержит десятичных значений. При приеме игнорируется.
- **Тип пакета.** Длина поля — 5 битов. 15 возможных десятичных значений.
- **Основной номер версии.** Единственное возможное десятичное значение.
- **NM** (No multicast, не многоадресатный). Длина поля — 1 бит. Если его значение — 1, то отправитель пакета не может получать данные с многоадресатной рассылки (и последующие пакеты для этой LAN должны быть широковещательными).

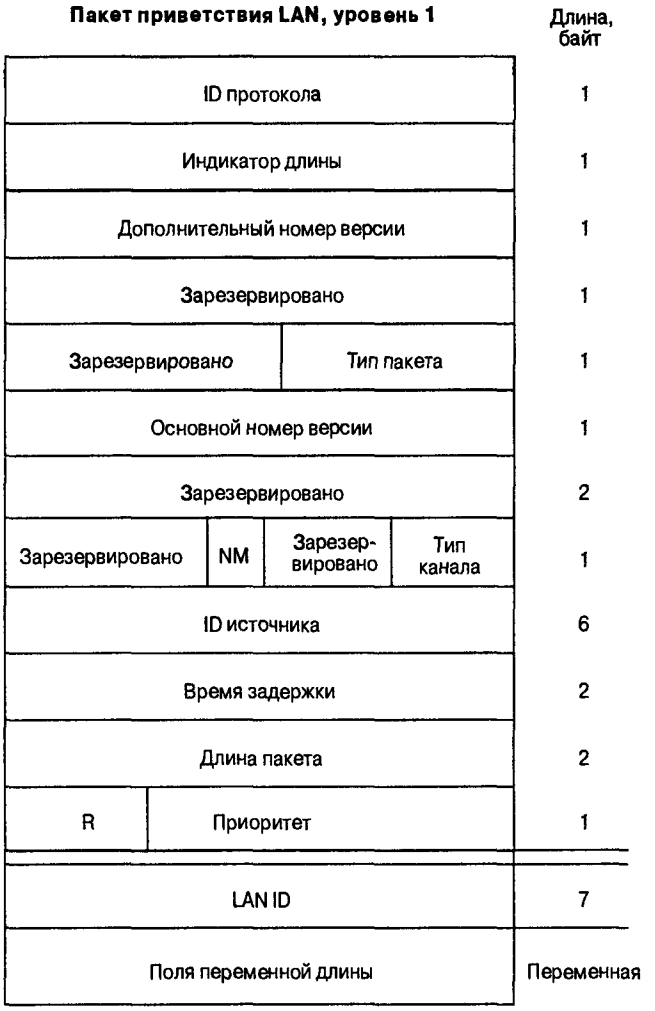


Рис. 46.4. Пакет приветствия 1-го уровня LAN

- **Тип канала** (Cct type). Длина поля — 2 бита. Это поле может принимать одно из следующих значений.
  - — **0** — зарезервированное значение; весь пакет игнорируется.
  - — **1** — только маршрутизация 1-го уровня.
  - — **2** — только маршрутизация 2-го уровня. (Отправитель использует этот канал для маршрутизации 2-го уровня.)
  - — **3** — уровни 1 и 2. (Отправитель является маршрутизатором 2-го уровня и использует данное соединение для передачи данных уровней 1 и 2.)
- **ID источника.** Идентификатор маршрутизатора-отправителя.
- **Таймер.** Значение таймера занятости в секундах, которое используется для маршрутизатора-отправителя.

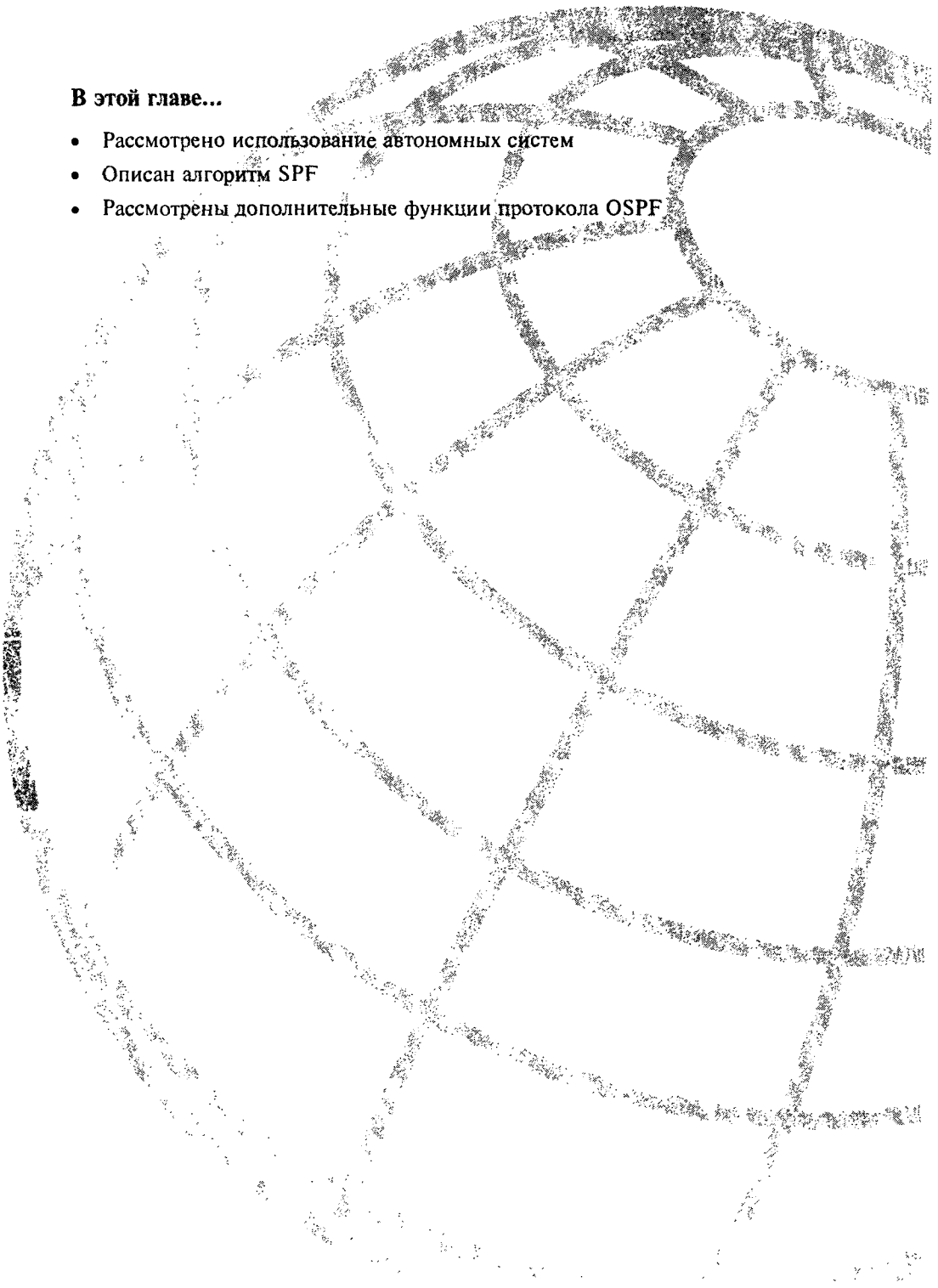
- **Длина пакета.** Полная длина пакета в байтах, включая заголовок NLSP.
- **R.** Не содержит возможных десятичных значений. При приеме игнорируется.
- **Приоритет.** Длина поля — 7 битов. Содержит значение приоритета, присваиваемое назначенному маршрутизатору 1-го уровня LAN (чем больше это значение, тем выше приоритет).
- **LAN ID.** Идентификатор (6 байтов) назначенного маршрутизатора 1-го уровня LAN, за которым следует поле, значение которого определяется этим маршрутизатором.
- **Поле переменной длины.** Несколько дополнительных полей.

Контрольные вопросы

1. Для чего предназначен маршрутизатор 2-го уровня в схеме иерархической маршрутизации NLSP?
2. В течение какого времени посылаются пакеты приветствия после того, как маршрутизатор инициализирован и начал работать?
3. Какой тип LSP посылается по WAN — одноадресатный или многоадресатный?

В этой главе...

- Рассмотрено использование автономных систем
- Описан алгоритм SPF
- Рассмотрены дополнительные функции протокола OSPF



Глава 47

Протокол OSPF

Протокол выбора кратчайшего пути OSPF (Open Shortest Path First — OSPF) представляет собой протокол маршрутизации, разработанный для IP-сетей рабочей группой Internet Engineering Task Force (IETF) по протоколам внутреннего шлюза. Эта рабочая группа была образована в 1988 г. для разработки протокола IGP на базе алгоритма выбора кратчайшего маршрута (Shortest Path First — SPF) в целях использования в сети Internet. Как и в случае с протоколом IGRP, причиной создания OSPF послужило то, что к середине 1980-х гг. возможности протокола RIP стали недостаточными для обслуживания крупных гетерогенных объединенных сетей. В настоящей главе описывается среда маршрутизации OSPF, лежащий в ее основе алгоритм маршрутизации и основные компоненты протокола OSPF.

Протокол OSPF явился результатом научных исследований в нескольких направлениях и его базой являются алгоритм SPF, разработанный для ARPANET в 1978 г. компанией Bolt, Beranek и Newman (BBN), исследования д-ра Радиа Перлмана (Dr. Radia Perlman) в области отказоустойчивой широковещательной рассылки маршрутной информации (1988), разработки компании BBN по зональной маршрутизации (1986) и одна из первых версий протокола маршрутизации IS-IS OSI.

Протокол OSPF имеет две основные характеристики. Первая из них заключается в том, что это открытый протокол, т.е. его спецификация общедоступна. Спецификация OSPF опубликована в RFC 1247. Второй особенностью OSPF является то, что в его основе лежит алгоритм SPF, который иногда называют алгоритмом Дейкстра (Dijkstra) по имени автора.

OSPF является протоколом маршрутизации по состоянию канала. Это означает, что он требует отправки объявлений о состоянии канала (Link-State Advertisements — LSA) всем остальным маршрутизаторам данной иерархической области. В сообщения LSA протокола OSPF входит информация о подключенных интерфейсах, использованных метриках и других переменных. По мере того как маршрутизаторы OSPF накапливают сведения о состоянии канала, они используют алгоритм SPF для расчета кратчайшего маршрута к каждому узлу.

Являясь алгоритмом маршрутизации по состоянию канала, OSPF отличается от протоколов RIP и IGRP, которые являются дистанционно-векторными протоколами маршрутизации (используют маршрутизацию по вектору расстояния). Маршрутизаторы, использующие алгоритм маршрутизации по вектору расстояния, включают в сообщения об обновлении маршрутов, отправляемые соседним маршрутизаторам, свою таблицу маршрутизации — всю или частично.

Иерархия маршрутизации

В отличие от протокола RIP, OSPF может работать в иерархической системе. Самым крупным объектом в этой иерархии является автономная система (Autonomous System — AS). AS представляет собой набор сетей с общим администрированием и единой стратегией маршрутизации. Хотя OSPF является протоколом маршрутизации внутри автономной системы AS (т.е. протоколом внутреннего шлюза), он также может принимать маршруты от других AS и отправлять им свои маршруты.

Автономную систему AS можно разделить на несколько зон (area). Зона представляет собой группу смежных сетей и подключенных к ним узлов. Маршрутизаторы с несколькими интерфейсами могут принадлежать нескольким зонам. На таких маршрутизаторах, называемых граничными (Area Border Router), хранятся отдельные топологические базы данных для каждой зоны.

В топологической базе данных хранится общая схема сети по отношению к маршрутизаторам. В ней также содержится набор сообщений LSA, полученных от всех маршрутизаторов данной зоны. Поскольку маршрутизаторы одной зоны пользуются одной и той же информацией, их топологические базы данных одинаковы.

Доменом иногда называют часть сети, в которой у всех маршрутизаторов топологическая база данных одинакова. Термин "домен" часто употребляется как синоним термина "автономная система".

Топология зоны является невидимой для устройств, находящихся вне этой зоны. Поддерживая отдельные топологии зон, OSPF позволяет уменьшить объем передаваемых данных маршрутизации.

Разделение на зоны приводит к использованию двух различных типов маршрутизации OSPF, в зависимости от того, находятся ли источник и получатель в одной или в разных зонах. В первом случае имеет место внутризонная, во втором — межзонная маршрутизация.

Распространение маршрутной информации между зонами происходит по магистрали OSPF. В состав магистрали OSPF входят все граничные маршрутизаторы, а также сети, которые не принадлежат полностью ни одной из зон, и подключенные к ним маршрутизаторы. На рис. 47.1 представлен пример объединенной сети с несколькими зонами.

На этом рисунке маршрутизаторы 4, 5, 6, 10, 11 и 12 образуют магистраль. Если узел H1 зоны 3 отправит пакет узлу H2 зоны 2, то пакет будет отправлен маршрутизатору 13, который передает его маршрутизатору 12, а тот, в свою очередь, отправляет его маршрутизатору 11. Маршрутизатор 11 передает пакет по магистрали граничному маршрутизатору 10, который отправляет пакет через два внутренних маршрутизатора этой зоны (маршрутизаторы 9 и 7), после чего он попадает к узлу H2.

Сама магистраль также является зоной OSPF, поэтому все магистральные маршрутизаторы используют для обработки маршрутной информации, передаваемой по магистрали, те же процедуры и алгоритмы, которые используются маршрутизаторами других зон. Топология магистрали невидима для внутренних маршрутизаторов обычных зон, точно так же, как топологии зон невидимы для магистрали.

Зоны могут быть определены таким образом, что магистраль не будет непрерывной. В этом случае непрерывность магистрали обеспечивается виртуальными каналами. Такие каналы создаются между любыми магистральными маршрутизаторами, которые одновременно поддерживают соединение с обычными зонами и функционируют так, как если бы были обычными каналами.

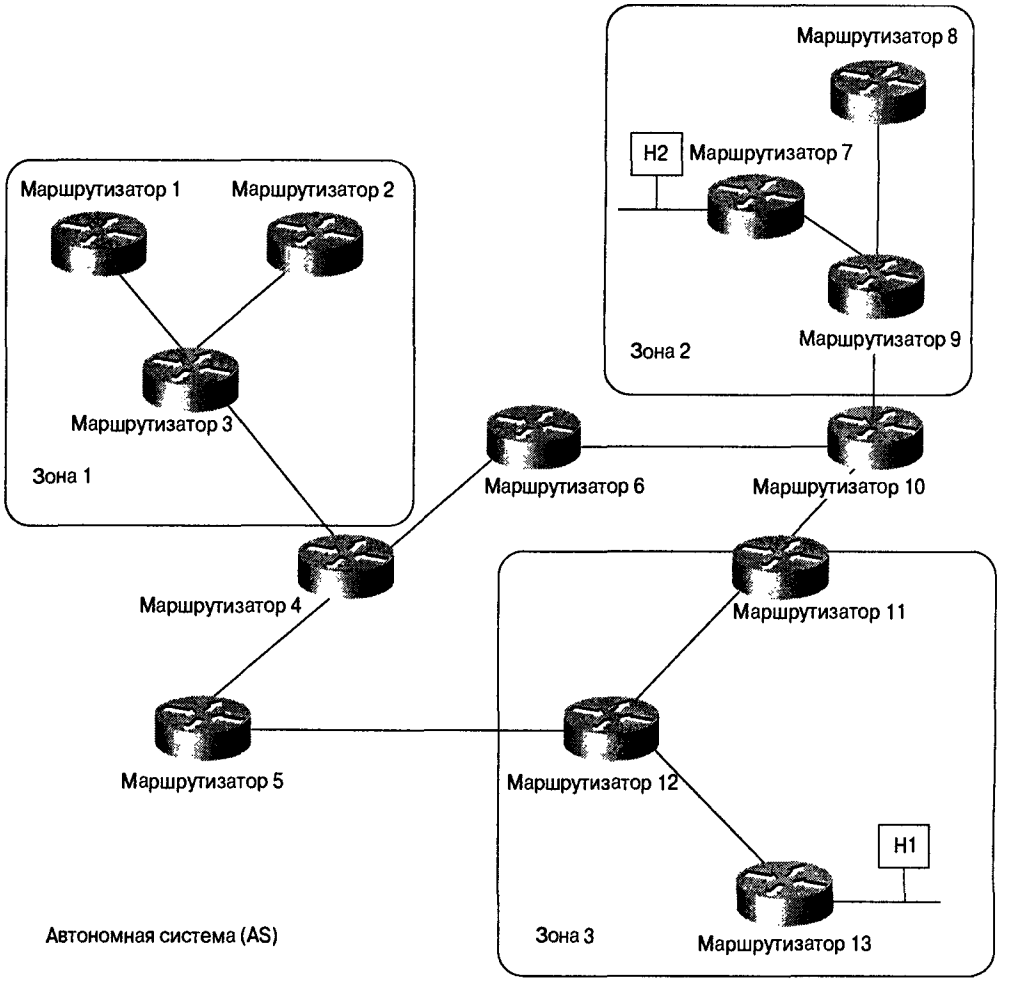


Рис. 47.1. Автономная система в сети OSPF состоит из нескольких зон, соединенных маршрутизаторами

Граничные маршрутизаторы AS, использующие OSPF, узнают о внешних маршрутизаторах при помощи протоколов внешнего шлюза, таких как протокол внешнего шлюза (Exterior Gateway Protocol — EGP), протокол граничного шлюза (Border Gateway Protocol — BGP) или через информацию о конфигурации. Более подробно эти протоколы рассматриваются в главе 41, "Протокол BGP".

Алгоритм SPF

Алгоритм выбора кратчайшего пути (Shortest Path First — SPF) является основой функционирования протокола OSPF. При включении маршрутизатор SPF инициализирует свои структуры данных, относящиеся к протоколу маршрутизации, а затем ожидает сообщений от протоколов низшего уровня о работоспособности его интерфейсов.

Получив такие подтверждения, маршрутизатор использует протокол приветствия OSPF (Hello protocol) для того, чтобы получить данные о соседних маршрутизаторах. Под соседними маршрутизаторами понимаются маршрутизаторы, интерфейсы которых подключены к общей сети. Маршрутизатор отправляет своим соседям пакеты приветствия и получает такие же пакеты от них. Кроме передачи информации о соседних маршрутизаторах, пакеты приветствия также служат подтверждением работоспособности маршрутизатора, сообщая другим маршрутизаторам, что отправитель пакета работоспособен.

В сетях с множественным доступом (поддерживающих более двух маршрутизаторов) протокол приветствия выбирает назначенный маршрутизатор и резервный назначенный маршрутизатор. Помимо других функций, назначенный маршрутизатор генерирует LSA-сообщения для всей сети множественного доступа. Благодаря назначенным маршрутизаторам уменьшается объем передаваемых по сети данных и размер топологической базы данных.

Если базы данных о состоянии канала двух соседних маршрутизаторов синхронизированы, то такие маршрутизаторы называются смежными. В сетях с множественным доступом назначенный маршрутизатор определяет, какие маршрутизаторы должны стать смежными, и их топологические базы данных попарно синхронизируются. Смежные маршрутизаторы управляют распределением пакетов протокола маршрутизации, которые отправляются и принимаются только между смежными маршрутизаторами.

Каждый маршрутизатор периодически рассылает сообщения LSA с информацией о смежных с ним маршрутизаторах и об изменении состояния маршрутизатора. Сравнение отношений смежности маршрутизаторов с состоянием канала позволяет быстро обнаружить неработающие маршрутизаторы и в внести в топологию сети соответствующие изменения. По топологической базе данных, генерируемой на основе полученных сообщений LSA, маршрутизатор рассчитывает дерево кратчайших маршрутов, корнем которого он является. В свою очередь, дерево кратчайших маршрутов позволяет создать таблицу маршрутизации.

Формат пакета

Все пакеты OSPF начинаются с 24-байтового заголовка, показанного на рис. 47.2.

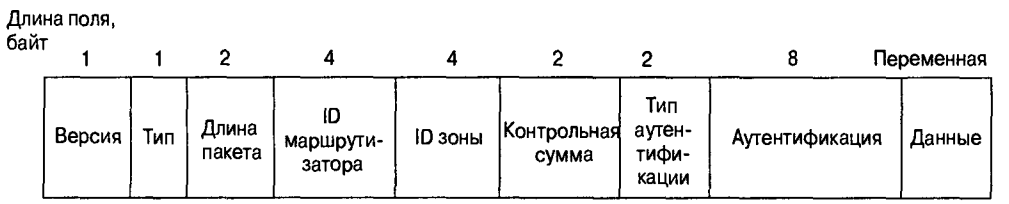


Рис. 47.2. Пакет OSPF содержит девять полей

Ниже описаны поля заголовка, показанные на рис. 47.2.

- **Версия.** Используемая версия **OSPF.**
- **Тип.** Один из описанных ниже типов пакета OSPF.
  - **Приветствие.** Устанавливает и поддерживает соединение между соседними маршрутизаторами.

— **Описание базы данных.** Описывает содержимое топологической базы данных. Обмен этими пакетами производится при инициализации отношений смежности.

— **Запрос о состоянии канала.** Запрашивает часть базы данных топологии соседних маршрутизаторов. Обмен этими пакетами производится после того, как маршрутизатор обнаружит (по пакетам описания базы данных), что часть его топологической базы данных устарела.

— **Обновление состояния канала.** Отвечает на пакеты запроса о состоянии канала. Эти сообщения также используются для регулярного распространения сообщений LSA. В одном пакете обновления состояния канала может содержаться несколько LSA.

— **Подтверждение состояния канала.** Подтверждает пакеты обновления состояния канала.

- **Длина пакета.** Длина пакета в байтах, включая заголовок OSPF.
- **ID маршрутизатора.** Идентифицирует источник пакета.
- **ID зоны.** Идентифицирует зону, которой принадлежит пакет. Все пакеты OSPF связаны с определенной зоной.
- **Контрольная сумма.** Проверяет содержимое всего пакета для выявления потенциальных повреждений при передаче.
- **Тип аутентификации.** Любой обмен данными по протоколу OSPF проводится с аутентификацией. Тип аутентификации определяется для каждой зоны.
- **Аутентификация.** Информация аутентификации.
- **Данные.** Инкапсулированная информация высшего уровня.

Дополнительные функции протокола OSPF

Дополнительными функциями OSRF являются маршрутизация по нескольким маршрутам по принципу равных оценок (equal cost), и маршрутизация на базе запросов типа обслуживания (Type of Service — ToS) высшего уровня. Маршрутизация на базе ToS поддерживает те протоколы высшего уровня, которые позволяют задать конкретный тип обслуживания. Например, приложение может объявить некоторые данные как срочные. Если в распоряжении OSPF есть каналы с высоким приоритетом, то они могут быть использованы для передачи срочных дейтаграмм.

OSPF поддерживает одну и более метрик. Если используется только одна метрика, то она считается произвольной и ToS не поддерживается. Если используется несколько метрик, то ToS может обеспечиваться отдельными метриками (и, следовательно, отдельной таблицей маршрутизации) для каждой из восьми комбинаций, образованной тремя битами ToS протокола IP (битом задержки, битом пропускной способности и битом надежности). Например, если биты ToS IP задают малую задержку, низкую производительность и высокую надежность, то протокол OSPF вычисляет маршруты ко всем получателям на основании этого типа обслуживания ToS.

В адрес каждого объявленного получателя включаются маски IP-подсети, что позволяет использовать маски подсети переменной длины. С помощью масок подсети

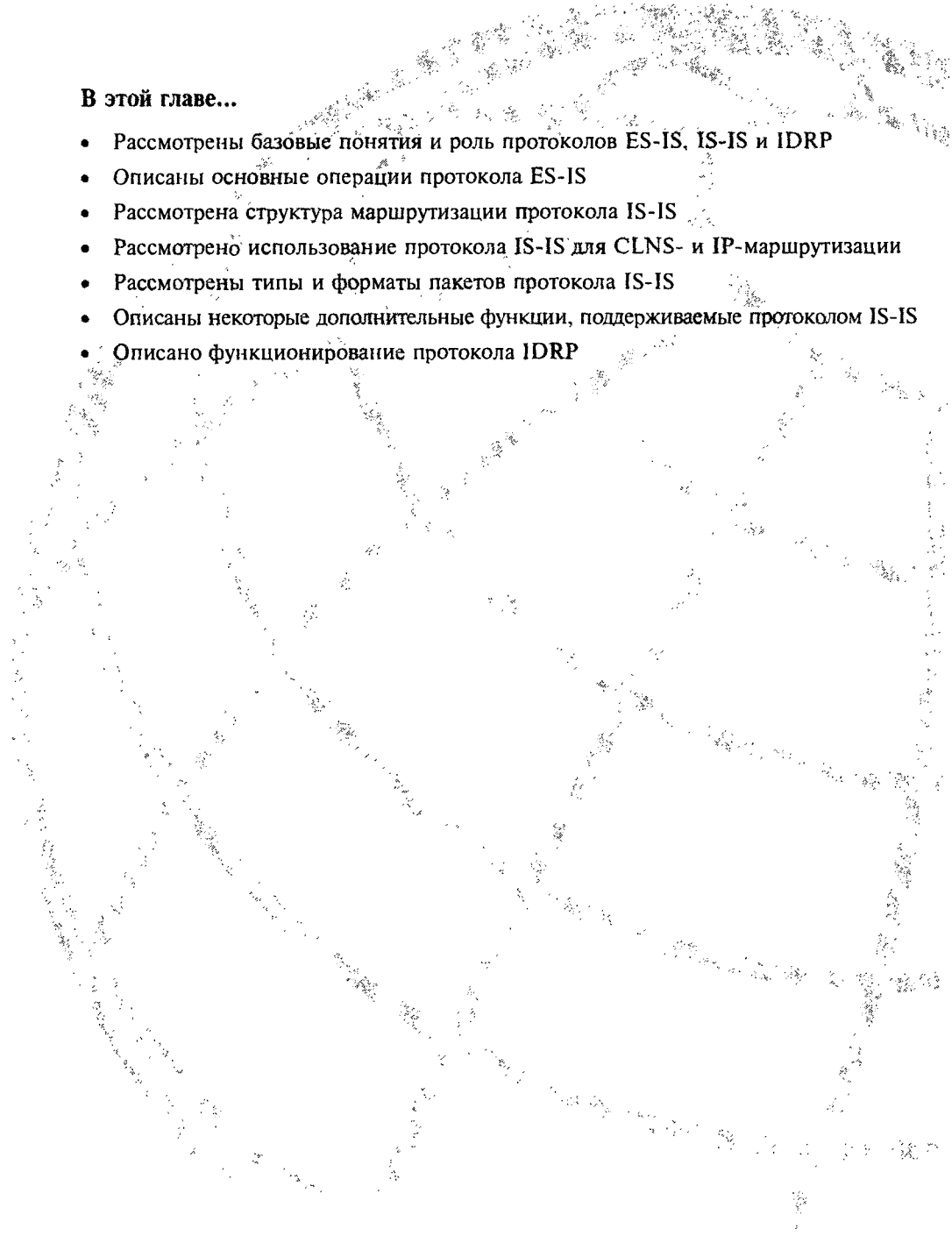
переменной длины можно разбить IP-сеть на несколько подсетей разных размеров, что предоставляет сетевым администраторам дополнительные возможности по выбору конфигурации сети.

Контрольные вопросы

1. Можно ли при использовании OSPF соединить две зоны, если интерфейс с зоной 0 есть только у одной AS?
2. Зона 0 содержит пять маршрутизаторов (A, B, C, D и E), а зона 1 — три (R, S и T). О каких маршрутизаторах известно маршрутизатору T, если маршрутизатор S является граничным?

В этой главе...

- Рассмотрены базовые понятия и роль протоколов ES-IS, IS-IS и IDRP
- Описаны основные операции протокола ES-IS
- Рассмотрена структура маршрутизации протокола IS-IS
- Рассмотрено использование протокола IS-IS для CLNS- и IP-маршрутизации
- Рассмотрены типы и форматы пакетов протокола IS-IS
- Описаны некоторые дополнительные функции, поддерживаемые протоколом IS-IS
- Описано функционирование протокола IDRP



Глава 48

Протоколы маршрутизации OSI

Введение

В основе протокола взаимодействия промежуточных систем (Intermediate System-to-Intermediate System — IS-IS) лежит технология, разработанная корпорацией Digital (Digital Equipment Corporation) для сетей DECnet/OSI (DECnet Phase V). Первоначально протокол IS-IS предназначался для маршрутизации в сетях протокола сетевого обслуживания без установки соединения (Connectionless Network Protocol — CLNP). Впоследствии была разработана версия этого протокола, поддерживающая как сети CLNP, так и IP-сети; обычно ее называют объединенным протоколом IS-IS (Integrated IS-IS) или Dual IS-IS.

Протоколы маршрутизации OSI описаны в нескольких документах Международной организации стандартизации (International Organization for Standardization — ISO), в том числе в ISO 10589 (описание протокола IS-IS). "Движущей силой" стандартизации протокола IS-IS, выполненной ISO, был Комитет по сетевым и транспортным протоколам (X3S3.3) при Национальном институте стандартизации США (American National Standards Institute — ANSI). Другими документами ISO являются стандарты ISO 9542 (описание протокола ES-IS) и ISO 10747 (описание IDRP).

Организация ISO разработала полный набор протоколов маршрутизации для использования в стеке протоколов OSI. Этот набор включает в себя протокол взаимодействия конечной системы с промежуточной системой (End System–to–Intermediate System — ES-IS), протокол IS-IS и протокол междоменной маршрутизации (Interdomain Routing Protocol — IDRP). В настоящей главе описаны основные операции каждого из этих протоколов. Также рассмотрена специфическая для OSI-маршрутизации терминология и приведен обзор операций маршрутизации. Описано расширение протокола IS-IS, позволяющее поддерживать не только службу сети без установки соединения (Connectionless Network Service — CLNP), но также и IP-сети. Это расширение вводит новые функции, такие как обход "черных дыр" и перераспределение потоков MPLS.

Терминология OSI

В сетях OSI используется несколько специфических терминов, таких как "конечная система" (End System — ES), относящийся к любому немаршрутизируемому узлу сети, и термин "промежуточная система" (Intermediate System — IS), относящийся к маршру-

тизаторам. Эти термины образуют основу OSI-протоколов ES-IS и IS-IS. Протокол ES-IS позволяет конечным и промежуточным системам распознать друг друга, а протокол IS-IS обеспечивает маршрутизацию между промежуточными системами.

Другими важными терминами OSI являются понятия зоны, домена, маршрутизации уровня 1 и маршрутизации уровня 2. Под зоной (area) понимают группу смежных сетей и связанных с ней узлов. Границы зоны определяются сетевым администратором или менеджером. Связанные между собой зоны называются доменом (domain). Домены маршрутизации обеспечивают связь между всеми принадлежащими им конечными системами. Под маршрутизацией уровня 1 понимается маршрутизация в пределах зон уровня 1, а под маршрутизацией уровня 2 — маршрутизация между зонами уровня 1. На рис. 48.1 показано, как связаны между собой зоны и домены, а также проиллюстрированы уровни маршрутизации между ними.

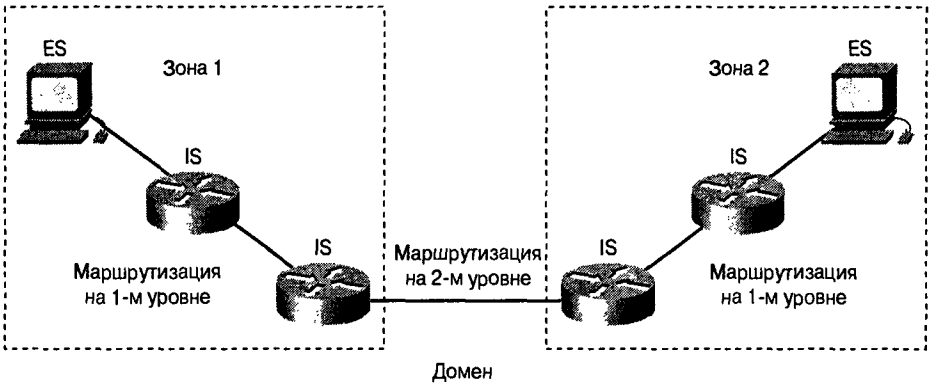


Рис. 48.1. Крупные домены делятся на зоны, связь между которыми осуществляется посредством маршрутизации уровня 2

Обзор операций маршрутизации протокола OSI

Каждая конечная система ES находится в некоторой зоне. Маршрутизация OSI начинается тогда, когда конечная система ES обнаруживает ближайшую промежуточную систему ES, прослушивая пакеты сообщений приветствия промежуточных систем (IS hello — ISH). В случае, когда конечной системе ES требуется послать пакет другой системе ES, она отправляет этот пакет одной из систем IS непосредственно подсоединенной к ней сети. После этого маршрутизатор просматривает адрес получателя и пересылает пакет по наилучшему маршруту. Если ES пункта назначения находится в той же самой подсети, то локальная система IS узнает об этом, прослушивая сообщения приветствия ES-системы, и пересылает пакет соответствующим образом. IS-система может также отправить отправителю сообщение о перенаправлении (изменении маршрута), для того чтобы сообщить о наличии более короткого маршрута.

Если адрес получателя является адресом промежуточной системы в другой подсети той же самой зоны, то IS-система знает правильный маршрут и отправляет пакет по этому маршруту. Если адрес пункта назначения соответствует ES-системе другой зоны, то IS-система уровня 1 посылает этот пакет ближайшей IS-системе уровня 2.

Пересылка через IS-системы уровня 2 продолжается до тех пор, пока пакет не достигнет IS-системы уровня 2 в зоне получателя. В этой зоне получателя IS-системы пересылают пакет по оптимальному маршруту до тех, пор пока он не достигнет конечной системы ES получателя.

Протокол ES-IS

Протокол взаимодействия конечной системы с промежуточной системой (End System-to-Intermediate System — ES-IS) представляет собой протокол OSI, описывающий процесс распознавания друг другом конечных систем (рабочих станций или узлов) и промежуточных систем (маршрутизаторов), известный как конфигурирование. Конфигурирование должно быть выполнено перед установкой маршрута между конечными устройствами (ES).

Протокол ES-IS следует рассматривать скорее как протокол распознавания, чем как протокол маршрутизации. Он позволяет различать три типа подсетей: подсети "точка-точка", широковещательные подсети и подсети с обычной топологией (рис. 48.2).

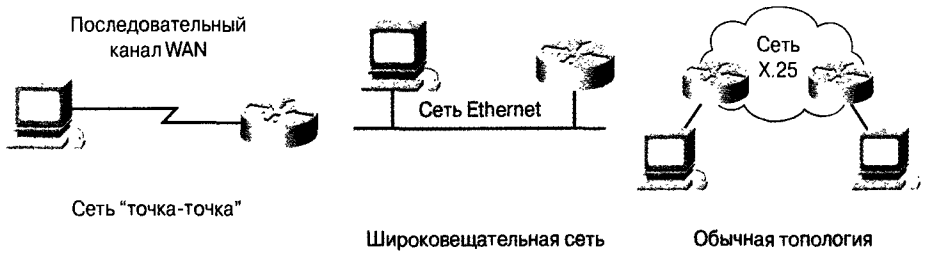


Рис. 48.2. Протокол ES-IS может использоваться в подсетях с топологиtq "точка-точка", широковещательной и обычной сети

Подсети "точка-точка", такие как глобальные последовательные линии связи WAN-сетей, обеспечивают непосредственное соединение между двумя системами. Широковещательные сети Ethernet и IEEE 802.3 и подобные им направляют одиночное физическое сообщение на все узлы подсети. Подсети с обычной топологией, такие как X.25, поддерживают произвольное количество систем. Однако, в отличие от широковещательных подсетей, стоимость передачи данных в сети с обычной топологией по n-направлениям увеличивается пропорционально размеру подсети.

Конфигурирование протокола ES-IS

Под конфигурированием протокола ES-IS понимается процесс, во время которого конечные и промежуточные системы распознают друг друга, что необходимо для установления маршрута между конечными системами. Конфигурационная информация ES-IS передается с постоянными интервалами посредством сообщений приветствия протокола ES (ES Hello — ESH) и протокола IS (IS Hello — ISH). Сообщения ESH генерируются конечными системами ES и рассылаются всем IS-системам подсети. Сообщения ISH создаются промежуточными системами IS и посылаются всем конечным ES-системам подсети. Главное назначение этих сообщений приветствия состоит

в передаче адресов сетевого и подсетевого уровней систем, которые генерируют такие сообщения.

Там, где это возможно, протокол ES-IS пытается отослать информацию о конфигурации сразу нескольким системам. В широковещательных подсетях сообщения приветствия ES-IS рассылаются всем промежуточным системам с использованием специального адреса многоадресатной рассылки, соответствующего всем конечным системам. В подсети с обычной топологией протокол ES-IS обычно не передает информацию о конфигурации из-за высокой стоимости многоадресатной рассылки.

Адресация протокола ES-IS

Протокол конфигурирования ES-IS передает адреса обоих уровней модели OSI — сетевого и подсетевого. Адреса сетевого уровня OSI определяют либо точку доступа к сетевой службе (Network Service Access Point — NSAP), которая служит интерфейсом между уровнями 3 и 4 модели OSI, либо заголовок сетевого элемента (Network Entity Title — NET) IS-системы, соответствующий сетевому уровню модели OSI. Адреса подсетей OSI, или адреса точек подключения подсетей (SubNetwork Point of Attachment Address — SNPA), представляют собой точки физического подключения к подсети промежуточных и конечных систем. Адреса SNPA однозначно идентифицируют каждую систему, подключенную к подсети. Например, в сети Ethernet адрес SNPA представляет собой 48-битовый MAC-адрес. Частью конфигурационной информации, передаваемой протоколом ES-IS, является преобразование адресов NSAP-SNPA или NET-SNPA.

Протокол IS-IS

Первоначально протокол IS-IS поддерживал только CLNS-сети OSI, но позднее был расширен для поддержки маршрутизации в IP-сетях без классов. Эта расширенная версия называется объединенным IS-IS (Integrated IS-IS) или иногда двойным IS-IS (Dual IS-IS) протоколом.

Независимо от того в какой сети он используется, протокол IS-IS является протоколом канального уровня и, следовательно, как и протокол OSPF, обладает определенными преимуществами перед дистанционно-векторными протоколами. Он обеспечивает быструю сходимость и быстрое лавинное распространение сообщений об изменениях в топологии сети. Он поддерживает иерархическую маршрутизацию посредством использования зон, что обеспечивает высокую масштабируемость. Кроме того, протокол IS-IS был усовершенствован в целях повышения его гибкости, что позволяет использовать его в качестве протокола внутреннего шлюза (Interior Gateway Protocol — IGP) в сетях, использующих перераспределение потоков MPLS (многопротокольная коммутация по метке — Multiprotocol Label Switching (MPLS) Traffic Engineering (TE)).

Объединенный протокол IS-IS

Как уже упоминалось выше, протокол IS-IS был расширен для поддержки IP-маршрутизации в дополнение к поддержке маршрутизации протокола CLNS. Поддержка IP-маршрутизации определена в RFC 1195. Протокол IS-IS популярен среди крупных провайдеров служб и часто используется в сетях, использующих только

протокол IP. Протокол IS-IS может поддерживать как IP-сети, так и сети протокола CLNS, по отдельности или вместе. При этом для поддержки передачи данных обоих протоколов — OSI и IP — нет необходимости поддерживать в сети работу двух абсолютно независимых протоколов маршрутизации и связанных с ними управляющих плоскостей.

Структура маршрутизации протокола IS-IS

Протокол IS-IS поддерживает иерархическую модель маршрутизации путем использования зон. При этом крупная сеть делится на сети меньшего размера. Маршрутизаторы протокола IS-IS, которые выполняют маршрутизацию только внутри зоны, называются маршрутизаторами 1-го уровня. Маршрутизаторы IS-IS, выполняющие маршрутизацию между зонами, называются маршрутизаторами 2-го уровня.

Магистраль протокола IS-IS не является отдельной нулевой зоной, как это имеет место в протоколе OSPF. Она представляет собой группу последовательно и непрерывно соединенных между собой маршрутизаторов 2-го уровня. Каждый маршрутизатор 2-го уровня функционирует только в рамках отдельной зоны, но может иметь каналы, которые соединяют его с маршрутизаторами 2-го уровня другой зоны. Следует отметить, что границей зоны является не маршрутизатор 2-го уровня, а канал между маршрутизаторами 2-го уровня. На рис. 48.3 показана иерархическая модель маршрутизации протокола IS-IS.

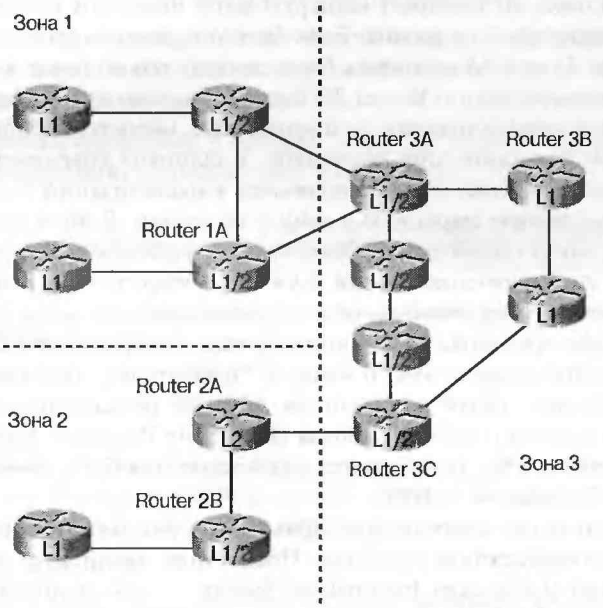


Рис. 48.3. Структура маршрутизации протокола IS-IS

Вообще говоря, маршрутизаторам 1-го уровня известна только информация о сети, относящаяся к зоне, в которой он находится. Если маршрутизатор 1-го уровня на основе информации о своей зоне не знает, куда переслать пакет, то он посылает пакет на ближайший маршрутизатор 2-го уровня, который затем направляет пакет в соответствующую зону. В зоне получателя пакет пересылается маршрутизаторами 1-го уровня этой зоны.

Если маршрутизатор 1-го или 2-го уровня подсоединен к другой зоне, то он оповещает об этом маршрутизаторы 1-го уровня собственной зоны путем установки прикрепленного бита при анонсировании маршрутизации. Маршрутизаторы 1-го уровня замечают этот установленный бит и с этого момента знают, что этот маршрутизатор 1-го или 2-го уровня можно использовать для доступа к сетям, находящимся вне данной зоны. При использовании объединенного протокола IS-IS (Integrated IS-IS) этот маршрутизатор 1-го или 2-го уровня инициирует маршрут по умолчанию в свою собственную зону. На рис. 48.3 оба маршрутизатора, Router 1A и Router 1B, устанавливают attached бит и/или инициируют маршрут по умолчанию к другим маршрутизаторам зоны 1.

Маршрутизаторы 2-го уровня знают только о межзонных маршрутах, но не знают маршруты в своей собственной зоне. В сетях, в которых используется только протокол OSI, маршрутизаторы уровня 2 не следует конфигурировать, поскольку всем OSI-маршрутизаторам необходимо знать топологию своей собственной зоны. Маршрутизатор может быть сконфигурирован как маршрутизатор уровня 1 или 2; в этом случае он будет знать как локальные маршруты зоны, так и межзонные маршруты. Маршрутизатор 1-го или 2-го уровня интегрированного протокола IS-IS передает IP-информацию 1-го уровня на 2-й уровень и может быть summarized во время этого процесса.

В зависимости от того, как была спроектирована сеть, направление к ближайшему маршрутизатору 2-го уровня может оказаться неоптимальным маршрутом передачи данных, однако маршрутизатор 1-го уровня не знает об этом, поскольку ему известны только маршруты 1-го уровня. Например, как показано на рис. 48.3, маршрутизатор 1-го уровня Router 3B выбирает маршрутизатор Router 3A в качестве своего ближайшего маршрутизатора 2-го уровня. Если бы поток данных был направлен в зону 2, то маршрутизатору Router 3A пришлось бы направить его по более длинному маршруту, чем если бы маршрутизатор Router 3B с самого начала принял решение отправить эти данные другому маршрутизатору 2-го уровня, т.е. маршрутизатору Router 3C.

Для того чтобы устранить этот недостаток, в протокол объединенного IS-IS было внесено усовершенствование, которое позволяет маршрутизатору 2-го уровня передавать отдельные выбранные маршруты в зону 1-го уровня. В этом случае маршрутизаторы 1-го уровня могут принять более оптимальное решение относительно пересылки пакетов. Однако это увеличение объема служебной информации о маршрутах уменьшает масштабируемость первоначальной структуры маршрутизации протокола IS-IS.

Маршрутизаторы протокола IS-IS автоматически обнаруживают своих соседей путем рассылки пакетов приветствия. В каналах "точка-точка" они образуют непосредственные одноранговые связи и лавинным образом рассылают свою информацию маршрутизации в пакетах состояния канала (Link-State Packets — LSPs). Информация, находящаяся в пакетах LSP, используется для построения базы данных состояния каналов (Link-State Database — LSDB).

В широковещательных сетях пакеты приветствия рассылаются по общеизвестным MAC-адресам многоадресатной рассылки. После этого выбирается назначенная промежуточная система (Designated Intermediate System — DIS), которая лавинным образом рассылает пакеты LSP от имени всех других маршрутизаторов данного сегмента.

Типы пакетов

Как уже говорилось выше, маршрутизаторы протокола IS-IS рассылают пакеты приветствия для автоматического обнаружения маршрутизаторов 1-го и 2-го уровня.

На рис. 48.4 показаны поля пакетов приветствия 1-го и 2-го уровня.

Ниже приведено описание полей этих пакетов.

- **Дискриминатор протокола междоменной маршрутизации.** 8 битов. Идентификатор сетевого уровня протокола IS-IS (0x83).
- **Индикатор длины заголовка.** 8 битов. Длина заголовка в битах.
- **Расширение версии/ ID протокола.** 8 битов. Устанавливается равным 1.
- **Длина идентификатора ID.** Длина поля "идентификатор источника". Значение, равное 0, означает стандартную длину поля идентификатора ID, которая равна 6 байт.
- **Зарезервировано/тип.** 3 бит/5 бит. Первые три бита зарезервированы. Последние пять битов определяют тип PDU. Пакеты приветствия имеют значения типа PDU, показанные в табл. 48.1

Таблица 48.1 Значения типа PDU для пакетов приветствия

Тип	Значение
15	Пакет приветствия протокола IS-IS LAN-сети 1-го уровня
16	Пакет приветствия протокола IS-IS LAN-сети 2-го уровня
17	Пакет приветствия протокола IS-IS сети типа "точка-точка"

- **Версия.** 8 битов. Текущим значением версии является 1.
- **Максимальный адрес зоны.** 8 битов. Адреса номеров зон, разрешенные для использования в этой зоне, должны находиться в диапазоне от 1 до 254. Значение 0 предполагает наличие трех адресов зон.
- **Зарезервировано/тип канала.** 6 битов/2 бита. Тип канала определяется в соответствии со значениями, приведенными в табл. 48.2

Таблица 48.2. Типы канала для пакетов приветствия

Значение	Описание
00	Зарезервировано
01	Уровень 1
10	Уровень 2
11	Уровни 1 и 2

- **ID источника.** Длина идентификатора ID, содержащаяся в поле ID Length. Системный идентификатор маршрутизатора-источника.
- **Таймер задержки.** 16 битов.
- **Длина модуля PDU.** 16 битов. Это значение включает в себя длину заголовка PDU и длину полей переменной длины.
- **Зарезервировано/приоритет.** 1 бит/7 битов. Задает приоритет при выборе DIS в широковещательной сети.
- **ID LAN-сети.** Системный идентификатор DIS плюс один дополнительный байт.
- **Поля переменной длины.** К ним относятся поля TLV.

Внимание!

PDU пакетоа приаетстаия сетей IS-IS типа "точка-точка" ао многом соападают с пакетами приветстаия LAN-сетей. Октет, содержащий поле приоритета опущен, поскольку а данном случае нет необходимости аыбирать DIS. Поле ID LAN-сети заменяется отдельным октетом идентификатора ID локального канала.

Маршрутизаторы протокола IS-IS обмениваются информацией маршрутизации с соседними маршрутизаторами, используя LSP-пакеты. Действительные анонсированные сетевые адреса хранятся как значения длины типа (Type Length Values — TLVs), находящиеся в конце LSP-пакета.

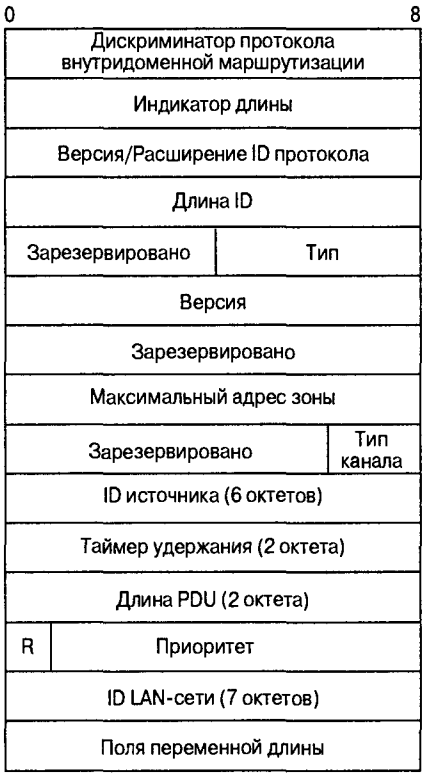


Рис 48.4. Поля пакетов приветствия 1-го и 2-го уровня протокола IS-IS

На рис. 48.5 показаны поля этого пакета.
Ниже приведено описание этих полей.

- **Дискриминатор протокола внутридоменной маршрутизации**. 8 бит. Идентификатор сетевого уровня протокола IS-IS (0x83).
- **Индикатор длины заголовка.** 8 битов. Длина заголовка в битах.
- **Расширение версии/ ID протокола.** 8 битов. Устанавливается равным 1.
- **Длина идентификатора ID.** Длина поля "идентификатор источника". Значение, равное 0, означает стандартную длину поля ID, которая равна 6 байтов.

- **Зарезервировано/тип PDU.** 3 бита/5 битов. Первые три бита зарезервированы. Последние пять битов определяют тип PDU. Пакеты приветствия имеют значения типов PDU, показанные в табл. 48.3

Таблица 48.3. Типы PDU пакетов приветствия

Значение	Описание
18	PDU состояния канала 1-го уровня
20	PDU состояния канала 2-го уровня

- **Версия.** 8 битов. Текущим значением версии является 1.
- **Максимальный адрес зоны.** 8 битов. Адреса номеров зоны, разрешенные для использования в этой зоне, должны находиться в диапазоне от 1 до 254. Значение 0 предполагает наличие трех адресов зон.
- **Длина PDU.** 16 битов.
- **Оставшееся время существования пакета.** Оставшееся время существования пакета LSP в секундах.
- **ID пакета LSP.** Длина ID плюс 16 битов. Идентификатор ID образуется из системного ID плюс 1D псевдоузла и номер фрагментации пакета LSP.
- **Контрольная сумма.** 32 битов. Вычисляется от поля ID LSP-пакета до конца PDU.
- **P (Partition).** 1 бит. Значение 1 указывает на то, что инициатор поддерживает восстановление partition.
- **Поле ATT (Attached).** 4 бита. Задает тип метрики маршрутизации: стандартная, задержка, затраты или ошибка.
- **Бит L.** 1 бит. Значение 1 означает, что инициатор перегружен и не должен учитываться при расчете дерева кратчайшего пути.
- **Тип промежуточной системы IS.** 2 бита. Указывает уровень IS в соответствии со значениями, приведенными в табл. 48.4

Таблица 48.4 Типы промежуточных систем IS

Value	Description
01	1-й уровень
11	2-й уровень

- **Поле длины.** В это поле помещается умноженное на 3 значение длины (Triple Length Value — TLV).

Значения TLV

Поле переменной длины в конце PDU пакета приветствия и поле длины типа (Type Length) содержат значения TLV. Это место, где действительные сетевые адреса содержатся в пакете LSP. Типовые поля для TLV описаны в табл. 48.5.

Первоначально для передачи такой информации, как CLNS-адреса, информация о соседних устройствах и аутентификации, были определены 10 TLV-кодов.

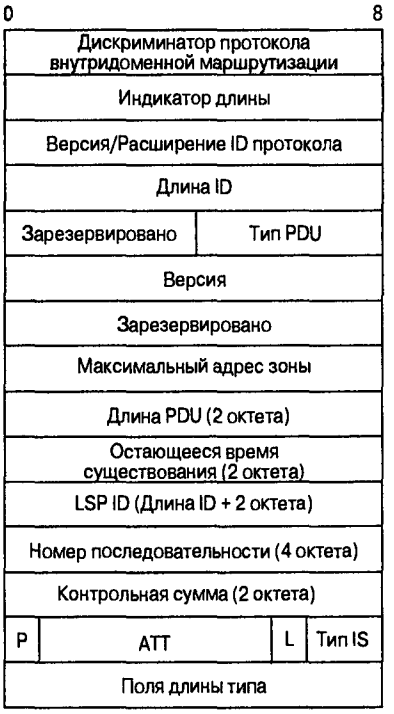


Рис 48.5. Поля пакетов LSP 1-го и 2-го уровня протокола IS-IS

Таблица 48.5. Формат поля TLV

Поле	Длина в октетах
Тип	1
Длина	1
Значение	Определяется длиной поля Length

Внимание!

В RFC 1195, описывающем интегрированный протокол IS-IS (Integrated IS-IS), введен новый набор TLV-кодов для поддержки адресов протокола IPV4.

Протокол IS-IS допускает расширение путем определения новых TLV. Таким способом в протоколе IS-IS были введены новые функции, такие как поддержка протокола IPv6 и перераспределения потоков TE MPLS.

В табл. 48.6 перечислены типовые значения TLV, реализованные в IOS Cisco.

Метрики протокола IS-IS

Четырьмя метриками, определенными в протоколе IS-IS, являются: оценка маршрута, задержка, затраты и ошибка. Из них только оценка маршрута является обязательной и используется в реализации IOS Cisco. Стандартная оценка устанавливается равной 10. Мак-

симальная оценка интерфейсов равна 63. Максимальное значение оценки маршрута, равное 1023, ограничивает размеры сети и накладывает ограничения при ее проектировании. Для решения этой проблемы IOS Cisco поддерживает расширенную метрику с 24-битовым полем. Однако перед применением этой функции необходимо убедиться в том, что ее поддерживают все маршрутизаторы IS-IS; в противном случае могут возникнуть проблемы при вычислении дерева кратчайшего маршрута.

Таблица 48.6. Типовые TLV

Значение	Описание
1	Адреса зон
2	Соседние IIS
8	Заполнитель
10	Аутентификация
22	Соседние IIS TE
128	Внутренняя достижимость IP
129	Поддерживаемые протоколы
130	Внешние IP-адреса
132	Внутренние IP-адреса
134	ID маршрутизатора TE
135	Досягаемость IP TE
137	Динамическое имя станции (узла)
10 и 133	Аутентификация

Обработка LSP-пакетов протокола IS-IS

Когда маршрутизатор получает LSP-пакеты, он добавляет их в свою базу LSDB, если номер последовательности LSP больше, чем тот, который уже хранится в базе. База LSDB описывает все сети, метрики и содержит информацию о досягаемости каждого маршрутизатора для построения дерева кратчайших маршрутов с использованием алгоритма Дейкстра (Dijkstra). На основе этой базы позднее строится таблица пересылки. Когда маршрутизатор получает LSP-пакет, он рассылает его лавинным образом всем своим соседям, за исключением того маршрутизатора, от которого этот пакет был получен. Протокол IS-IS использует надежный механизм лавинной рассылки и некоторые дополнительные типы PDU: PDU полного номера последовательности (Complete Sequence Number PDU — CSNP) и PDU частичного номера последовательности (Partial Sequence Number PDU — PSNP). Кроме того, существуют типы PDU 1-го и 2-го уровня протоколов CSNP и PSNP.

Получающий пакет маршрутизатор посылает назад PSNP (содержащий номер последовательности LSP-пакета) своему соседнему устройству в качестве подтверждения получения LSP-пакета. Когда маршрутизатор-источник получает это подтверждение, он прекращает обновление LSP-пакета на данном интерфейсе, но продолжает делать это на других интерфейсах, где еще не было получено PSNP.

В широковещательной среде, PSNP в качестве подтверждений не рассылаются. Маршрутизаторы ожидают получения CSNP, который содержит список LSP-пакетов

и их номер последовательности. Принимающие маршрутизаторы могут затем определить, не были ли пропущены какие-либо LSP-пакеты и не устарели ли они, и при необходимости запрашивают их с помощью PSNP.

Выбор DIS-системы протокола IS-IS

В широковещательной среде один из маршрутизаторов IS-IS становится DIS-системой и образует псевдоузел. Выбор DIS основывается на значении приоритета, которое конфигурируется на каждом интерфейсе маршрутизатора. Псевдоузел представляет собой сегмент LAN-сети, и все маршрутизаторы (не являющиеся псевдоузлами) становятся для него смежными устройствами.

Следует отметить, что выбор DIS является preemptive. Если в систему добавляется новый маршрутизатор с более высоким приоритетом, то он заменяет текущий маршрутизатор DIS и сам становится DIS-маршрутизатором, создавая тем самым новый псевдоузел. Каждые 3 сек DIS рассылает листинги протокола CSNP, в которых перечислены все LSP-пакеты. Каждый маршрутизатор может запросить отсутствующие у него LSP-пакеты или самые последние пакеты путем отправки PSNP. Аналогичным образом любой маршрутизатор может обновить информацию на псевдоузле путем отправки DIS-маршрутизатору отсутствующих у последнего LSP-пакетов или самых последних пакетов.

Обход "черных дыр" с использованием протокола IS-IS

Использование бита перегрузки позволяет маршрутизатору, который испытывает недостаток критически важных ресурсов, сообщить своим соседним устройствам о том, что его не следует больше использовать в качестве маршрута для транзитной передачи данных. Однако при этом данный маршрутизатор продолжает присутствовать в иерархии маршрутизаторов протокола IS-IS. Этот бит перегрузки также используется в RFC 3277, *Intermediate System–to–Intermediate System (IS-IS) Transient Blackhole Avoidance Feature.*

При использовании в IP-сети протоколов IS-IS/BGP в случае, когда маршрутизатор базовой сети, который обычно находится на маршруте передачи данных, осуществляет перезагрузку, он быстрее осуществляет конвергенцию протокола IS-IS, чем протокола BGP. В этом случае другие маршрутизаторы посылают потоки данных в то место, где к следующему переходу протокола BGP для этих данных можно получить доступ по протоколу IS-IS. Когда данные поступают на этот недавно перезагруженный маршрутизатор, у него нет позиции пересылки для адреса получателя этих данных, поскольку протокол BGP еще не закончил конвергенцию. В таком случае говорят, что поток данных попал в "черную дыру".

Согласно RFC 3277, перезагружающийся маршрутизатор устанавливает бит перезагрузки в своих LSP-пакетах до тех пор, пока не закончится конвергенция протокола BGP. К этому маршрутизатору по-прежнему могут получить доступ другие маршрутизаторы, однако он не используется для транзитной передачи данных. Когда конвергенция протокола BGP закончена, бит перегрузки устанавливается в ноль и маршрутизатор снова может использоваться для передачи данных по маршруту к следующему переходу протокола BGP.

Проникновение маршрутов

Как уже говорилось ранее, Проникновение маршрутов со 2-го уровня на 1-й уровень позволяет маршрутизаторам 1-го уровня выбрать более оптимальный маршрут, если в зоне имеется более одного маршрутизатора 2-го уровня. В обычной ситуации выбирается ближайший маршрутизатор. Другим применением перетекания маршрутов является поддержка виртуальных частных сетей (VPN) MPLS. Виртуальные частные сети VPN MPLS используют протокол mBGP для обмена информацией между PE-маршрутизаторами и должны видеть следующий переход протокола BGP (32-битовый адрес узла с маской) в своей собственной таблице маршрутизации, для того чтобы этот маршрут был действительным.

Перераспределение потоков в сетях MPLS

Перераспределение потоков (Traffic Engineering — TE) в сетях MPLS, позволяет принимать решения о пересылке пакетов, основываясь на информации, отличной от IP-префиксов следующего перехода. Маршрутизатор MPLS может устанавливать туннели на основе информации о доступности ресурсов в сети. Эти туннели могут базироваться на явном или динамически выбираемом маршруте с коммутацией по метке (Label-Switched Path — LSP). Установка динамического маршрута LSP определяется информацией о доступности ресурсов на маршруте, таких как доступная полоса пропускания, близость каналов и оценка канала, используемая в MPLS. Эти параметры описывают соседние устройства и IP-сети таким же образом, как это выполняют TLV 2, 128 и 130.

Однако эти новые значения TLV также допускают использование вспомогательных вторичных значений TLV в первичных TLV для описания дополнительных характеристик соседних устройств или их префикса, таких как доступная полоса пропускания.

Более подробная информация об этих и других функциях протокола IS-IS приведена в ссылках раздела "Дополнительные источники" настоящей главы.

Протокол IDRP

Протокол междоменной маршрутизации IDRP (InterDomain Routing Protocol — IDRP) представляет собой протокол OSI, определяющий способ обмена данными между маршрутизаторами, расположенными в разных доменах. Протокол IDRP предназначен для совместной работы с протоколами CLNP, ES-IS и IS-IS. Протокол IDPR основан на BGP — междоменном протоколе маршрутизации, который ведет свое происхождение от протоколов IP. Ниже перечислены функции протокола IDPR:

- поддержка качества обслуживания (QoS) для CLNP;
- устранение петель путем отслеживания RD, передаваемых по маршруту;
- сокращение объема маршрутной информации и упрощение обработки при помощи конфедераций, сжатия маршрутной информации RD и пр.;
- обеспечение надежности за счет встроенных механизмов надежной передачи;
- обеспечение безопасности за счет криптографических сигнатур для каждого пакета;
- серверы маршрутизации.

Терминология IDRP

При описании протокола IDRP применяется несколько специфических терминов: внешняя промежуточная система (BIS), домен маршрутизации (RD), идентификатор домена маршрутизации (RDI), маршрутная база данных (RIB) и конфедерация.

Внешняя промежуточная система (Border Intermediate System — BIS) представляет собой промежуточную систему (IS), которая принимает участие в междоменной маршрутизации и, следовательно, использует протокол IDRP. Домен маршрутизации (Routing Domain — RD) — это группа конечных систем (ES) и промежуточных систем (IS), которая подчиняется одним и тем же правилам администрирования и имеет общий план маршрутизации. Идентификатор домена маршрутизации (Routing Domain Identifier — RDI) представляет собой уникальный идентификатор RD. Маршрутная база данных (Routing Information Base — RIB) является базой данных, которую использует протокол IDRP. Она создается каждой BIS на основе информации, полученной от RD и других BIS. База RIB содержит маршруты, используемые отдельными BIS. Конфедерация представляет собой группу RD, которая воспринимается внешними RD, не относящимися к конфедерации, как один RD. Внешним RD неизвестна топология конфедерации. Конфедерации располагаются одна внутри другой и позволяют сократить объем передачи данных по сети, играя роль межсетевых брандмауэров. На рис. 48.5 показана взаимосвязь элементов протокола IDRP.

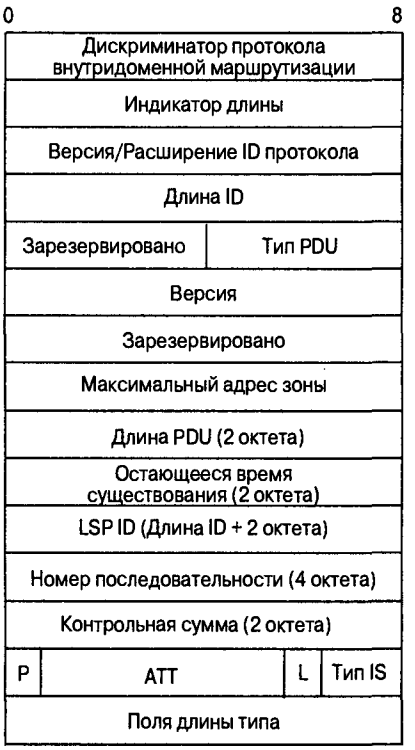


Рис. 48.5. Домены обмениваются данными при помощи BIS

IDRP-маршрутизация

Маршрут IDRP представляет собой последовательность RDI, причем некоторые из них могут быть конфедерациями. Каждая BIS "знает", какой RD принадлежит какой конфедерации. Сведения о других BIS, RD и конфедерациях она получает во время обмена информацией с соседними системами. Как и при дистанционно-векторной маршрутизации, маршрут к получателю строится от этого получателя. Другим BIS передаются только специально отобранные маршруты, удовлетворяющие локальным политикам BIS. Повторно маршрут вычисляется только частично, и происходит это в одном из трех случаев: при получении инкрементного обновления маршрутизации с новыми маршрутами, а также при отключении или подключении соседней системы BIS.

Резюме

В основе протокола взаимодействия промежуточных систем (Intermediate System-to-Intermediate System — IS-IS) лежит технология, разработанная корпорацией Digital (Digital Equipment Corporation). Протоколы маршрутизации OSI обобщены в нескольких документах Международной организации стандартизации (International Organiztion for Standardazation — ISO). Организация ISO разработала полный набор протоколов маршрутизации для использования в стеке протоколов OSI.

В сфере применения сетей OSI используются такие специальные термины, как "конечная система" (End System — ES) (этот термин относится к любому сетевому узлу, который не осуществляет маршрутизации) и "промежуточная система" (Intermediate system — IS) — этот термин относится к маршрутизаторам.

Маршрутизация OSI начинается, когда конечная система ES обнаруживает ближайшую промежуточную систему IS. Когда конечной системе ES требуется отправить пакет другой конечной системе ES, она посылает пакет одной из промежуточных систем IS по своей непосредственно подсоединенной сети.

Протокол взаимодействия конечной системы с промежуточной системой (End System-to-Intermediate System — ES-IS) является протоколом стека OSI, который определяет, каким образом конечные системы (рабочие станции) и промежуточные системы (маршрутизаторы) распознают друг друга.

Протокол взаимодействия промежуточных систем (Intermediate system-to-intermediate system — IS-IS) был расширен для того, чтобы он поддерживал также и бесклассовые IP-сети. Эта расширенная версия известна как интегрированный протокол IS-IS. Протокол междоменной маршрутизации (Interdomain Routing Protocol — IDRP) является протоколом OSI, который определяет, каким образом маршрутизаторы осуществляют связь с маршрутизаторами других доменов.

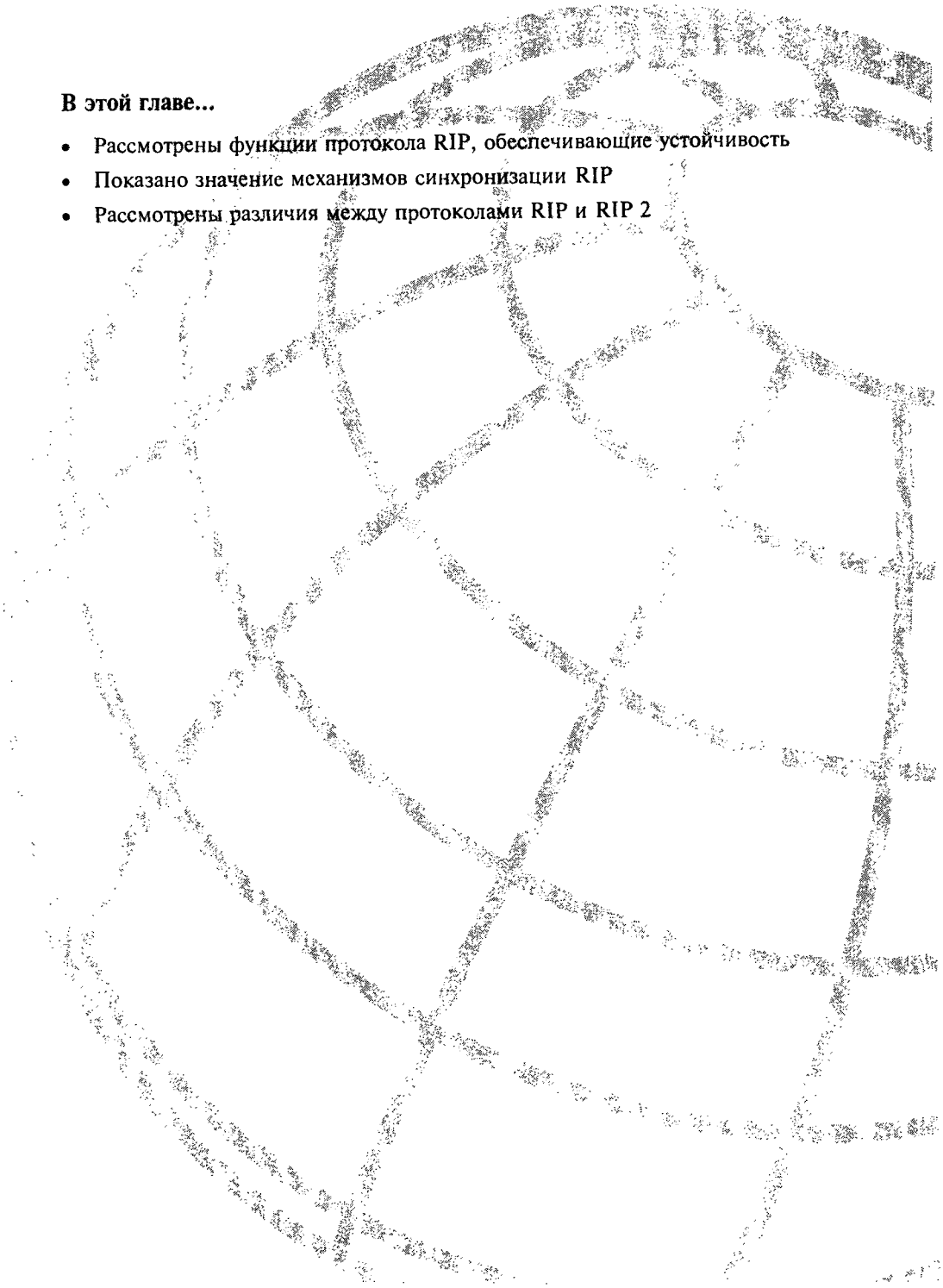
Контрольные вопросы

1. Какие два типа сообщений передаются между системами по протоколу ES-IS?
2. В чем состоит различие между маршрутизаторами IS-IS 1-го и 2-го уровней?
3. Опишите, каким образом маршрутизаторы протокола IS-IS осуществляют связь между собой в широковещательных сетях.

4. Каково первоначальное предназначение бита перегрузки?
5. Что такое TLV?
6. Каким образом в каждом канале конфигурируется метрика протокола IS-IS?

Дополнительные источники

- Стандарт ISO/IEC 10589:2002: Intermediate System-to-Intermediate System intradomain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473), www.iso.org.
- White paper: "Intermediate System–to–Intermediate System (IS-IS) TLVs," Cisco Systems, 2002, www.cisco.com.
- White paper: "Introduction to Intermediate System–to–Intermediate System Protocol," Cisco Systems, 2002, www.cisco.com.
- RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments, Callon, R. (Digital Equipment Corporation), December 1990, www.ietf.org.
- RFC 3277, Intermediate System–to–Intermediate System (IS-IS) Transient Blackhole Avoidance, McPherson, D. (TCB), April 2002, www.ietf.org.



В этой главе...

- Рассмотрены функции протокола RIP, обеспечивающие устойчивость
- Показано значение механизмов синхронизации RIP
- Рассмотрены различия между протоколами RIP и RIP 2

Глава 49

Протокол RIP

Введение

Протокол маршрутной информации RIP (Routing Information Protocol — RIP) является одним из самых живучих протоколов маршрутизации. Вместе с тем RIP — один из самых запутанных протоколов из-за того, что существует множество RIP-подобных протоколов, причем многие имеют то же название. Протокол RIP и огромное количество похожих на него основаны на одном и том же наборе алгоритмов, использующих вектор расстояния для математического сравнения маршрутов и выбора наилучшего маршрута к месту назначения. Эти алгоритмы появились в результате академических исследований, восходящих к 1957 г.

Современный открытый стандарт RIP, иногда называемый IP RIP, формально описан в двух документах: RFC 1058 и Internet Standard (STD) 56. Поскольку IP-сети становятся все более многочисленными и крупными, группа IETF (Internet Engineering Task Force) пришла к выводу, что RIP нуждается в обновлении. Поэтому в январе 1993 г. IETF опубликовала RFC 1388, а в ноябре 1994 г. — RFC 1723, где был описан RIP 2 (вторая версия RIP). При разработке этих документов, описывающих расширенные возможности RIP, не ставилась, однако, цель заменить предыдущую версию RIP. В версии RIP 2 в сообщениях RIP можно передавать больше информации, что позволяет использовать простой механизм аутентификации для обеспечения безопасности обновления таблиц. Что более важно, RIP 2 поддерживает маски подсети — важную функцию, отсутствовавшую в RIP.

В данной главе описываются основные функции и возможности RIP, в том числе процесс обновления маршрутов, метрики маршрутизации RIP, устойчивость маршрутизации и таймеры маршрутизации.

Обновление маршрутов

Протокол RIP посылает сообщения об обновлении маршрутов через регулярные интервалы, а также при изменении топологии сети. Когда маршрутизатор получает информацию об обновлении маршрутов, куда входят измененные записи маршрутной таблицы, он обновляет свою маршрутную таблицу, занося в нее новый маршрут. Значение метрики маршрута увеличивается на 1, и отправитель сообщения указывается

в качестве следующего перехода. RIP-маршрутизаторы запоминают только наилучший маршрут к получателю (маршрут с наименьшим значением метрики). После обновления маршрутной таблицы маршрутизатор немедленно начинает передачу сообщений об обновлении маршрутов, чтобы сообщить другим маршрутизаторам в сети о произошедших изменениях. Эта информация посылается независимо от плановых, регулярных обновлений, посылаемых RIP-маршрутизаторами.

Метрика маршрута RIP

Для измерения расстояния между сетью-источником и сетью-получателем RIP использует единую метрику — количество переходов. Каждому переходу на маршруте от источника к получателю присваивается значение счетчика переходов, которое обычно равно 1. При получении сообщения об обновлении маршрутов с новой или измененной записью о сети-получателе маршрутизатор добавляет единицу к значению метрики, указанному в сообщении и обновляет свою таблицу маршрутизации, включая в нее новый маршрут. IP-адрес отправителя используется в качестве следующего перехода.

Функции обеспечения устойчивости протокола RIP

RIP предотвращает зацикливание в маршрутных петлях путем ограничения количества переходов на маршруте между источником и получателем. Максимальное число переходов равно 15. Если маршрутизатор получает маршрутное обновление, где содержится новый или измененный элемент, и увеличение метрики на 1 приводит к значению 16, то данный получатель считается недоступным. Недостатком этой функции обеспечения устойчивости является ограничение максимального диаметра сети RIP 16 переходами.

В RIP есть и другие средства обеспечения устойчивости, используемые многими другими протоколам маршрутизации. Эти функции разрабатывались для сохранения устойчивости, несмотря на возможные резкие изменения сетевой топологии. Например, в RIP во избежание распространения некорректной маршрутной информации применяются расщепление горизонта и механизмы удержания (задержки фиксации изменений).

Таймеры RIP

Для регулирования производительности в RIP используются различные таймеры, в том числе таймер обновления маршрутов, таймер ожидания и таймер смещения маршрута. Таймер обновления маршрутов задает интервал между периодическими обновлениями маршрутов. Обычно такой интервал составляет 30 секунд, с добавлением небольшого случайного количества времени всякий раз, когда таймер сбрасывается. Это делается во избежание перегрузки, которая может возникнуть, если все маршрутизаторы одновременно попытаются передать обновленную маршрутную информацию своим соседям. Каждая запись в маршрутной таблице имеет свой таймер ожидания. Когда значение интервала, заданное в этом таймере, истекает, маршрут помечается как недействительный, но сохраняется в таблице до тех пор, пока не истечет время, заданное в таймере смещения маршрута.

Форматы пакетов

В этом разделе рассматриваются форматы пакетов IP RIP и IP RIP 2, показанные на рис. 44.1 и 44.2. Каждый рисунок сопровождается описанием полей пакета.

Формат пакета RIP

На рис. 49.1 показан формат пакета RIP IP.

Команда (1 октет)	Версия (1 октет)	Нулевое поле (2 октета)	AFI (2 октета)	Нулевое поле (2 октета)	IP-адрес (4 октета)	Нулевое поле (4 октета)	Нулевое поле (4 октета)	Метрика (4 октета)

Рис. 49.1. Пакет RIP IP состоит из девяти полей

Ниже описаны поля пакета формата IP RIP, показанного на рис. 49.1.

- **Команда.** Показывает, является ли пакет запросом или ответом. Запрос требует, чтобы маршрутизатор отправил маршрутную таблицу — всю или частично. Ответ может быть незапрашиваемым регулярным обновлением маршрутной информации или ответом на запрос. В ответах содержатся записи маршрутной таблицы. Для передачи информации из больших маршрутных таблиц используется несколько RIP-пакетов.
- **Версия.** Номер версии RIP. Это поле может использоваться для информирования о потенциально несовместимых версиях.
- **Нулевое поле.** В RIP, описанном в RFC 1058, это поле фактически не используется. Оно добавляется исключительно для обеспечения обратной совместимости с нестандартными версиями RIP и содержит нулевое значение.
- **Идентификатор AFI.** Идентификатор семейства адреса (Address-Family Identifier). RIP предназначен для передачи маршрутной информации нескольких различных протоколов. Каждая запись имеет идентификатор семейства адреса, который определяет тип адреса. AFI для IP равно 2.
- **Адрес.** IP-адрес записи.
- **Метрика.** Определяет, сколько переходов (транзитных участков между маршрутизаторами) было пройдено на пути к получателю. Для действующих маршрутов эта величина находится в диапазоне между 1 и 15, а для недействующих она равна 16.

Примечание

В одном пакете IP RIP может содержаться до 25 полей AFI, а также адреса и метрики. (В одном пакете RIP может быть перечислено до 25 получателей.)

Формат пакета RIP 2

Спецификация RIP 2, описанная в RFC 1723, позволяет включать в пакеты RIP больше информации и обеспечивает простой механизм аутентификации, который не поддерживается протоколом RIP. Формат пакета IP RIP показан на рис. 49.2.

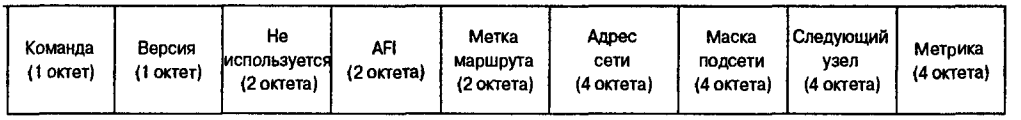


Рис. 49.2. Пакет IP RIP 2 состоит из тех же полей, что и пакет IP RIP

Ниже описаны поля пакета формата IP RIP 2, показанные на рис. 49.2.

- **Команда.** Показывает, является ли пакет запросом или ответом. Запрос требует, чтобы маршрутизатор отправил маршрутную таблицу — всю или частично. Ответ может быть незапрашиваемым регулярным обновлением маршрутной информации или ответом на запрос. В ответах содержатся записи маршрутной таблицы. Для передачи информации из больших маршрутных таблиц используется несколько RIP-пакетов.
- **Версия.** Версия RIP. В пакетах RIP, где есть поля RIP 2 или используется аутентификация, значение такого поля равно 2.
- **Не используется.** Это поле содержит нулевое значение.
- **Идентификатор AFI.** Идентификатор семейства адреса (Address-Family Identifier). Поле AFI для RIP 2 функционирует аналогично полю AFI для RIP RFC 1058, с единственным исключением: если AFI для первой записи сообщения равно 0xFFFF, то эта запись содержит аутентификанционную информацию. В настоящее время единственным типом аутентификанционной информации является пароль.
- **Метка маршрута**. Служит для распознавания внутренних маршрутов (опознаваемых RIP) и внешних маршрутов (опознаваемых другими протоколами).
- **IP-адрес.** IP-адрес записи.
- **Маска подсети.** Маска подсети элемента. Если это поле равно нулю, то для данного элемента маска подсети не определена.
- **Следующий узел.** IP-адрес следующего узла, куда направляются пакеты.
- **Метрика.** Количество узлов (маршрутизаторов) между сетями до получателя. Эта величина находится между 1 и 15 для действительных маршрутов и равна 16 для недействительных.

Примечание

В одном пакете IP RIP допускается до 25 полей AFI, адреса и метрики. Таким образом, в одном пакете RIP может быть перечислено до 25 получателей. Если AFI определяет аутентифицированное сообщение, то в маршрутной таблице может быть определено только 24 записи. Если отдельные записи в таблице не фрагментированы на пакеты, то для протокола RIP нет необходимости в механизме упорядочения дейтаграмм, содержащих обновления маршрутной информации от соседних маршрутизаторов.

Резюме

Несмотря на солидный возраст и появление более сложных протоколов маршрутизации, протокол RIP еще далеко не устарел. RIP является развитым, устойчивым, широко поддерживаемым и легко настраиваемым протоколом. Благодаря простоте его

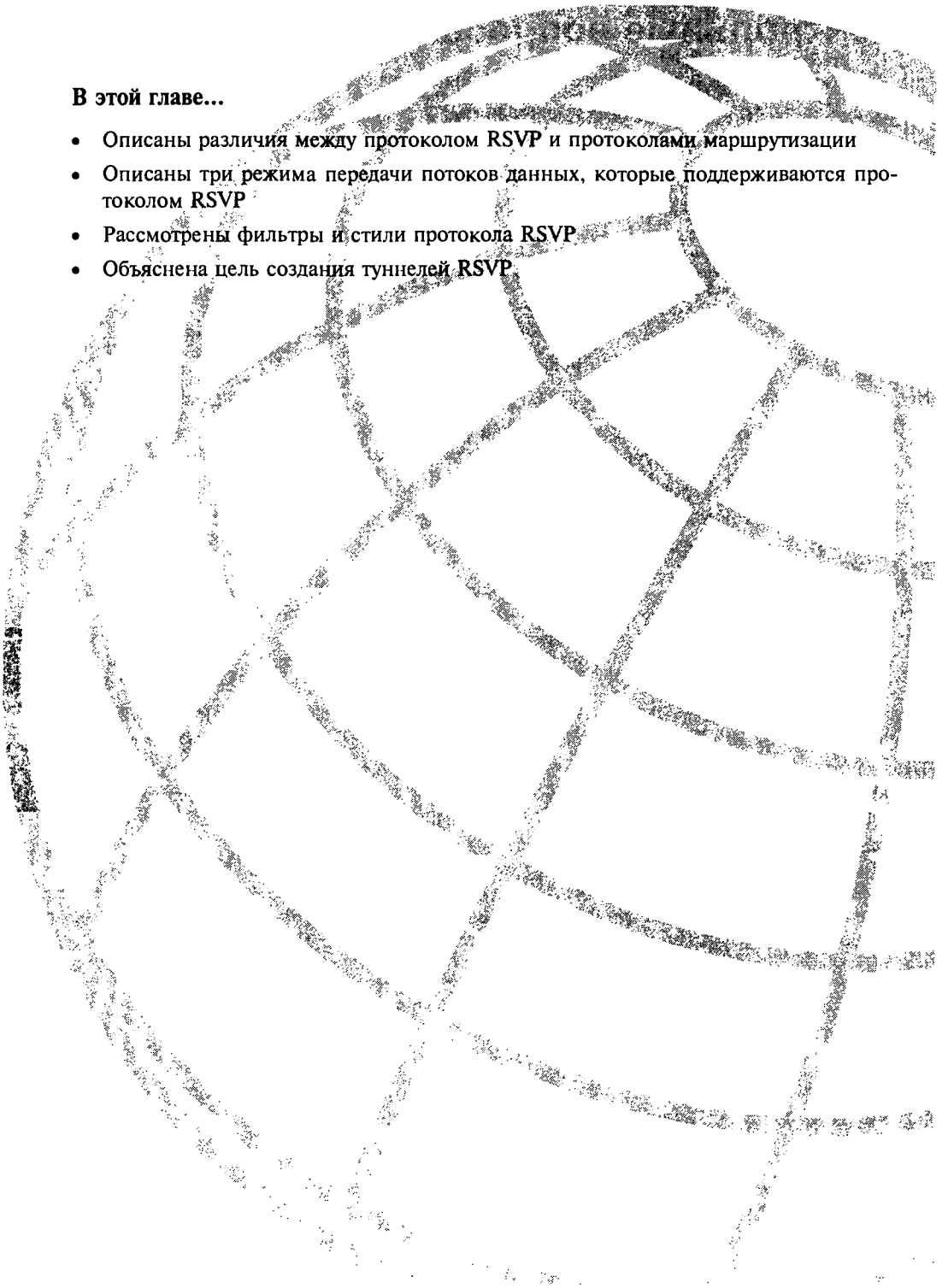
удобно использовать в тупиковых сетях и небольших автономных системах, где нет достаточного количества избыточных маршрутов, оправдывающих применение более сложных протоколов.

Контрольные вопросы

1. Каковы средства обеспечения устойчивости протокола RIP?.
2. Каково назначение таймера ожидания?
3. Какие две функции поддерживаются в версии RIP 2 и не поддерживаются в протоколе RIP?
4. Каков максимальный диаметр сети RIP?

Дополнительные источники

- Sportack M. A. *IP Routing Fundamentals.* Indianapolis: Cisco Press, 1999.
- http://www.ietf.org/rfc/rfc1058.txt
- http://www.ietf.org/rfc/rfc1723.txt
- http://www.cisco.com/cpress/cc/td/cpress/fund/ith2nd/it2444.htm



В этой главе...

- Описаны различия между протоколом RSVP и протоколами маршрутизации
- Описаны три режима передачи потоков данных, которые поддерживаются протоколом RSVP
- Рассмотрены фильтры и стили протокола RSVP
- Объяснена цель создания туннелей RSVP

Глава 50

Протокол RSVP

Введение

Протокол резервирования ресурсов (Resource Reservation Protocol — RSVP) представляет собой протокол управления сетью, позволяющий Internet-приложениям использовать различное качество обслуживания (Quality of Service — QoS) для разных потоков данных. Требуемая скорость обработки данных сетью зависит от приложения. Некоторые приложения, в том числе традиционные интерактивные и пакетные, нуждаются в надежной доставке данных, но не предъявляют строгих требований к ее своевременности. Более новые типы приложений, такие как видеоконференции, IP-телефония и другие мультимедийные коммуникации, требуют обратного: данные должны доставляться вовремя, но не обязательно с гарантией. Протокол RSVP предназначен для обеспечения в IP-сетях возможности выполнять различные требования по производительности, предъявляемые разными типами приложений.

Важно отметить, что RSVP не является протоколом маршрутизации. Он работает совместно с протоколами маршрутизации и создает вдоль маршрутов, вычисляемых при помощи последних, эквиваленты списков динамического доступа. Поэтому применение RSVP в существующей сети не требует перехода на новый протокол маршрутизации.

Первые варианты протокола RSVP были разработаны совместно Институтом научной информации (Information Sciences Institute — ISI) при Южнокалифорнийском университете (University of Southern California — USC) и исследовательским центром Xerox в Пало-Альто (Xerox's Palo Alto Research Center — PARC). Позже проблемная группа проектирования Internet (Internet Engineering Task Force — IETF) предложила открытую версию RSVP, созданную на основе версии USC и PARC. Данная версия RSVP описана в RFC 2205. В этой главе описываются функциональные возможности RSVP, касающиеся потоков данных, качества обслуживания, запуска сеансов, стиля резервирования и реализации "мягкого" состояния. Среда RSVP показана на рис. 50.1.

Потоки данных протокола RSVP

В RSVP поток данных представляет собой последовательность дейтаграмм, имеющих один источник и получатель (последний может представлять собой как одну, так и несколько физических станций). С понятием потока данных тесно связано качество об-

служивания. Требования QoS передаются по сети путем *спецификации потока (flow specification)*. Она представляет собой структуру данных, используемую узлами в объединенных сетях для запросов специальных услуг. Спецификация потока описывает уровень обслуживания потока данных. Существует три типа потоков данных, соответствующих классам обслуживания RSVP.

1. Гарантированная доставка.
2. Гарантированная скорость.
3. Гарантированная задержка.

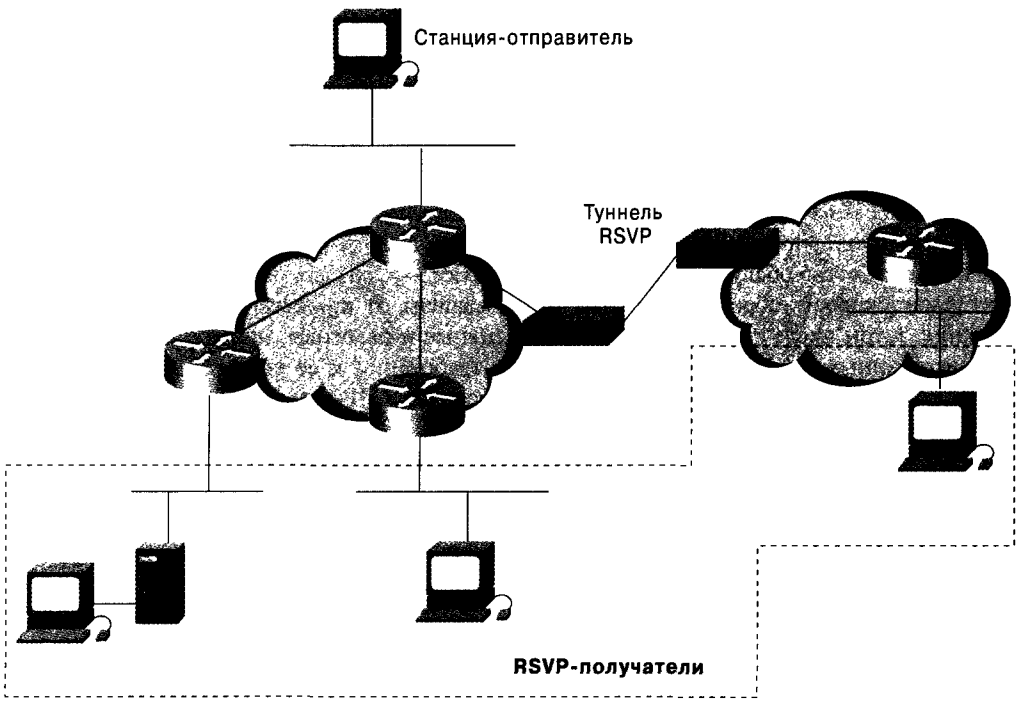


Рис. 50.1. В протоколе RSVP информация об узле доставляется получателям вместе с потоками данных

Режим негарантированной доставки (best-effort traffic) представляют собой традиционные потоки данных протокола IP. Этот режим применяется при передаче файлов (например, электронной почты), монтировании дисков, интерактивной регистрации, а также при электронных транзакциях. Эти приложения требуют гарантированной доставки данных независимо от того, сколько времени на это потребуется. Для упорядочения принятых случайным образом дейтаграмм и для запроса повторной передачи потерянных и искаженных дейтаграмм передача данных гарантированной доставки опирается на собственные механизмы протокола TCP.

Режим *гарантированной скорости (rate-sensitive traffic)* требует гарантированной скорости передачи от источника к получателю. Примером такого приложения являются видеоконференции H.323, работающие под управлением ISDN (H.320) или ATM (H.310), но применяемые также в Internet и во многих интранет-сетях протокола IP. Шифрование H.323 имеет постоянную (или почти постоянную)

скорость и требует постоянной скорости передачи, такой как в сети с коммутацией каналов. IP-сети по своей природе является сетями с коммутацией пакетов. Им не хватает механизмов для поддержки постоянной битовой скорости обслуживания потоков данных любых приложений. Протокол RSVP обеспечивает постоянную битовую скорость обслуживания в сети с коммутацией благодаря уровню обслуживания с гарантированной скоростью. Эту службу иногда называют службой гарантированной скорости.

Режим гарантированной максимальной задержки (delay-sensitive traffic) применяется к потокам данных, требующим своевременной доставки и соответствующего изменения скорости. Например, скорость передачи видео MPEG-II колеблется от 3 до 7 Мбит/с, в зависимости от того, насколько интенсивно изменяется изображение. Если на экране показывают окрашенную стену, то достаточно 3 Мбит/с, а для океанских волн потребуется 7 Мбит/с. Источник видеосигнала MPEG-II посылает ключевые и дельта-фреймы. Обычно в секунду передается 1 или 2 ключевых фрейма с изображением всей картинки и от 13 до 28 дельта-фреймов, описывающих изменения ключевого фрейма. Дельта-фреймы, как правило, значительно меньше ключевых. В результате скорость передачи фреймов может изменяется в широких пределах. Однако для нормальной работы кодека (кодера-декодера) необходимо, чтобы каждый фрейм передавался в течение заданного времени. Необходимо согласовать определенный приоритет передачи данных в дельта-фреймах. К службам RSVP, поддерживающим передачу данных с гарантированной задержкой, относятся *служба управления задержками* (не являюшаяся службой реального времени) и *прогнозирующая служба* (служба реального времени).

Обработка потоков данных по протоколу RSVP

В отличие от протоколов маршрутизации, протокол RSVP предназначен для управления потоками данных, а не для принятия решений относительно каждой дейтаграммы. Потоки данных состоят из дискретных сеансов связи между источником и получателями. Более точное определение сеанса — простой поток дейтаграмм к получателю и протокол транспортного уровня. Таким образом, сеансы идентифицируются следующими параметрами: адрес получателя, идентификатор протокола и порт получателя. Протокол RSVP поддерживает как одно-, так и многоадресатные симплексные сеансы.

Примечание

Следует обратить внимание, что сеансы RSVP являются симплексными. Таким образом, двунаправленный обмен данными между двумя станциями в действительности состоит из двух отдельных симплексных сеансов RSVP.

При многоадресатном сеансе копия каждой дейтаграммы, переданной одним источником, отправляется нескольким получателям. Одноадресатный сеанс характеризуется одним источником и одним получателем. Иногда адреса источника и получателя RSVP указывают на один и тот же Internet-узел. Однако один узел может содержать несколько логических источников и получателей, различающихся номерами портов, так что каждый номер порта соответствует отдельному приложению. Если RSVP отслеживает такую информацию о приложении, то одноадресатный сеанс может привести к передаче данных нескольким приложениям, расположенным на одном узле-получателе.

Качество обслуживания RSVP

В контексте RSVP *качество обслуживания (Quality of Service — QoS)* является атрибутом, описанным в спецификациях потока, которые используются для определения маршрута обмена данными между объектами (маршрутизаторами, получателями и источниками). Протокол RSVP используется для определения QoS узлами и маршрутизаторами. узлы используют RSVP для запросов уровня QoS потоков данных приложений. Маршрутизаторы применяют RSVP для доставки запросов QoS другим маршрутизаторам по маршруту следования потока данных. Таким образом, RSVP поддерживает состояние маршрутизаторов и узлов для предоставления запрашиваемой службы.

Запуск сеанса RSVP

Для того чтобы запустить многоадресатный сеанс RSVP, получатель первым присоединяется к многоадресатной группе, определенной IP-адресом получателя при помощи протокола IGMP. При одноадресатном сеансе одноадресатная маршрутизация выполняет ту же роль, что и IGMP совместно с адресом протокола PIM (Protocol-Independent Multicast, независимый от протокола групповой адрес) для многоадресатного сеанса. После того как получатель присоединится к группе, потенциальный источник начинает посылать сообщения по маршруту RSVP на IP-адрес получателя. Приложение-получатель получает маршрутное сообщение и начинает посылать соответствующие запросы на резервирование, определяющие желательные признаки потока, используя протокол RSVP. После получения запроса на резервирование приложение-источник начинает отправлять пакеты данных.

Стиль резервирования RSVP

Стилем резервирования называют набор управляющих переменных, которые определяют количество поддерживаемых параметров. Протокол RSVP поддерживает два основных класса резервирования: *раздельное* и *совместное*. При раздельном резервировании каждому источнику в каждом сеансе выделяется свой поток. Совместное резервирование применяется для нескольких источников, которые заведомо не пересекаются друг с другом. На рис. 50.2 показаны схемы раздельного и совместного резервирования RSVP и их назначение. Все возможные варианты "стиль/назначение" описываются ниже.

Стиль групповой фильтрации

Стиль *групповой фильтрации (Wildcard-Filter — WF)* заключается в совместном или групповом резервировании. WF-резервирование представляет собой одиночное резервирование, при котором смешиваются все источники. Резервирование можно представить как "трубу" с совместным доступом, размер которой определяется наибольшим из ресурсов, запрошенных всеми получателями данного канала, независимо от количества источников. Резервирование распространяется на все узлы источников, в том числе автоматически — на новые источники по мере их появления.

Масштаб	Резервирование	
	Раздельное	Совместное
Явное	Фиксированный фильтр (стиль FF)	Явное совместное (стиль SE)
Групповое	Не определено	Групповая фильтрация (стиль WF)

Рис. 50.2. Протокол RSVP поддерживает как совместное, так и индивидуальное резервирование

Стиль фиксированной фильтрации

Стиль *фиксированной фильтрации (Fixed-Filter — FF)* определяет индивидуальное резервирование с явным указанием масштаба. При использовании FF-стиля создаются отдельные запросы на резервирование для пакетов данных, поступающих из разных источников. Масштаб резервирования определяется явно, по списку источников. Общее резервирование канала для данного сеанса представляет собой совокупность FF-резервирований для всех источников, указанных в запросе. Запросы на FF-резервирование от разных получателей, но для одного источника, должны быть объединены для совместного резервирования в данном узле.

Стиль явного совместного резервирования

Стиль *явного совместного резервирования (Shared-Explicit — SE)* определяет совместное резервирование среды с явным указанием масштаба. При использовании SE-стиля создается одиночное резервирование, в котором смешиваются все источники. Как и при FF-резервировании, набор источников (и, следовательно, масштаб) явно определяются получателем, создающим данное резервирование.

Применение стилей резервирования RSVP

WF и SE являются вариантами совместного резервирования, подходящими для тех многоадресатных приложений, которые в силу своих особенностей не предполагают одновременной передачи данных из нескольких источников. В качестве примера можно привести аудиоконференции, где говорит одновременно только ограниченное количество людей. Каждый получатель может послать запрос на WF- или SE-резервирование для одного аудиоканала дважды (чтобы обеспечить некоторый избыток). FF-стиль создает независимое резервирование для потоков, поступающих из различных источников. FF-стиль больше подходит для видеосигналов. К сожалению, объединить совместное и одиночное резервирование невозможно.

Гибкое состояние RSVP

В любой RSVP-сети *гибким состоянием (soft state)* называется состояние, когда обновление маршрутизаторов и конечных узлов становится возможным благодаря специальным RSVP-сообщениям. Параметры гибкого состояния обеспечивают динамическое изменение членства в группах сети RSVP и настройку сети в соответствии с изменениями в маршрутизации. Обычно гибкое состояние поддерживается сетью RSVP для того, чтобы можно было изменять ее состояние без обращения к конечным точкам, в отличие от архитектуры с коммутацией каналов, где конечные точки посылают запрос и в случае сбоя повторяют его.

Механизмы протокола RSVP обеспечивают общие средства создания и обслуживания состояния распределенного резервирования многоадресатных и одноадресатных маршрутов доставки.

Для обслуживания состояния резервирования RSVP следит за гибким состоянием в узлах маршрутизаторов и узлов. Гибкое состояние RSVP создается и должно периодически обновляться запросами маршрута и резервирования. Если в течение заданного времени соответствующих сообщений обновления не поступит, то состояние удаляется. Гибкое состояние также может быть удалено в результате явного сообщения о разрыве. RSVP периодически проверяет гибкое состояние, чтобы формировать и передавать запросы об обновлении маршрутов и резервирования следующим узлам.

При изменении маршрута следующее маршрутное сообщение инициализирует состояние нового маршрута. Последующие запросы на резервирование устанавливают состояние резервирования. Состояние неиспользуемого сегмента сбрасывается по истечении установленного времени. (Спецификация RSVP требует, чтобы новое резервирование начиналось через 2 секунды после изменения топологии.)

При изменении состояния RSVP распространяет сообщения об этом по всей сети RSVP без задержки. Если полученное состояние отличается от предыдущего, то последнее обновляется. Если результат приводит к изменению генерируемых сообщений об обновлении, то такие сообщения генерируются и отправляются немедленно.

Функционирование RSVP

Под управлением RSVP сетевые ресурсы резервируются для простых (однонаправленных) потоков данных. Логически каждый источник отделен от получателя, но любое приложение может быть и источником, и получателем. Запросы на резервирование ресурсов исходят от получателей. На рис. 50.3 показана общая схема функционирования. Последовательность событий описывается в следующем разделе.

Основные операции протокола RSVP

Процесс резервирования ресурсов RSVP начинается тогда, когда домен RSVP обращается к локальному протоколу (или протоколам) маршрутизации при поиске маршрута. Узел рассылает по пути доставки многоадресатной группы сообщения IGMP для присоединения к этой группе и сообщения RSVP для резервирования ресурсов. Каждый маршрутизатор, способный принять участие в резервировании ресурсов, передает входящие пакеты данных классификатору пакетов, после чего по мере необходимости помещает их в очередь планировщика пакетов. Классификатор пакетов RSVP

определяет маршрут и класс QoS каждого пакета. Планировщик RSVP распределяет ресурсы для передачи по тому носителю канального уровня, который используется данным интерфейсом. Если этот носитель канального уровня имеет собственные средства управления QoS, то планировщик пакетов должен выполнить на канальном уровне необходимое согласование, которое обеспечит QoS, требуемое RSVP.

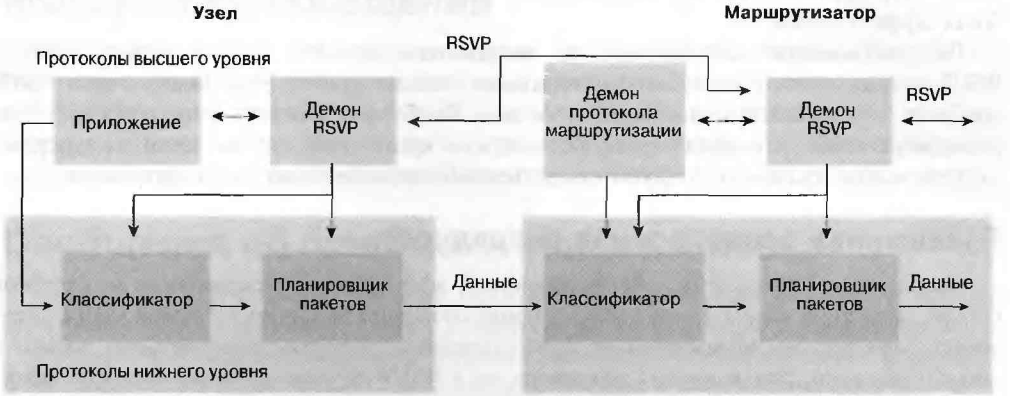


Рис. 50.3. Резервирование ресурсов для однонаправленных потоков данных в среде RSVP

Главная задача планировщика состоит в распределении ресурсов для передачи пакетов для QoS-пассивного носителя, такого как выделенная линия. Кроме того, иногда он распределяет другие системные ресурсы, например время или буферы центрального процессора. Запрос QoS, обычно поступающий от получателя главного приложения, пересылается локальной реализации RSVP в качестве демона RSVP.

Затем при помощи протокола RSVP запрос передается всем узлам (маршрутизаторам и узлам) по обратному маршруту к источнику (источникам) данных. В каждом узле программа RSVP применяет локальную процедуру принятия решения, называемую управлением доступом, чтобы определить, соответствует ли он запрашиваемому QoS. Если ответ положителен, то программа RSVP настраивает классификатор и планировщик пакетов на получение желаемого QoS. В противном случае программа RSVP возвращает приложению, от которого исходит запрос, сообщение об ошибке.

Туннели протокола RSVP

RSVP, как и любой новый протокол, невозможно распространить сразу на всю сеть Internet. Возможно, что RSVP вообще никогда не станет единым стандартом. Поэтому RSVP должен правильно работать даже в тех случаях, когда между двумя RSVP-маршрутизаторами находится несколько других маршрутизаторов. Промежуточные звенья этой цепочки, не поддерживающие RSVP, не способны резервировать ресурсы и, следовательно, не гарантируют обслуживание. Однако если эти маршрутизаторы обладают достаточной дополнительной мощностью, то они могут обеспечить приемлемое обслуживание в режиме реального времени.

Для обеспечения связи между RSVP-сетями через сети других протоколов RSVP предусматривает автоматическое создание туннелей через другие протоколы. Туннелирование требует, чтобы RSVP-маршрутизаторы и маршрутизаторы, не поддерживающие RSVP, передавали маршрутные сообщения к получателю при помощи локальной таблицы маршрутизации. Когда маршрутное сообщение про-

ходит через маршрутизаторы, не поддерживающие RSVP, оно копирует IP-адрес последнего RSVP-маршрутизатора. Сообщения с запросами на резервирование передаются следующему RSVP-маршрутизатору цепочки.

В пользу RSVP-туннелирования говорят два аргумента. Во-первых, RSVP будет использоваться скорее время от времени, чем регулярно. Во-вторых, благодаря управлению перегрузкой там, где она заведомо имеет место, туннелирование может быть более эффективным.

Распространение местами или по частям означает, что на некоторых участках RSVP начнет активно использоваться раньше, чем на других. Если бы протокол RSVP требовал непрерывной поддержки, то он был бы бесполезен без почти повсеместного распространения, что вряд ли осуществимо — кроме того случая, если уже первые эксперименты продемонстрируют существенные преимущества этого протокола.

Взвешенная равноправная очередность

Применение технологии, обеспечивающей эффективное резервирование ресурсов (такой, как схема взвешенной равноправной очередности Cisco) в "узком месте" сети может быть весьма эффективным. Туннелирование является рискованным только в том случае, если "узкое место" находится не в RSVP-домене и его невозможно обойти. На рис. 50.4 показана среда RSVP с туннелем между RSVP-сетями.

RSVP-сообщения

RSVP поддерживает четыре основных типа сообщений, кратко описанных в последующих разделах: запросы на резервирование, маршрутные сообщения, сообщения об ошибках, подтверждения, а также сообщения о разрыве соединения.

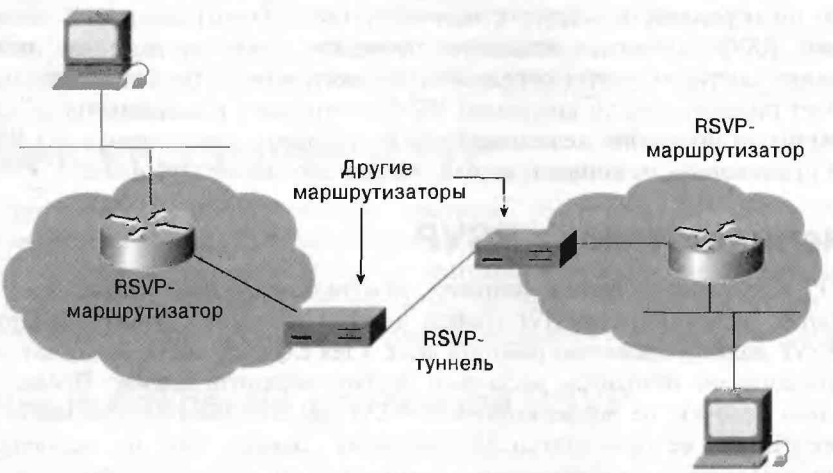


Рис. 50.4. Среда RSVP с туннелем между RSVP-сетями

Запросы на резервирование

Запрос на резервирование представляет собой сообщение, которое узел-получатель посылает источникам. Оно идет по тем же маршрутам, что и пакеты

данных, но навстречу им, к узлам-источникам. Запрос на резервирование должен быть доставлен узлам-источникам для того, чтобы они могли устанавливать соответствующие параметры управления передачей данных для первого узла. RSVP не посылает подтверждающих сообщений.

Маршрутные сообщения

Маршрутное RSVP-сообщение посылается источником по одноадресатным или многоадресатным маршрутам, определенным протоколом (или протоколами) маршрутизации. Маршрутное сообщение используется для того, чтобы сохранять состояние маршрута в каждом узле. Состояние маршрута используется для передачи в обратном направлении запросов на резервирование.

Сообщения об ошибках и подтверждения

Существуют три формы сообщений об ошибках и подтверждений: ошибки маршрута, ошибки запроса на резервирование и подтверждения запроса на резервирование.

Сообщения об ошибках маршрута формируются на основе маршрутных сообщений и направляются к источникам. Они передаются от узла к узлу по данным о состоянии маршрута. В каждом узле IP-адресом получателя служит адрес предыдущего узла.

Сообщения об ошибках запроса на резервирование формируются на основе сообщений запроса на резервирование и направляются к получателю. Эти сообщения передаются от узла к узлу, используя состояние резервирования. В каждом узле IP-адресом получателя служит адрес следующего узла. Сообщения об ошибке могут содержать следующую информацию:

- отказ в доступе;
- канал недоступен;
- служба не поддерживается;
- неправильная спецификация потока;
- неточный маршрут.

Сообщения о подтверждении запроса на резервирование посылаются в ответ на появление в запросе на резервирование объекта подтверждения резервирования. В этом сообщении содержится копия подтверждения резервирования. Сообщения о подтверждении посылаются по адресу узла-получателя и по адресу, который содержится в объекте подтверждения резервирования. Сообщение о подтверждении запроса на резервирование передается получателю по маршруту от узла к узлу, чтобы настроить механизм проверки целостности маршрута.

Сообщения о разрыве

RSVP-сообщения о разрыве (teardown messages) удаляют маршрут и отменяют состояние резервирования, не ожидая превышения лимита времени. Сообщения о разрыве могут быть вызваны приложением, работающим на конечной системе (источник или получатель) или маршрутизатором в результате истечения времени ожидания. Протокол RSVP поддерживает два типа сообщений о разрыве: *разрыв маршрута* и *разрыв запроса на резервирование.* Сообщения о разрыве маршрута удаляют состояние маршрута

(и состояние резервирования), передаются всем получателям, начиная с исходной точки, и маршрутизируются так же, как маршрутные сообщения. *Сообщения о разрыве запроса на резервирование* снимают состояние резервирования, передаются всем предшествующим отправителям начиная от точки разрыва и маршрутизируются так же, как соответствующие запросы на резервирование.

Формат пакета RSVP

Формат пакета RSVP показан на рис. 50.5. Заголовок и поля объектов, показанных на рис. 50.5, описаны ниже.

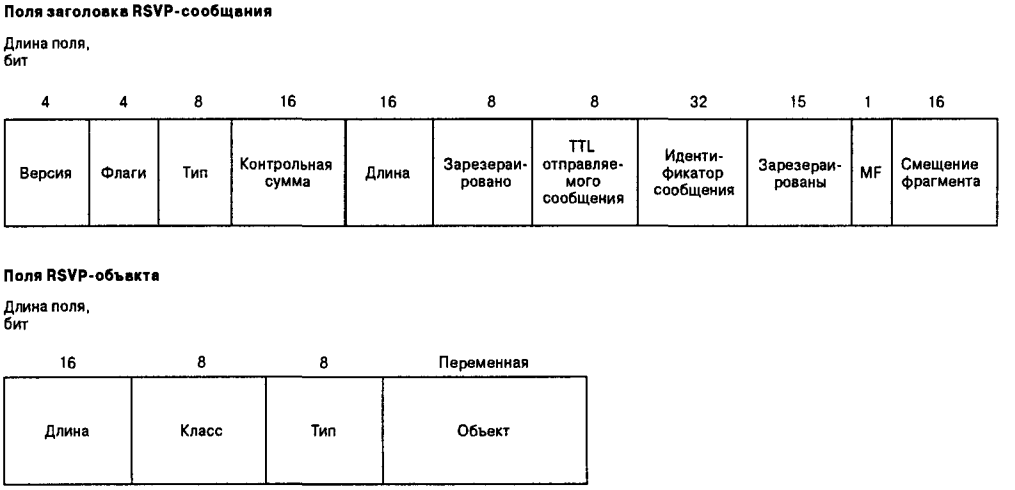


Рис. 50.5. Пакет RSVP состоит из заголовков сообщений и полей объектов

Поля заголовка RSVP-сообщения

Поля заголовка сообщения RSVP содержат следующие значения.

- **Версия.** 4-разрядное поле, в котором содержится номер версии протокола (в настоящее время это версия 1).
- **Флаги.** 4-разрядное поле. Пока эти флаги не определены.
- **Тип.** 8-разрядное поле, может принимать одно из значений (целые), перечисленных в табл. 50.1.
- **Контрольная сумма.** 16-разрядное поле, в котором содержится стандартная контрольная сумма TCP/UDP, рассчитанная для содержимого RSVP-сообщения, где в поле контрольной суммы стоит 0.
- **Длина.** 16-разрядное поле, в котором содержится длина RSVP-пакета в байтах, включая общий заголовок и следующие за ним объекты переменной длины. Если установлен флаг дополнительных фрагментов MF (More Fragments — MF) или поле смещения фрагмента содержит ненулевое значение, то в поле длины указывается длина текущего фрагмента большего сообщения.

Таблица 50.1. Типы RSVP-сообщений

Зиачение поля	Тип сообщения
1	Маршрут
2	Запрос на резервирование
3	Ошибка маршрута
4	Ошибка запроса на резервирование
5	Разрыв маршрута
6	Разрыв резервирования
7	Подтверждение запроса на резервирование

- **TTL отправляемого сообщения.** 8-разрядное поле, содержащее значение времени жизни (time-to-live — TTL) отправляемого сообщения.
- **Идентнфнкатор сообщения.** 32-разрядное поле, содержащее общую для всех фрагментов метку сообщения, которую оно имеет между двумя данными пунктами RSVP.
- **Флаг MF** (More Fragments, дополнительные фрагменты). Младший бит 1-байтового слова, 7 остальных разрядов которого зарезервированы. Флаг MF устанавливается для всех фрагментов сообщения, кроме последнего.
- **Смещенне фрагмента.** 24-разрядное поле, указывающее положение фрагмента в сообщении.

Поля объектов RSVP

Объекты RSVP имеют следующие поля.

- **Длнна.** 16-разрядное поле, содержащее полную длину объекта в байтах (всегда кратную 4).
- **Класс (Class-Num).** Идентификатор класса объекта. Каждый класс объекта имеет имя. В табл. 48.2 перечислены классы, распознаваемые любой реализацией RSVP.
- Старший бит поля класса определяет, какое действие должен выполнить узел, если класс объекта не распознан.
- **Тнп (C-type).** Тип объекта, уникальный для данного класса. Максимальная длина объекта составляет 65528 байт. Объединение полей класса и типа (включая бит флага) можно использовать для хранения 16-разрядного числа, определяющего уникальный тип объекта.
- **Содержимое объекта.** Поля длины, класса и типа определяют форму содержимого объекта. Классы объектов, которые могут быть включены в содержание объекта, описаны в табл. 50.2.

Резюме

Протокол RSVP представляет собой протокол транспортного уровня, позволяющий обслуживать потоки данных в зависимости от их специфики. Не подлежит сомнению, что разные типы приложений предъявляют различные требования к производительности.

RSVP распознает эти различия и обеспечивает механизмы, позволяющие определить, какая производительность требуется данному приложению, и изменить поведение сети соответствующим образом. Со временем, по мере совершенствования и распространения приложений, зависящих от скорости работы сети и времени задержки, потребность в RSVP будет возрастать.

Таблица 50.2. Классы RSVP-объектов

Класс объекта	Описание
Null (Нуль)	Идентификатор класса равен 0, тип игнорируется. Длина должна быть не меньше 4 и кратна 4. Нулевой объект может появляться в любом месте последовательности объектов, и его содержание игнорируется получателем
Session (Сеанс)	Содержит IP-адрес и, возможно, обобщенный порт получателя, определяющие сеанс для последующих объектов. Присутствует в любом RSVP-сообщении
RSVP Hop (Узел RSVP)	IP-адрес RSVP-узла, отправившего сообщение.
Time Values (Временные переменные)	Необязательный элемент. Содержит значения периода обновления и TTL, переопределяющие стандартные параметры
Style (Стиль)	Стиль резервирования и его параметры, не относящиеся к спецификациям потока и фильтра (которые есть в запросе на резервирование)
Flow Specification (Спецификация потока)	Требуемое QoS (указанное в запросе на резервирование)
Filter Specification (Спецификация фильтра)	Подмножество пакета с данными сеанса, которые должны получить требуемое QoS (определенное спецификацией потока в запросе на резервирование)
Sender Template (Шаблон источника)	IP-адрес источника и, возможно, некоторая дополнительная информация для демультиплексирования, идентифицирующая источник (указывается в маршрутном сообщении)
Sender TSPEC (TSPEC источника)	Параметры потока данных, исходящего от источника (указывается в маршрутном сообщении)
Adspec (Параметры объявления)	Данные объявления в маршрутном сообщении
Error Specification (Спецификация ошибки)	Описание ошибки (указывается в сообщении об ошибке маршрута или об ошибке запроса на резервирование)
Policy Data (Данные политики)	Информация для настройки модуля локальной политики, который принимает решение об административной допустимости данного резервирования (указывается в маршрутном сообщении или в запросе на резервирование)
Integrity (Целостность)	Криптографические данные для аутентификации исходного узла и, возможно, верификации содержимого данного запроса на резервирование
Scope (Масштаб)	Явное описание масштаба для передачи запроса на резервирование
Reservation Confirmation (Подтверждение резервирования)	IP-адрес получателя, который запросил подтверждение. Присутствует в запросе на резервирование и подтверждении запроса на резервирование

Контрольные вопросы

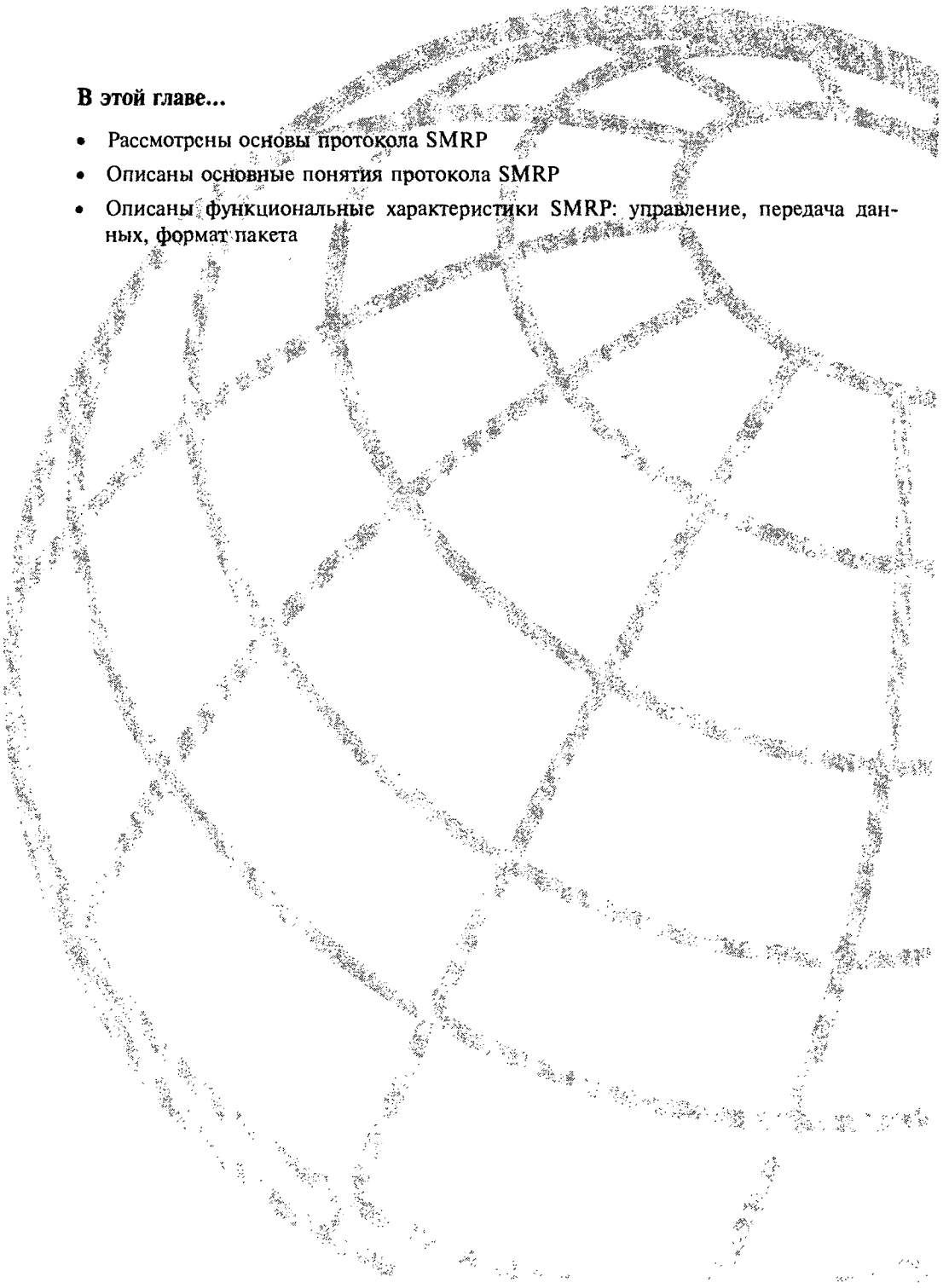
1. Обязательно ли переходить от существующего протокола маршрутизации к RSVP?
2. Назовите три уровня служб RSVP и объясните, в чем состоит различие между ними.
3. Какие существуют два класса резервирования RSVP и чем они отличаются друг от друга?
4. Что такое фильтры RSVP?
5. Как можно использовать RSVP, если в сети есть области, не поддерживающие RSVP?

Дополнительные источники

- http://www.ietf.org/rfc/rfc2205.txt
- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/rsvp.htm

В этой главе...

- Рассмотрены основы протокола SMRP
- Описаны основные понятия протокола SMRP
- Описаны функциональные характеристики SMRP: управление, передача данных, формат пакета



Глава 51

Протокол SMRP

Введение

Простой протокол многоадресатной маршрутизации (Simple Multicast Routing Protocol — SMRP) представляет собой протокол транспортного уровня для маршрутизации мультимедийных потоков данных по сетям AppleTalk. SMRP поддерживает технологию Apple Computers QuickTime Conferencing (QTC) и обеспечивает гарантированную доставку многоадресатных дейтаграмм без подтверждения соединения. Функционирование SMRP основано на протоколах сетевого уровня. В частности, SMRP облегчает передачу данных от одного источника нескольким получателям. В этой главе описываются функциональные элементы и работа протокола SMRP. На рис. 51.1 показана обобщенная SMRP-среда.

При создании протокола SMRP компания Apple позаимствовала некоторые стратегии и концепции других протоколов и технологий. В результате многие термины в среде SMRP получили другое значение. В табл. 51.1 представлен краткий обзор терминов протокола SMRP и их определения. Эти термины будут использоваться на протяжении данной главы.

Таблица 51.1. Термины протокола SMRP и их определения

Термин	Определение
Родительский адрес (port parent)	Адрес узла, обрабатывающего запросы группы
Группа (group)	Множество конечных точек-получателей, групповой адрес
Дерево источника (source tree)	Связное дерево маршрутизации в локальной сети, где маршруты направлены за пределы этой сети
Дерево получателей (destination tree)	Связное дерево маршрутизации в локальной сети с маршрутами к локальной группе
Связное дерево (spanning tree)	Связное множество маршрутов, использующих локальные сети между узлами объединенной сети, в котором между любыми двумя узлами существует только один маршрут
Локальный канал (local net)	Общедоступный канал и связанный с ним протокол сетевого уровня. Сеть LAN может поддерживать несколько локальных каналов

Окончание табл. 51.1

Термин	Определение
Обратный маршрут (reverse path)	Обратный маршрут присоединения, маршрут по дереву источника для локального канала, использованного для передачи многоадресатных данных
Маршрут присоединения (joining path)	Маршрут дерева получателей для локальной сети, позволяющий достичь исходного узла и построенный по SMRP-алгоритму маршрутизации по вектору расстояния
Порт (port)	Интерфейс локальной сети или туннеля на SMRP-маршрутизаторе
Дочерний порт (child port)	Порт, являющийся интерфейсом одного или нескольких дочерних узлов для данной группы
Родительский порт (parent port)	Порт, который является интерфейсом родительского узла данной группы
Конечная точка (endpoint)	Немаршрутизируемый источник или получатель многоадресатных пакетов
Дочерняя конечная точка (child endpoint)	Смежная конечная точка, куда из узла посылаются многоадресатные данные
Исходная конечная точка (creator endpoint)	Конечная точка, которая является инициатором запроса на создание группы и источником данных, передаваемых группе
Смежная конечная точка (adjacent endpoint)	Конечная точка в той же локальной сети, что и данный узел или конечная точка, либо узел, соединенный с данным через туннельное соединение
Конечная точка-член группы (member endpoint)	Конечная точка, принадлежащая группе
Туннель (tunnel)	Соединение "точка-точка" между узлами несмежных сетей, через маршрутизаторы, не поддерживающие SMRP
Узел (node)	SMRP-маршрутизатор
Вторичный узел (secondary node)	Узел, готовый заменить первичный в случае сбоя последнего
Дочерний узел (child node)	Соседний узел, который находится дальше от исходной конечной точки, чем данный узел или группа
Исходный узел (creator node)	Первый узел, с которого была создана группа
Назначенный узел (designated node)	SMRP-маршрутизатор, назначенный первичным или вторичным узлом
Первичный узел (primary node)	Узел локальной сети, ответственный за создание групп
Родительский узел (parent node)	Соседний узел, который находится ближе к исходному узлу, чем данный узел-член группы или группа
Смежный узел (adjacent node)	Узел в той же локальной сети, что и данный узел или конечная точка
Соседний узел (neighbor node)	Смежный узел по отношению к данному узлу-члену группы или группе, принадлежащий к дереву получателей этой группы
Узел-член группы (member node)	Узел, принадлежащий дереву получателей группы
Покинуть (leave) группу	Перестать быть членом группы
Присоединиться (join) к группе	Стать членом группы

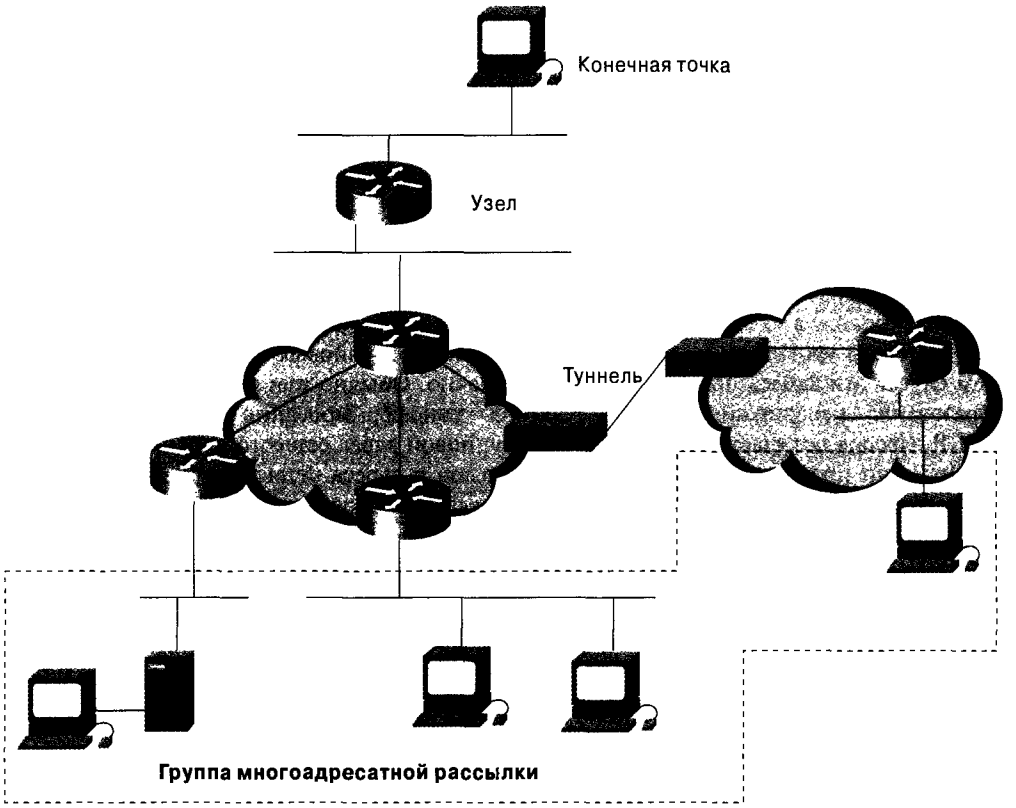


Рис. 51.1. Обобщенная схема SMRP-среды с многоадресатной группой, соединенной с конечной точкой

Многоадресатные транспортные службы SMRP

Протокол SMRP предназначен для того, чтобы маршрутизаторы и конечные станции могли передавать многоадресатные пакеты по стандартным сетевым протоколам. SMRP управляет назначением групповых адресов и позволяет отправлять данные из одного источника по уникальному групповому адресу. Получатели могут присоединяться к этой группе, если они заинтересованы в получении предназначенных для нее данных. Для поддержки этих функций SMRP использует ряд служб. Ниже будут рассмотрены ключевые процессы и технологии, лежащие в основе служб SMRP, такие как протокол многоадресатный протокол передачи (Multicast Transaction Protocol — MTP), управление узлами, управление многоадресатной маршрутизацией, передача данных и управление топологией.

Управление групповыми SMRP-адресами

SMRP-адресация основана на локальной сети исходных конечных точек. SMRP-адрес состоит из двух частей: трехбайтного номера сети и однобайтового

номера сокета. Каждая локальная сеть представлена диапазоном уникальных сетевых номеров.

Сетевые номера, назначаемые локальным сетям, должны быть уникальными во всей объединенной сети. Каждой локальной сети может быть присвоен любой непрерывный диапазон трехбайтовых номеров. Количество адресных групп, доступных в локальной сети, равно количеству ее сетевых номеров, умноженному на 254. Сетевые номера могут быть сконфигурированы или преобразованы из сетевого номера базовых протоколов сетевого уровня. Диапазоны уникальных сетевых номеров могут быть зарезервированы для поддерживаемых сетевых протоколов.

При преобразовании групповых адресов SMRP-адреса трансформируются в адреса сетевого уровня, а последние, в свою очередь, в адреса канального уровня. Каждому типу сетевого уровня должен соответствовать блок групповых адресов SMRP. В лучшем случае эти адреса преобразуются однозначно. Обычно взаимно-однозначное преобразование невозможно, и в результате трансформирования разных групповых SMRP-адресов получается один и тот же групповой адрес сетевого уровня.

Принцип преобразования групповых адресов в адреса сетевого уровня зависит от сетевого уровня. Если групповые SMRP-адреса транспортного уровня не преобразуются однозначно в групповые адреса сетевого уровня, то необходима фильтрация групповых SMRP-адресов. Если групповые адреса сетевого уровня не трансформируются однозначно в групповые адреса канального уровня, то необходима фильтрация незарегистрированных групповых адресов на сетевом уровне.

Групповые адреса сетевого уровня предварительно заданы для адресов AllEndpoints, AllNodes и AllEntities. Сообщения AllEndpoints, отправленные по этому групповому адресу, ретранслируются во все конечные точки сети; AllNodes — во все маршрутные SMRP-узлы, а AllEntities — во все конечные точки и во все маршрутные SMRP-узлы.

Протокол многоадресатной передачи SMRP

SMRP использует протокол многоадресатной передачи (Multicast Transaction Protocol — MTP), который обеспечивает три типа передачи данных: узел, конечная точка и одновременная передача в узел и конечную точку. Обмен данными между смежными узлами и между узлами и конечными точками происходит путем обмена данными типа "запрос-ответ".

Ответы всегда являются одноадресатными. В случае ошибок MTP предусматривает повторную передачу запросов или ответов. В виде многоадресатных сообщения посылаются только пакеты приветствия и запросы назначенных узлов. Остальные сообщения являются одноадресатными. Запросы из конечной точки в узел отправляются как многоадресатные, а запросы из узла в конечную точку могут быть как одно-, так и многоадресатными.

Простейшая структура MTP реализована в маршрутизаторах SMRP в виде двух очередей, через которые передаются все данные — очереди запросов и очереди ответов. Элементы очереди запросов удаляются после того, как маршрутизатор обработает полученный ответ. Ответ является обработанным, если он удовлетворяет запросу. Последнее определяется при помощи обратного вызова, определенного в элементе очереди.

После обработки ответа запрос отбрасывается. Если запрос остался без ответа, то в ответ на запрос посылается генерируемый маршрутизатором отказ с указанием ошибки MCNoResponse. Запросы могут отправляться по одиночному адресу или по групповым адресам AllNodes или AllEndpoints, в зависимости от контекста. При отсутствии явного перенаправления запросы направляются по групповому адресу AllNodes.

Элементы очереди ответов создаются по мере получения пакетов запросов. К таким элементам происходит обращение все время, пока обрабатывается запрос, и обработанный элемент остается в очереди до тех пор, пока не истечет срок его хранения. После этого он удаляется из очередности. В случае дублирования запроса, пока SMRP-маршрутизатор еще обрабатывает первоначальный запрос, повторный запрос игнорируется. Если же повторный запрос получен после окончания обработки первоначального запроса, то отправляется повторный ответ. Ответы всегда являются одноадресатными и адресованы источнику запроса. Некоторые полученные запросы требуют от узла маршрутизации SMRP генерирования дополнительных запросов. В этом случае первоначальный запрос (запросы) будет обработан функцией обратного вызова очереди запросов узла маршрутизации.

Управление SMRP-узлами

При передаче многоадресатных дейтаграмм SMRP опирается на взаимосвязи между узлами, включая назначенные, смежные и туннельные узлы.

Назначенные узлы представляет собой SMRP-маршрутизаторы, назначенные первичными или вторичными узлами. Назначенный первичный узел распределяет групповые адреса. В любой локальной сети с SMRP-узлами обязательно должен быть первичный узел. Назначенный вторичный узел необходим при наличии в локальной сети нескольких узлов. Вторичный узел необходим для хранения копии таблицы создания групп и выполняет функции первичного узла в случае его сбоя.

Основной процесс определения первичного и вторичного узлов начинается при запуске. Сначала новый узел пытается стать назначенным вторичным узлом в каждой локальной сети по очереди. Если это удается, то он пытается стать назначенным первичным узлом. Передача данных начинается по запросу первичного или вторичного узла. Отсутствие ответа на запрос говорит об успешном, а положительный ответ — о неудачном согласовании. Если сразу два узла пытаются стать назначенным первичным или вторичным узлом, то назначенным узлом становится тот из них, чей одиночный адрес принадлежит к более низкому сетевому уровню. Затем первичный узел посылает вторичному узлу локальной сети пакеты присоединения к группе и удаления из группы, чтобы сохранить идентичность таблицы создания групп.

Смежный узел данного узла или конечной точки принадлежит той же локальной сети. Периодически во все порты узлы рассылают пакеты приветствия. Если смежный узел не получит пакет приветствия в течение определенного времени, то состояние смежного узла изменится на нерабочее, а связанные маршруты отмечаются как недостижимые. Всякий раз, когда состояние порта в узле изменяется на противоположное, всем смежным узлам рассылаются пакеты уведомления. В таблице узлов, хранящейся на всех узлах, каждому смежному узлу соответствует отдельная запись. Первый раз такая запись таблицы создается, когда поступает пакет от смежного узла. В этих записях хранится время поступления последних пакетов приветствия и состояние узла.

Туннельные узлы представляет собой соединения "точка-точка" между узлами несмежных сетей через маршрутизаторы, не поддерживающие SMRP. Существует два вида туннельных узлов: туннели между узлами и туннели между узлом и конечной точкой.

В отношении использования пакетов приветствия и уведомлений туннельные узлы подобно другим смежным узлам рассматриваются как записи таблицы смежных узлов в каждом узле. Аналогичным образом SMRP позволяет включать туннельные узлы в состав групп и исключать их оттуда так же, как и другие смежные узлы.

Примечание

Cisco не поддерживает туннельные узлы. Однако протокол SMRP допускает туннелирование на сетевом уровне между несмежными узлами.

Многоадресатные маршруты протокола SMRP

При определении маршрутов многоадресатных данных протокол SMRP использует схему передачи по связующему дереву. Этот процесс основан на алгоритме маршрутизации по вектору расстояния. При запуске и изменении маршрута узел рассылает смежным узлам запросы векторов расстояния. Расстояние, заданное в векторе, представляет собой количество транзитных участков на пути к определенному диапазону сетевых адресов. Узлы содержат векторы всех записей таблицы маршрутизации и рассылают столько пакетов, сколько необходимо для рассылки всех векторов. При изменении маршрутов каждый узел рассылает запросы вектора расстояния всем смежным узлам.

Когда на порт поступает маршрут, всем портам должен быть присвоен адрес родительского порта для этого маршрута. Поскольку групповой адрес привязан к адресу сети, адрес родительского порта используется также при обработке узлом многоадресатного запроса. Если адрес родительского порта совпадает с собственным адресом узла, то обработку запроса выполняет этот узел. Из двух узлов с равными маршрутами за запрос отвечает узел со старшим сетевым адресом.

Когда узел получает запрос вектора расстояния с записями неизвестных локальных сетей, в таблицу маршрутизации узла добавляются сетевые диапазоны связанных локальных сетей, где полученное расстояние увеличивается на 1. Затем смежный узел, пославший пакет вектора расстояния, становится родительским узлом локальной сети. Запись в таблице обновляется, если получен пакет вектора расстояния для известных локальных сетей или если значение вектора расстояния, увеличенное на 1, меньше, чем значение записи в таблице маршрутизации узла. Если пакет вектора расстояния получен от смежного узла, находящегося на таком же расстоянии до локальной сети, то включается прерыватель связи. Прерыватель связи представляет собой смежный узел с более старшим одиночным адресом сетевого уровня. Такой узел идентифицируется как родительский узел для локальной сети

Управление многоадресатными группами SMRP

Членство в многоадресатных группах SMRP определяется процессом, при котором происходит согласование между конечными точками и узлами сети. Конечная точка пытается присоединиться к многоадресатной группе, обращаясь к узлу локальной сети. Узел, к которому она обращается, отвечает за присоединение к связному дереву группы, активизируя маршруты к существующему связному дереву. Узлы перемещаются из связного дерева в группы путем деактивации маршрутов, если в группе на этом маршруте не осталось ни одной конечной точки. Управление группами SMRP сводится к четырем основным процессам: созданию, присоединению, исключению и удалению.

Если конечная точка намерена начать отправку данных в группу, то она посылает назначенному первичному узлу запрос на создание группы. Первичный узел назначает неиспользуемый групповой адрес и создает запись в таблице создания групп. После этого первичный узел возвращает адрес группы исходной конечной точке и посылает вторичному узлу, если таковой существует, запрос на присоединение к группе.

Конечные точки посылают запросы для создания многоадресатной группы. Родительский узел группы в локальной сети отвечает на пакеты запросов на присоединение, посылаемые конечными точками. (Узел определяет, является ли этот узел родительским, путем проверки номера сети в адресе группы.) Когда родительский узел группы получает пакет запроса на присоединение к группе и данный узел еще не принадлежит группе, он передает запрос на присоединение исходному узлу группы. Наконец, пакет запроса на присоединение к группе доходит до узла — члена группы или исходного узла группы и по обратному маршруту отправляется пакет подтверждения присоединения к группе. Узел–член группы или исходный узел заносит в многоадресатную таблицу передачи дочерний порт, на который поступил запрос на присоединение. После того как данные пройдут обратный маршрут, они рассылаются по всем дочерним портам. Когда исходный узел получает первый запрос на присоединение к группе, он передает этот запрос исходной конечной точке, чтобы она могла начать отправку данных.

Для того чтобы покинуть многоадресатную группу, конечные точки посылают по локальному каналу пакеты запросов на исключение из группы. Родительский узел, расположенный на локальном канале, возвращает конечной точке пакет подтверждения исключения из группы и отсылает дочернему порту пакет запросов на членство в группе. Если на дочерний порт родительского узла не поступит пакет подтверждения членства в группе от узла или конечной точки, то родительский узел удаляет этот порт из записи таблицы. Если в записи родительского узла не осталось дочерних портов, то он присваивает записи состояние исключения и посылает по связному дереву к своему родительскому узлу пакет запроса на исключение из группы. Каждый соответствующий родительский узел, получив пакет подтверждения исключения из группы, удаляет запись из многоадресатной таблицы передачи.

Если конечная точка желает прекратить передачу данных группе, то она посылает запрос на удаление этой группы. На такой запрос отвечает только назначенный первичный узел.

Передача многоадресатных дейтаграмм

Передача данных SMRP заключается в пересылке узлами многоадресатных дейтаграмм по активным маршрутам дерева источников данной группы. Подмножество активных маршрутов дерева источников называется деревом распространения группы. Передача данных SMRP требует серии согласований между конечными точками и узлами. Обычно узлы получают многоадресатные дейтаграммы, когда конечные точки посылают данные группе. Исходная конечная точка, получив от исходного узла запрос на присоединение, может отправить пакеты данных своей локальной сети по групповому адресу сетевого уровня. Родительские узлы локальной сети получают этот многоадресатный пакет и передают его всем дочерним портам в многоадресатной таблице передачи. Узел выполняет многоадресатную рассылку пакета по локальной сети только в том случае, если он является родительским узлом группы в этой локальной сети и если данные поступили на родительский порт данной группы. Узлы также передают данные смежным туннельным узлам, которые принадлежат этой группе. При передаче по SNMP-туннелю многоадресатные дейтаграммы инкапсулируются в одноадресатный пакет сетевого уровня.

Обработка изменений SNMP-топологии

Протокол SNMP поддерживает карты топологии для управления маршрутами и изменениями состава групп. В среде SNMP предусматриваются некоторые типичные топологические изменения и имеет специальные технологии для их обработки.

Исчезновение конечной точки–члена группы

Для обнаружения исчезновения конечных точек–членов группы узлы периодически посылают запросы членства в группе всем активным дочерним узлам. Если родительский узел не получает подтверждения членства в группе, то он посылает своему родительскому узлу запрос на исключение из группы, после чего удаляет соответствующую запись группы.

Группы с циклами

Для обнаружения групп с циклами исходные узлы периодически отправляют исходным конечным точкам запросы на создание группы. Если после нескольких попыток исходный узел не получает подтверждения создания группы, то последняя удаляется. Обновление сетевых таблиц маршрутизации происходит путем отправки узлами своим смежным узлам векторов расстояния в случае изменения маршрута. Таким образом узлы изменяют маршрутизацию многоадресатной группы в соответствии с изменениями топологии.

Пример передачи данных SNMP

Типичный сеанс передачи данных по протоколу SNMP заключается в создании группы рабочей станцией Macintosh, присоединения к этой группе других рабочих станций Macintosh и собственно передачи данных членам такой группы.

При типичном SNMP-сеансе обмена данными компьютер Macintosh (назовем его Creator-Mac) посылает всем узлам данной сети запрос на создание группы. Первичный маршрутизатор (Primary) локальной сети выбирает неиспользуемый групповой адрес и возвращает этот адрес Creator-Mac. Macintosh в удаленной сети (назовем его Member-Mac) обнаруживает Creator-Mac по протоколу протокол связи имен (Name Binding Protocol — NBP).

Затем Creator-Mac отправляет NBP-ответ с адресом группы. Member-Mac посылает всем узлам запрос на присоединение к группе. Удаленный маршрутизатор (назовем его маршрутизатор M), зная корректный маршрут к группе и корректный родительский порт, передает запрос на присоединение к группе маршрутизатору Primary.

Primary получает запрос на присоединение к группе и посылает его Creator-Mac. Он также заносит входящий порт в запись группы в таблице передачи. Creator-Mac подтверждает запрос на присоединение к группе и посылает данные этой группе. Маршрутизатор Primary получает данные и передает их дочерним портам группы.

Наконец, данные поступают на маршрутизатор M, который находит группу в таблице передачи и рассылает многоадресатные данные. Затем Member-Mac получает данные группы.

Формат SMRP-пакета

Общий формат SMRP-пакета представлен на рис. 51.2.

Рис. 51.2. Общий вид SMRP-пакета

Ниже описаны поля SMRP-пакета, показанные на рис. 51.2.

- **Версия протокола.** Версия SMRP.
- **Тип.** Состоит из двух подполей. Старшие 2 бита определяют, содержатся ли в пакете передаваемые данные и, если содержатся, — тип передачи. Младшие 6 бит определяют тип пакета.
- **Порядковый номер.** Определяет соответствие ответов запросам во избежание дублирования запросов и ответов. Все типы пакетов имеют ненулевой порядковый номер (за исключением многоадресатных пакетов данных и пакетов приветствий).
- **Групповой адрес.** Служит назначенным первичным узлом и назначает групповые адреса всем многоадресатным источникам локальной сети. У локальной сети может быть несколько сетевых номеров, но эти номера должны образовывать непрерывный диапазон. Во избежание коллизий групповых адресов сетевые номера, назначаемые узлами, должны быть уникальными для каждой локальной сети и каждого первичного узла. Когда первичный узел назначает новый групповой адрес, от выбирает в качестве сетевого номера случайным образом первый неиспользуемый групповой адрес.
- **Данные.** Зависят от типа SMRP-пакета. Характеристики данных для различных SMRP-пакетов представлены в табл. 51.2.

Таблица 50.2. Характеристики данных SMRP-пакетов

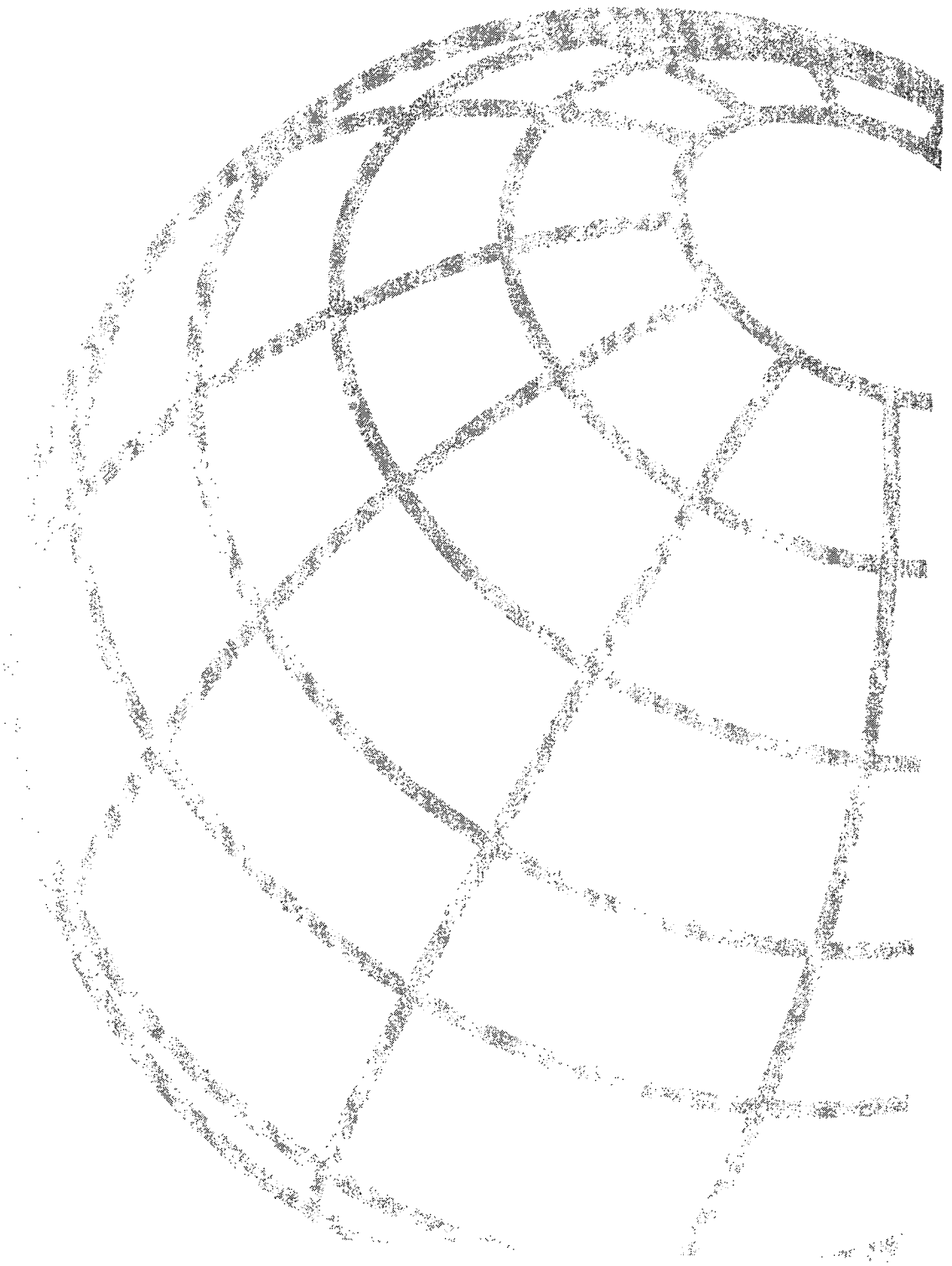
Тип пакета	Данные	Размер, байтов
Многоадресатные данные	Данные	Переменный, в зависимости от размера дейтаграммы сетевого уровня
Приветствие	Состояние порта	2
Уведомление	Состояние порта	1
Назначенный узел	Нет	0
Вектор расстояния	Многоадресатный вектор	8
Создание группы	Нет	0

Окончание табл. 51.2

Тип пакета	Данные	Размер, байт
Уничтожение группы	Нет	0
Присоединение к группе	Нет	0
Создание записи группы	Одиночный адрес сетевого уровня	Переменная, в зависимости от формата адреса сетевого уровня
Удаление группы	Нет	0
Исключение из группы	Нет	0
Ответ исходного узла	Нет	0
Ответ узла-члена группы	Нет	0
Отказ	Индикация ошибки	Короткое целое число в интервале от -7700 до -7710, в зависимости от ошибки

Контрольные вопросы

1. Что представляет собой SMRP-адрес?
2. Сообщение какого типа посылается при запросе между конечной точкой и узлом? Между узлом и конечной точкой?
3. Как узел становится назначенным первичным узлом в сети?



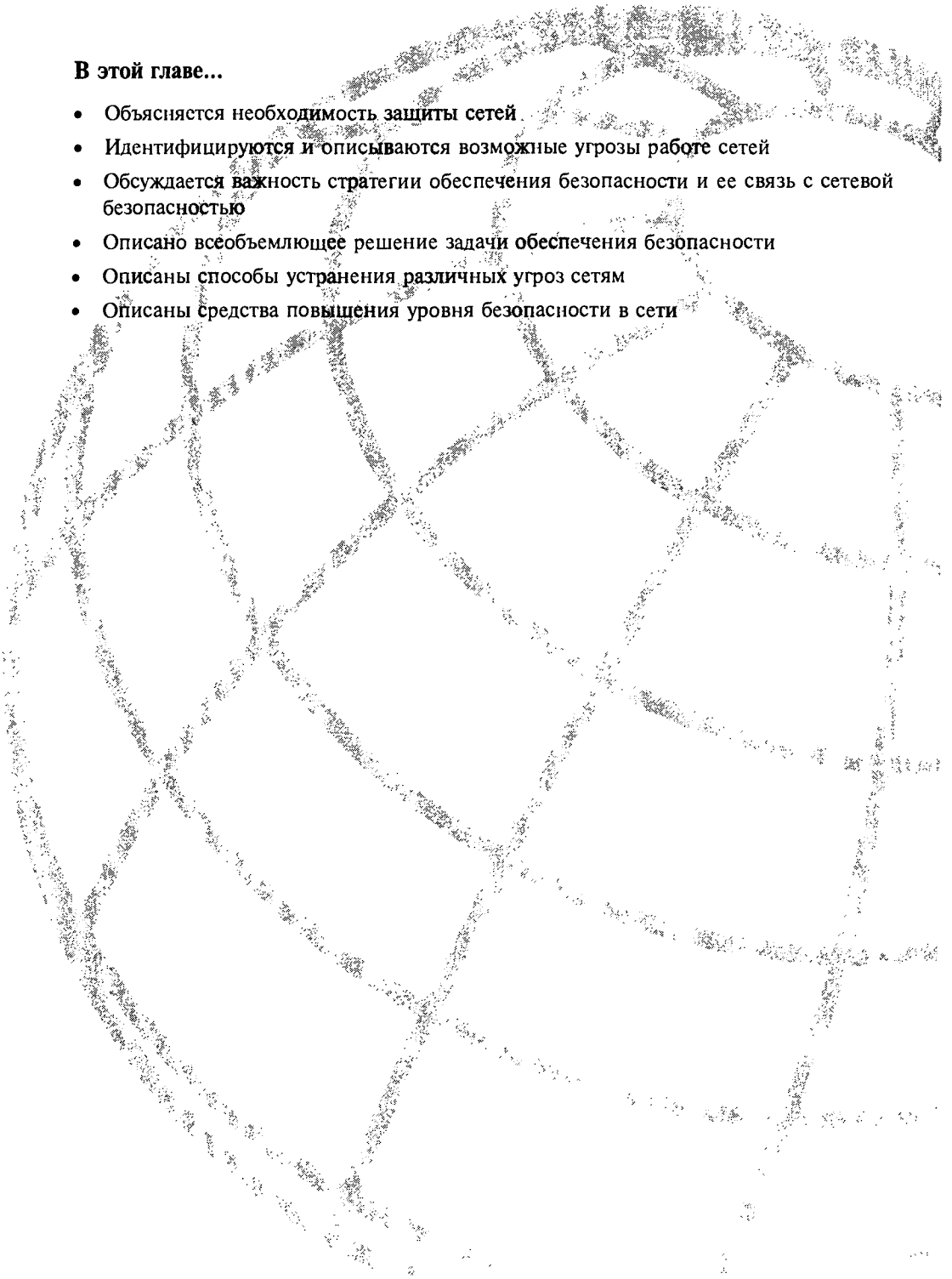
Часть VIII

Управление сетями

Глава 52. Технологии защиты сетей
Глава 53. Сетевые каталоги
Глава 54. Технологии сетевого кэширования
Глава 55. Сети для хранения информации
Глава 56. Управление сетями IBM
Глава 57. Удаленный мониторинг
Глава 58. Протокол SNMP
Глава 59. Качество обслуживания

В этой главе...

- Объясняется необходимость защиты сетей
- Идентифицируются и описываются возможные угрозы работе сетей
- Обсуждается важность стратегии обеспечения безопасности и ее связь с сетевой безопасностью
- Описано всеобъемлющее решение задачи обеспечения безопасности
- Описаны способы устранения различных угроз сетям
- Описаны средства повышения уровня безопасности в сети



Глава 52

Технологии защиты сетей

Сеть Internet прошла путь от простого средства передачи файлов до средства связи, используемого для покупки автомобилей, выписки рецептов, взятия ссуды для покупки дома и для оплаты счетов. Вместе с тем коммерческие и финансовые компании осознали, что для эффективного использования своих сетей они должны обеспечить их безопасность. Правительственные органы также оказались перед необходимостью обеспечить конфиденциальность индивидуальной частной информации при ее использовании третьей стороной, такой как медицинские учреждения или финансовые организации.

В настоящей главе обсуждаются возможные угрозы сетям и принципы всесторонней защиты при отражении этих угроз.

Почему важно обеспечить безопасность сети?

Компьютерные сети предоставляют компаниям и отдельным пользователям значительные возможности и преимущества. Для онлайновых книжных магазинов доступность Internet позволяет пользователям купить книгу в любое время и любом месте земного шара. Студенту в Южной Африке серверы австралийской компании онлайнового обучения позволяют закончить курс пройдя практическое обучение. В конечном итоге сетевая безопасность жизненно важна как для провайдера, так и для конечного пользователя. В настоящем разделе основное внимание уделяется следующим факторам, которые часто требуют защиты сетей.

- рост применения Internet-приложений;
- более быстрый доступ к Internet;
- требования законодательства.

Internet-приложения прошли путь от электронной почты до потокового видео и онлайновых банковских операций.

Появление этих новых приложений создало почву для того, чтобы хакерское сообщество обнаружило и стало использовать новые уязвимые места в сетевых системах. Эти уязвимые места включают в себя возможность кражи паролей, вызывающей нарушение работы службы и возможность несанкционированного доступа к системным ресурсам.

Более быстрый доступ к Internet для домашних пользователей с помощью цифровых абонентских каналов (Digital Subscriber Line — DSL) и кабельных технологий еще более расширил границы этой уязвимости. В настоящее время персональные компьютеры домашнего пользователя более подвержены атакам, ранее обычно проводившимся против корпоративных компьютеров, поскольку эти домашние компьютеры "всегда включены".

Кроме того, более быстрый доступ к Internet помог компаниям повысить производительность труда, побуждая своих сотрудников работать на дому. Наличие рабочей станции дома у сотрудника расширяет границы сети компании за пределы помещений компании, однако в результате этого компания сталкивается с дополнительными угрозами безопасности.

Правительственные органы также осознали важность безопасности в сетях и ту огромную роль, которую она играет в экономической жизни и в инфраструктуре страны, в частности, в таких сферах, как транспорт, системы водоснабжения, системы действий в чрезвычайных ситуациях и в сфере обороны. В результате этого было разработано и принято законодательство, требующее, чтобы в сетях были реализованы соответствующие меры безопасности. Например, в США акт защиты конфиденциальности информации о здоровье граждан (Health Information Privacy Protection Act — HIPPA) требует, чтобы провайдеры медицинских учреждений соблюдали конфиденциальность историй болезни граждан. Европейский Союз (European Union — EU) принял директиву ЕС о защите данных, которая описывает требования к защите персональных данных.

Различные виды угроз безопасности сетей

В настоящем разделе описаны наиболее типичные случаи угрозы безопасности сетей:

- несанкционированный доступ к сети;
- низкий уровень аутентификации;
- взлом паролей;
- атаки с использованием анализаторов пакетов;
- атаки на уровне приложений;
- вирусы, черви и "троянские кони";
- подделка IP-адресов;
- атаки типа "отказ в обслуживании".

Несанкционированный доступ

Под этой угрозой общего типа понимается использование любой системы без согласия ее владельца, простирается от использования сети компании для установки на сервер онлайновой игры для многих игроков до похищения хакером личной информации домашнего пользователя с его персонального компьютера.

Низкий уровень аутентификации

Эта угроза безопасности обусловлена тем, что система не требует аутентификации, либо имеющийся механизм аутентификации обеспечивает низкий уровень безопасности или вообще ее не обеспечивает. Примером низкого уровня аутентификации могут служить Web-приложения, которые позволяют любому пользователю добавлять в систему учетные записи без предварительной аутентификации в качестве системного администратора.

Внимание!

Во многих системах имеются достаточно строгие механизмы аутентификации, однако они часто не используются.

Пароли

Пароли часто являются первой линией обороны от хакерских атак. Пароли используются для аутентификации и авторизации пользователей. Атакующие часто опираются на тот факт, что пользователи назначают слишком простые пароли или используют один и то же пароль на нескольких системах. Системы генерируют пробные пароли (hashes) основываясь на таких алгоритмах, как MD5. Пользователь вводит пароль который затем используется для входа в систему. Этот пароль пользователи пытаются взломать. Слишком простые пароли легко могут быть взломаны с использованием различных средств взлома паролей. Эти средства используют два основных метода для взлома: метод грубой силы или метод словаря. В методе грубой силы используются произвольные комбинации букв, цифр и специальных символов для генерации пробных паролей. В методе словаря для взлома паролей используется список слов для генерирования пробных паролей. При применении обоих методов пробный пароль сравнивается с паролем, сгенерированном системой. Если сравнение дает положительный результат, то пароль оказывается взломанным.

Анализаторы пакетов

Анализаторы пакетов (Packet sniffers), также называемые сетевыми анализаторами (network sniffers), представляют собой приложения, которые перехватывают пакеты, проходящие по кабелю.

Внимание!

Анализаторы способны перехватывать пакеты от всех устройств, находящихся в одном и том же широковещательном домене.

Первоначально анализаторы пакетов применялись в основном для анализа потоков данных в сети с целью определения требований к полосе пропускания и обнаружения проблем в сети. Однако позднее хакерское сообщество разработало анализаторы пакетов, предназначенные для перехвата чувствительной информации, такой как пароли, с целью ее использования для получения несанкционированного доступа к системе. Эти анализаторы пакетов, как правило, перехватывают только пакеты сеансов, связанных с протоколами и приложениями, в которых требуется пароль (такими, как Telnet, FTP, HTTP и POP).

Уровень приложений

При атаках на уровне приложений делается попытка воспользоваться уязвимыми местами в установленном в сети программном обеспечении. Типичным уязвимым состоянием в приложениях является переполнение буфера. Оно возникает при попытке сохранить в буфере больше данных, чем позволяет имеющееся в нем свободное место. Переполнение буфера обычно предоставляет атакующей стороне механизм выполнения опасного для системы кода с привилегиями уровня сетевого администратора или с привилегиями базового уровня.

Внимание!

Технические детали процесса переполнения буфера подробно описаны в книге Алефа Ван (Aleph One) "Smashing the Stack for Fun and Profit".

Вирусы, черви и "троянские кони"

Вирусом называется скрытая, самодублирующаяся часть компьютерного программного обеспечения, обычно написанная с недоброжелательными целями, которая распространяется путем заражения (т.е. вставкой собственной копии) другой программы. Вирус не является самостоятельно работающей программой; для того, чтобы вирус активизировался, необходим запуск содержащей его программы. Вирусы обычно распространяются через приложения к электронным сообщениям (e-mail), через документы текстовых процессоров и рабочие листы электронных таблиц. Вирус внедряется в эти приложения и заражает систему когда пользователь выполняет соответствующее приложение. Примерами вирусов могут служить Melissa, BugBear или Klez.

Червем (worm) называется компьютерная программа, которая может работать самостоятельно или распространять свою полную рабочую версию (копию) на другие рабочие станции сети. Такая программа может разрушительным образом потреблять ресурсы компьютера. Часто черви рассматриваются как разновидность вирусов. Например, производители антивирусных программ включают червей в свои вирусные базы данных. Примерами червей могут служить Nimda, CodeRed, Slapper или Slammer.

"Троянским конем " (Trojan horse) называют компьютерную программу, которая выглядит как программа, выполняющая полезную функцию, но также имеет скрытую и потенциально опасную функцию, которая не обнаруживается механизмами безопасности. Иногда для этого используется легальная авторизация системного элемента, который вызывает эту программу.

Подделка IP-адреса

Атака, связанная с подделкой IP-адреса характеризуется тем, что хакер, находящийся в сети или вне ее, пытается представить себя санкционированным пользователем. Он может сделать это одним из двух способов: использовать IP-адрес из диапазона внутренних легальных сетевых адресов или авторизованный внешний IP-адрес, с которого разрешен доступ к некоторым ресурсам системы. Атака, связанная с подделкой IP-адреса, часто служит отправной точкой для атак иного типа.

Атака типа "отказ в обслуживании"

Атак типа "отказ в обслуживании" (Denial of Service — DoS) боятся более всего, поскольку простой сети означает потерю доходов. Целью атаки DoS является полное или частичное лишение легитимного пользователя возможности доступа к системным ресурсам. Простая форма DoS-атаки может быть осуществлена путем грубого взлома пароля, в результате чего становится возможной блокировка учетных записей пользователей. Это легко может быть сделано с одной атакующей станции. DoS-атаки включают в себя рассылку большого количества нежелательных пакетов в атакуемую сеть с подделанного IP-адреса.

Новая форма DoS-атаки — распределенный отказ в обслуживании (Distributed Denial of Service — DDoS) появилась в 2000 году. DdoS-атака использует ресурсы различных систем при посредстве агентского программного обеспечения, управление которым осуществляется с ведущей системы. Это позволяет передавать в атакуемую сеть большее количество пакетов.

Политика безопасности

Политика безопасности определяет цели и способы обеспечения безопасности в сети. Она, как правило, включает в себя следующие аспекты:

- политика допустимого использования сети;
- политика использования паролей;
- политика пользования электронной почтой и выхода в Internet;
- меры, предпринимаемые в случае инцидентов в сети;
- политика доступа к сети удаленных пользователей;
- политика в сфере extranet-соединений;
- политика использования общедоступных служб.

Политика допустимого использования сети (acceptable use policy — AUP) определяет, какие действия пользователя в сети являются разрешенными и неразрешенными. Она также определяет ответственность авторизованных пользователей. Например, политика AUP может предусматривать обязательное ежедневное выполнение антивирусной программы.

Политика использования паролей определяет какие пароли являются надежными, частоту смены паролей и определение круга лиц, имеющих доступ к системным паролям. Например, политика использования паролей может требовать, чтобы пароль маршрутизатора состоял из 10 символов и менялся каждые три месяца, а также в каждом случае, когда системный администратор прекращает работать в компании.

Политика использования электронной почты и выхода в Internet (e-mail and Internet policy — EIP) определяет каким пользователям предоставлено право пользования электронной почтой и право выхода в Internet. Например, политика EIP может предусматривать, что электронная почта может использоваться только для коммерческих целей, а доступ к Internet ограничен рабочими местами сотрудников, которым это необходимо для выполнения служебных обязанностей.

Процедуры поведения в ситуациях угрозы безопасности сети и соответствующие предпринимаемые меры определяют, что должны делать сотрудники компании в случае инцидентов в сети, таких как заражение вирусом или попытка несанкциониро-

ванного доступа к сети. Процедуры поведения в случае попытки несанкционированного доступа к сети определяют к кому и каким образом следует обращаться, если обнаруживается такая попытка.

Политика доступа к сети удаленных пользователей (remote user access policy — RAP) определяет, каким образом сотрудники компании получают доступ к корпоративной сети компании из небезопасной сети, такой, например, как сеть Internet-провайдера. Политика RAP может, например, потребовать, чтобы для получения доступа с домашнего компьютера к корпоративной сети или к сетевым ресурсам каждый удаленный пользователь использовал клиентское программное обеспечение виртуальных частных сетей (Virtual Private Network — VPN) и одноразовые пароли (one-time password — OTP).

Политика в сфере extranet-соединений (extranet connection policy — ECP) определяет каким образом создаются соединения с бизнес-партнерами. Политика ECP может, например, определять, что партнерам разрешено осуществлять соединение с корпоративным сайтом только путем создания между сайтами VPN-туннеля с использованием стандарта тройного шифрования данных (Triple Data Encryption Standard — 3DES).

Политика допустимого использования общедоступных служб (allowed public services policy — APP) определяет, какие сетевые службы являются доступными из Internet. Как правило общедоступными службами являются FTP, SMTP, HTTP и DNS. Политика APP может предусматривать, что служба DNS доступна только базовым DNS-серверам.

Поэтапное решение задачи обеспечения безопасности

Традиционное решение проблемы обеспечения безопасности является точечным решением или решением для одного устройства. Принцип такой защиты формулируется следующим образом: "Необходимо обеспечить безопасность сети или установить брандмауэр, что решает проблему защита сети". В настоящее время сетевое сообщество, постоянно сталкиваясь с проблемами защиты сетей, пришло к выводу, что обеспечение безопасности в сети, как и любой коммерческий процесс, осуществляется поэтапно.

Кольцо безопасности, показанное на рис. 52.1, иллюстрирует рекомендуемый процесс поддержки безопасности в сети. Центром кольца является политика обеспечения безопасности. Ее реализация включает в себя описанные ниже этапы:

Этап 1. Обеспечить безопасность сети. Для этого следует реализовать все механизмы защиты, определенные политикой защиты. Например, потребовать аутентификации для всех маршрутизаторов и коммутаторов сети.

Этап 2. Выполнить мониторинг сети. Установить программное обеспечение, такое как система обнаружения вторжения (intrusion detection system — IDS) для наблюдения за функционированием сети. В частности, можно установить сетевую систему IDS для наблюдения за потоками данных, которым разрешено прохождение через Internet-брандмауэр.

Этап 3. Протестировать безопасность сети. Необходимо регулярно тестировать безопасность сети для нахождения новых уязвимых мест. Для этого следует пригласить консультанта со стороны или использовать программное обеспечение сканера уязвимых мест для их нахождения и определения эффективности механизмов защиты, реализованных на первом этапе обеспечения безопасности. Популярным средством разметки сети является программа Nmap ("network mapper").

Этап 4. Повысить уровень безопасности в сети. Основываясь на результатах тестирования повысить степень защиты сети. Например, если на этапе тестирования было

обнаружено уязвимое место в программном обеспечении Web-сервера, то следует установить соответствующее программное исправление (patch) в соответствии с рекомендациями производителя.

Рис. 52.1. Кольцо безопасности

Стратегию концентрической защиты можно сравнить с ремнем и подтяжками. Если ремень расстегнулся, то подтяжки не дадут упасть брюкам. В сетях в качестве ремня может выступать фильтрующий маршрутизатор, а в качестве подтяжек выступает приложение брандмауэра. Иными словами, не следует полагаться только одну линию защиты. Каждая линия обороны обеспечивает дополнительную защиту на случай если предыдущая линия обороны вышла из строя или была взломана. На рис. 52.2 проиллюстрировано концентрическое решение.

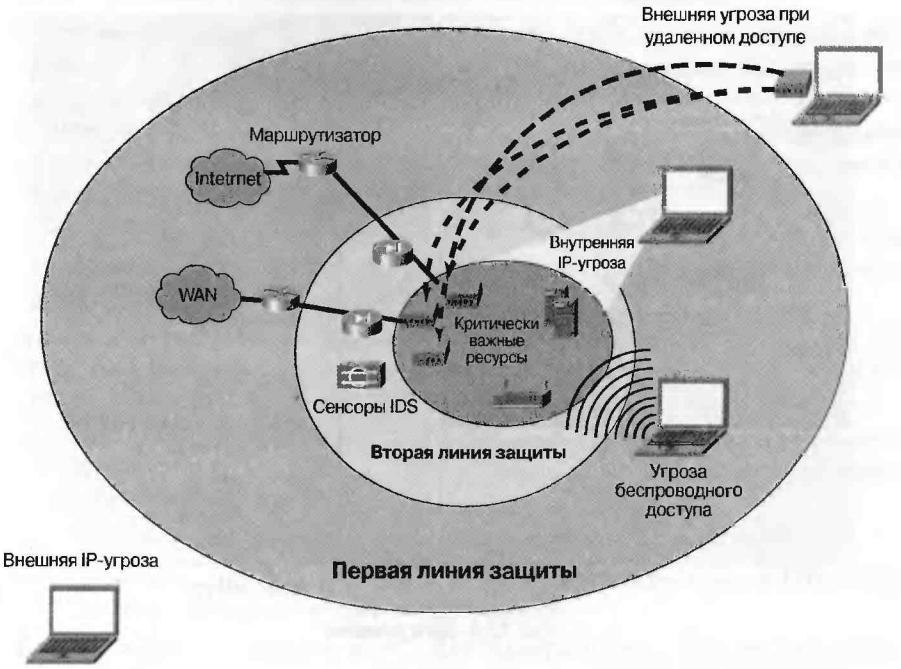


Рис 52.2. Линии защиты

На рис. 52.2 первой линией защиты сети являются фильтрующие маршрутизаторы-брандмауэры. Второй линией обороны являются выделенные брандмауэры и IDS-сенсоры. Критические ресурсы, такие как серверы, дополнительно защищены IDS на рабочих станциях, которые являются окончательной линией защиты.

Стратегия концентрической защиты строится на основе того, что сеть имеет несколько периметров или зон. Политика защиты сети определяет уровень защиты, который должен быть реализован в каждой зоне. Каждая зона защищает устройства, которые требуют различных уровней защиты, а между зонами требуется использовать дополнительные технологии защиты. При необходимости зоны могут быть подразделены на подзоны. На рис. 52.3 показана сеть, разделенная на зоны и подзоны.

Внимание!

На протяжении всей настоящей главы термин "зона " используется вместо термина "периметр".

Первичными зонами на рис. 52.3 являются Internet и Campus. Зона Internet подразделена на логические зоны меньшего размера (подзоны) — Public Services и WAN. В зоне Internet имеются устройства, которые имеют доступ к Internet. Серверы в зоне Public Services обеспечивают пользователям Internet сетевые службы, такие как HTTP и FTP. В зоне Internet защита осуществляется с помощью фильтрующих маршрутизаторов, приложения брандмауэра и программного обеспечения для обнаружения вторжений в сеть. В зоне Public Services используется обнаружение вторжения на рабочих станциях в качестве механизма дополняющего механизм защиты, реализованный в зоне Internet.

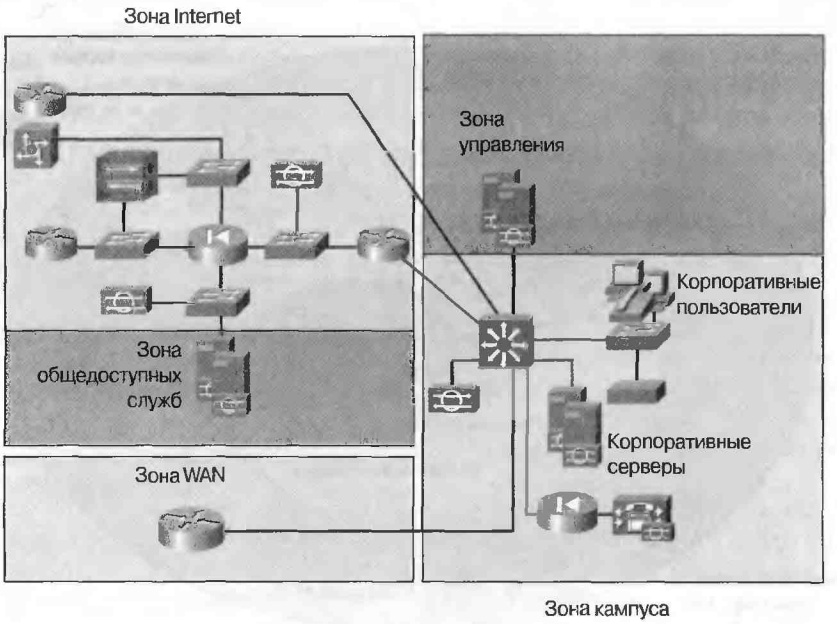


Рис 52.3. Зоны защиты

Ослабление угроз безопасности сетей

Не все угрозы безопасности сети могут быть полностью устранены; в этом причина того, что в настоящем разделе основное внимание уделено ослаблению угроз сетям. В конечном итоге компании должны использовать политику защиты для определения приемлемого риска и методы ослабления всех возможных угроз. Ниже приведены рекомендуемые методы ослабления установленных угроз.

- **Несанкционированный доступ.** Следует реализовать соответствующий контроль доступа, определяющий, каким потокам данных разрешено поступать в сеть и выходить из нее.
- **Ненадежная аутентификация.** Следует потребовать использования паролей на всех сетевых устройствах. В средах, где требуется надежная аутентификация, следует реализовать механизмы аутентификации, такие как OTP или биометрический анализ.
- **Ненадежные пароли.** Следует реализовать систему создания надежных паролей. Надежный пароль должен иметь длину от 7 до 14 символов и не должен включать в себя имеющиеся в словарях слова или сленговые термины. Следует установить срок действия паролей и контроль истории для того, чтобы от пользователей периодически требовалось менять пароли и не использовать пароли повторно. Большинство операционных систем позволяют реализовать политику надежных паролей.
- **Использование анализаторов пакетов.** Все данные, передаваемые открытым текстом, могут быть перехвачены анализатором пактов. Для уменьшения этой угрозы применяются приведенные ниже стандартные методы.
  - **Надежная аутентификация.** Использование OTP-паролей уменьшает вероятность использования перехваченных пролей, поскольку они используются лишь один раз.
  - **Коммутация.** Использование коммутаторов уменьшает непосредственную угрозу того, что анализатор пакетов poses в сети, в которой установлены концентраторы.
  - **Шифрование.** В сетях, которым требуется особо надежная защита, следует использовать механизмы шифрования; в частности рекомендуется использовать механизмы протокола IP Security (IPSec).
- **Атаки на уровне приложений.** Атаки уровня приложений не могут быть полностью исключены. Новые уязвимые места обнаруживаются практически ежедневно. Ниже приведены общие методы уменьшения такой угрозы.
  - Следует постоянно быть в курсе процесса поиска уязвимых мест используемых приложений; для этого рекомендуется подписаться на рассылку производителя.
  - Установить программные заплатки, связанные с защитой системы.
  - На рабочих станциях и в сети в целом следует использовать IDS для обнаружения атак против серверов приложений.
- **Вирусы, черви и "троянские кони".** Для защиты настольных систем адекватную защиту обеспечивает антивирусное программное обеспечение. На настольных

системах могут быть установлены персональные брандмауэры. На серверах, требующих дополнительной защиты могут быть использованы host-based IDS.

- **Подделка IP-адресов.** Рекомендуется реализовать соответствующую входную и выходную фильтрацию, как рекомендуется в RFC 2827. Также целесообразно использовать фильтрацию адресов согласно RFC 1918
- **Отказ в обслуживании.** В дополнение к входной и выходной фильтрации рекомендуется согласовать с Internet-провайдером свои действия по ограничению скорости передачи на маршрутизаторе Internet-провайдера. Такое ограничение можно также реализовать на граничном маршрутизаторе корпоративной сети. Следует включить функции анти-DoS, которые контролируют количество соединений, разрешенных конкретной рабочей станции.

Средства защиты сетей

Важнейшим аспектом обеспечения безопасности сети является знание того объекта, который необходимо защитить. Многие проблемы безопасности возникают вследствие того, что уязвимое устройство включается в сеть без уведомления обеспечения безопасности этом сетевого администратора. Для того , чтобы быть уверенным в том, что известны все имеющиеся в сети устройства и доступные службы, необходимо выполнить полную инвентаризацию сети. Для проведения такой инвентаризации обычно используются устройства сканирования портов. Ниже описаны базовые функции сканера порта.

- Сканер порта посылает эхо-пакеты Internet-протокола управляющих сообщений (Internet Control Message Protocol (ICMP) для обнаружения всех имеющихся в сети устройств. Это обычно называется ping sweeping сети.
- Он посылает пакеты запросов на соединение протокола транспортного управления (Transport Control Protocol (TCP) для определения доступных общих TCP-служб, таких как HTTP, FTP Telnet.
- Сканер рассылает устройствам сети потоки данных протокола пользовательских дейтаграмм (User Diagram Protocol — UDP) для выяснения доступности служб протокола UDP, таких как DNS и SNMP.

Сканер защиты сети используется для проверки уязвимости сетевых служб. Это устройство имеет базу данных, в которую заносятся известные уязвимые места и проверяет не являются ли уязвимыми сетевые службы. Ниже объяснены некоторые механизмы, используемые этим устройством для проверки уязвимости сетевых служб.

- Сканер считывает версию операционной системы. Это называется *"снятием отпечатков пальцев" (fingerprinting).*
- Он считывает версию программного обеспечения, используемого в системе.
- Сканер имитирует реальную атаку на сеть. Например, если сервер некорректно обрабатывает запрос длинного URL, то сканер может послать длинный URL и проверить. Возвращает ли сервер соответствующий код.

Ниже приведены некоторые средства защиты, которые можно использовать для обеспечения безопасности сети.

- Nmap представляет собой утилиту открытого источника для исследования сети и аудита безопасности. Эту утилиту можно выполнить на большинстве типов компьютеров; доступны ее консольная и графическая версии.

- Препроцессор GTK+для Nmap доступен для пользователей, которые предпочитают графический интерфейс пользователя интерфейсу командной строки (рис. 52.4). Более подробная информация приведена на Web-сайте www.insecure.org.
- Nessus представляет собой бесплатную утилиту для аудита безопасности, которая способна находить уязвимые места в сети. Более подробная информация приведена на Web-сайте www.nessus.org. пример отчета, выдаваемого утилитой Nessus приведен на рис. 52.5.
- SomarSoft включает в себя набор бесплатных утилит Microsoft Windows, предназначенных для того, чтобы предоставить сетевому администратору информацию, необходимую для защиты Windows-системы. Первой утилитой является DumpSec, которая представляет собой программу аудита безопасности в сети для операционных систем Windows NT и Windows 2000. Вторая утилита — DumpEvt, являетс программой для Windows NT, которая dump the Event Log в формат, пригодный для импорта в базу данных. Третьей является утилита, представляющая собой программу для Windows NT and Windows 95, которая dumps системный реестр (Registry), что облегчает нахождение ключей и значений, содержащих некоторую строку. Более подробная информация приведена на Web-сайте www.somarsoft.
- John the Ripper представляет собой средство взлома паролей открытого источника, которое способно обнаруживать ненадежные пароли. Более подробная информация приведена на Web-сайте www.openwall.com/john/.

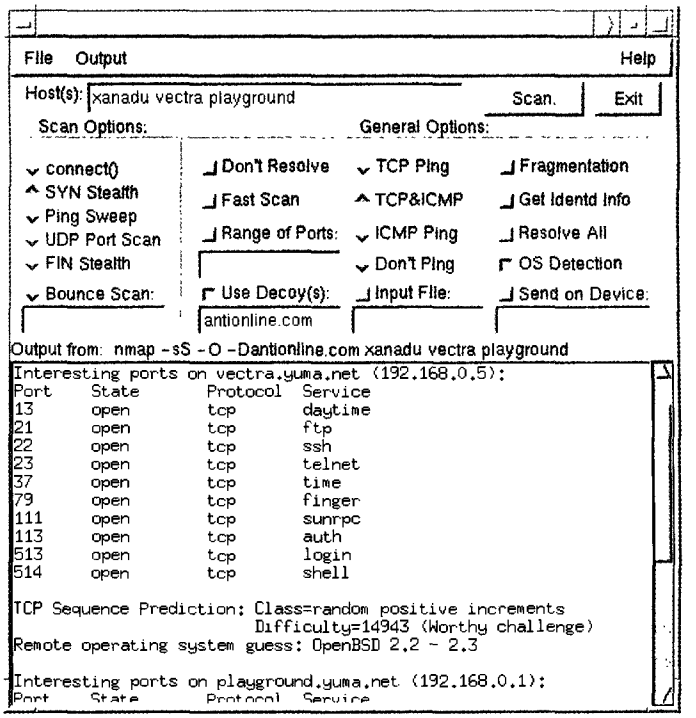


Рис 52.4. Препроцессор Nmap

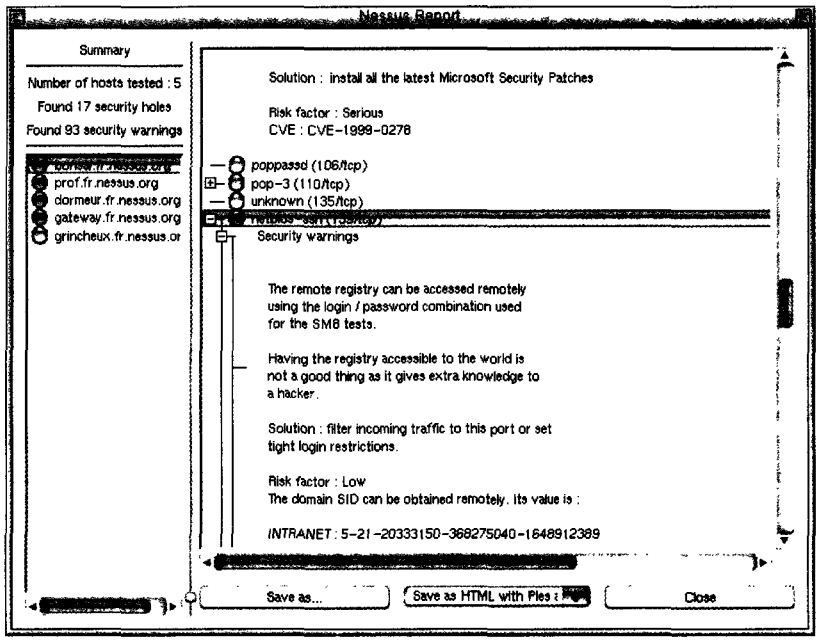


Рис 52.5. Пример отчета Nessus

Резюме

В настоящее время глобальная сеть Internet перестала быть просто средством передачи сообщений электронной почты и файлов. Она изменила нашу повседневную жизнь и стиль работы компаний. Обеспечение сетевой безопасности стало играть ключевую роль в достижении своих целей как частными лицами, так и коммерческими компаниями. Частным лицам требуется чтобы при онлайновых покупках или регистрации для онлайнового обучения сохранялась конфиденциальность их личной информации. Правительства требуют от компаний обеспечения сохранности данных, которые хранятся в их сетях.

Типичными угрозами для сетей являются: попытки несанкционированного доступа, попытки обойти ненадежную аутентификацию, взлом паролей, использование анализаторов пакетов, атаки уровня приложений, вирусы, черви, "троянские кони", подделка IP-адресов и DoS-атаки. Политика безопасности в сети представляет собой документально зафиксированную стратегию, которая определяет уровень безопасности в сети и описывает соответствующие требования к пользователям. Политика безопасности определяет каким образом пользователи, являющиеся сотрудникам компании могут использовать сеть, какие действия должны предприниматься в случае инцидентов, связанных с угрозами сетевой безопасности и каким образом компания осуществляет связь с сетями своих партнеров.

Концентрическое решение проблемы сетевой безопасности основано на принципе создания нескольких периметров защиты сети, образующих защитные зоны. Каждая зона обеспечивает дополнительные механизмы защиты для того, чтобы в слу-

чае прорыва какого-либо периметра защиты следующая зона не допустила успешного завершения атаки.

Методы устранения угроз и защиты сети зависят от типа возникшей угрозы. Для устранения угроз, связанных со взломом паролей используется метод периодической замены паролей. Для устранения угрозы подделки IP-адреосв используются методы входной и выходной фильтрации, описанные в RFC 2827. Для повышения уровня сетевой безопасности системные администраторы могут использовать сканеры портов, сканеры уязвимых мест и средства проверки надежности паролей. Сканеры портов позволяют определить какие сетевые устройства и службы являются доступными извне. Сканеры уязвимых мест находят уязвимые места устройств сети, таких как маршрутизаторы, коммутаторы, серверы и настольные персональные компьютеры. Средства проверки надежности паролей помогают повысить надежность паролей путем выявления паролей, которые не отвечают требованиям надежности.

Контрольные вопросы

1. Чем обусловлена важность обеспечения безопасности в сети?
2. Как повлияли на проблемы безопасности в сетях рост Internet и новые технологии?
3. Как влияет на работу сети компании проводимая в ней политика безопасности?
4. Приведите пример последовательного решения проблемы безопасности?
5. Каковы основные типы атак на сеть?
6. Какой тип атак на сеть приводит к лавинообразному заполнению сети нежелательными пакетами?
7. Какой тип атак включает в себя рассылку приложений к сообщениям электронной почты? Каким образом отражается такая атака?
8. Каким образом отражаются атаки, связанные с подделкой IP-адресов?
9. Каким образом коммутируемая инфраструктура позволяет отражать атаки, связанные с использованием анализаторов пакетов?
10. Какое средство обеспечения безопасности обнаруживает доступные в сети устройства и службы?
11. Какое средство обеспечения безопасности обнаруживает уязвимые места сетевых устройств?
12. Какое средство обеспечения безопасности обнаруживает ненадежные пароли?

Дополнительные источники

Web-сайты

- CERT, www.cert.org
- Cisco SAFE, www.cisco.com/go/safe
- Fact Sheet on EU Privacy Directive, www.dss.state.ct.us/digital/eupriv.html
- Health Privacy Project, www.healthprivacy.org/

- RFC 1918, Address Allocation for Private Networks, www.ietf.org/rfc/rfc1918.txt
- RFC 2196, Site Security Handbook, www.ietf.org/rfc/rfc2196.txt
- RFC 2827, Network Address Ingress Filtering, www.ietf.org/rfc/rfc2827.txt

Книги

- Carter, Earl. Cisco Secure Intrusion Detection, Cisco Press: Indianapolis, 2001.
- Дэвид Чепмен, Энди Фокс. *Брандмауэры Cisco Secure PIX.* ИД "Вильямс", 2003.
- Mason, Andrew. Cisco Secure Virtual Private Networks, Indianapolis: Cisco Press, 2001.
- Wenstrom, Michael. Managing Cisco Network Security, Indianapolis: Cisco Press, 2001.

Группа новостей

- Bugtraq mailing list, www.securityfocus.com
- Cisco Security Consulting Security Bytes, www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns267/networking_solutions_newsletters_list.html
- NTBugtraq mailing list, www.ntbugtraq.com

Глоссарий

Аутентификация (authentication). Процесс проверки идентичности обращающегося к сети устройства.

Стандарт шифрования данных (Data Encryption Standard — DES). Стандарт правительства США (FP046), определяющий алгоритм шифрования данных (Data Encryption Algorithm) и политику его использования для защиты неклассифицированных чувствительных данных.

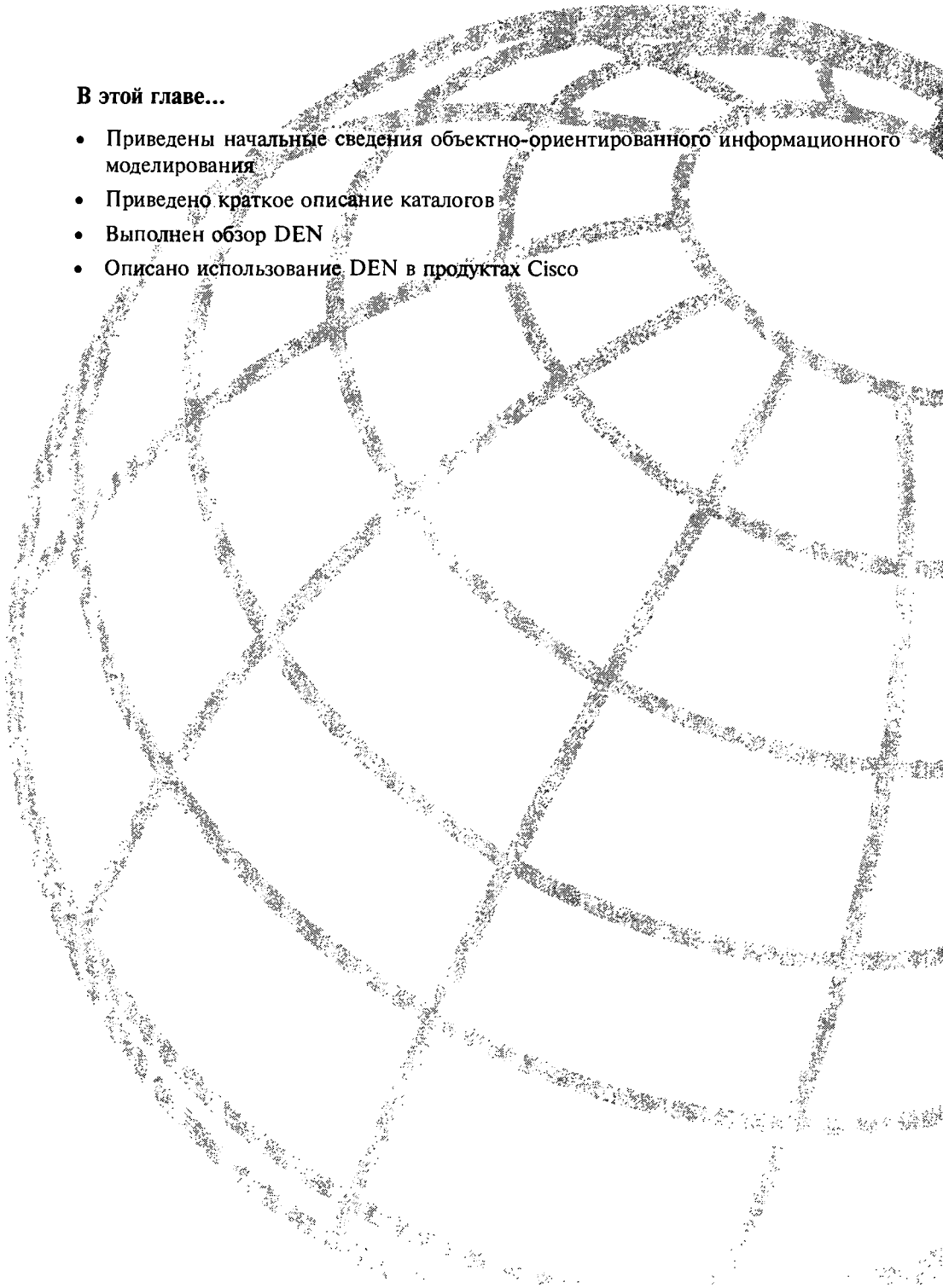
Безопасность протокола Internet (Internet Protocol Security — IPSec). Общее название архитектуры и набора протоколов служб обеспечения безопасности для потоков данных протокола IP. См. www.ietf.org/rfc/rfc2401.txt.

Обнаружение вторжения (intrusion detection). Служба обеспечения безопасности, которая осуществляет мониторинг событий в системе и анализирует их с целью нахождения и обеспечения предупреждений реального времени и near-real-time о попытках несанкционированного доступа к системным ресурсам.

Одноразовый пароль (one-time password — OTP). Простой метод аутентификации, в котором пароль используется лишь один раз в качестве аутентификационной информации для проверки идентичности пользователя. Этот метод позволяет предотвратить угрозу атаки воспроизведения пароля, которая основана на воспроизведении перехваченного пароля.

ping sweep (ping sweep). Тип атаки на сеть, при котором посылаются эхо-запросы (ping-запросы) протокола ICMP (RFC 792) диапазону IP-адресов с целью нахождения станций, в которых есть уязвимые места.

Уязвимость (vulnerability). Пробел в проектировании, реализации, функционировании или управлении системы, который может быть использован для нарушения политики безопасности в сети.



В этой главе...

- Приведены начальные сведения объектно-ориентированного информационного моделирования
- Приведено краткое описание каталогов
- Выполнен обзор DEN
- Описано использование DEN в продуктах Cisco

Глава 53

Сетевые каталоги

Сетевые каталоги представляют собой не продукт и даже не технологию. Скорее это *философия*, описанная спецификацией Directory-Enabled Networks (DEN) и позволяющая связать службы, доступные в сети и клиентов, использующих эту сеть. Спецификация DEN позволяет приложениям расширить возможности сети и одновременно повысить качество обслуживания этих приложений сетью.

Фактически DEN состоит из следующих двух частей.

1. Спецификация объективно-ориентированной информационной модели, описывающей сетевые элементы и службы как часть управляемой среды, независимо от типа хранилища.
2. Преобразование этой информации в форму, удобную для реализации в каталоге, который использует в качестве протокола доступа LDAP или X.500.

Более подробные сведения о сетевых каталогах содержатся в книге Джона Страсснера (John Strassner) *Directory Enabled Networks.*

Объективно-ориентированное моделирование информации

Информационная модель принципиально отличается от модели данных или схемы (рис. 53.1).

- **Модель данных** представляет собой представление характеристик совокупности связанных объектов в терминах, соответствующих данному хранилищу и технологии доступа.
- **Схема** представляет собой совокупность моделей данных, описывающая множество связанных управляемых объектов.
- **Информационная модель** представляет собой *технологически независимую* спецификацию, описывающая характеристики совокупности объектов и их связь с другими объектами в управляемой среде без указания метода хранения, протоколов доступа или конкретных типов хранилищ.

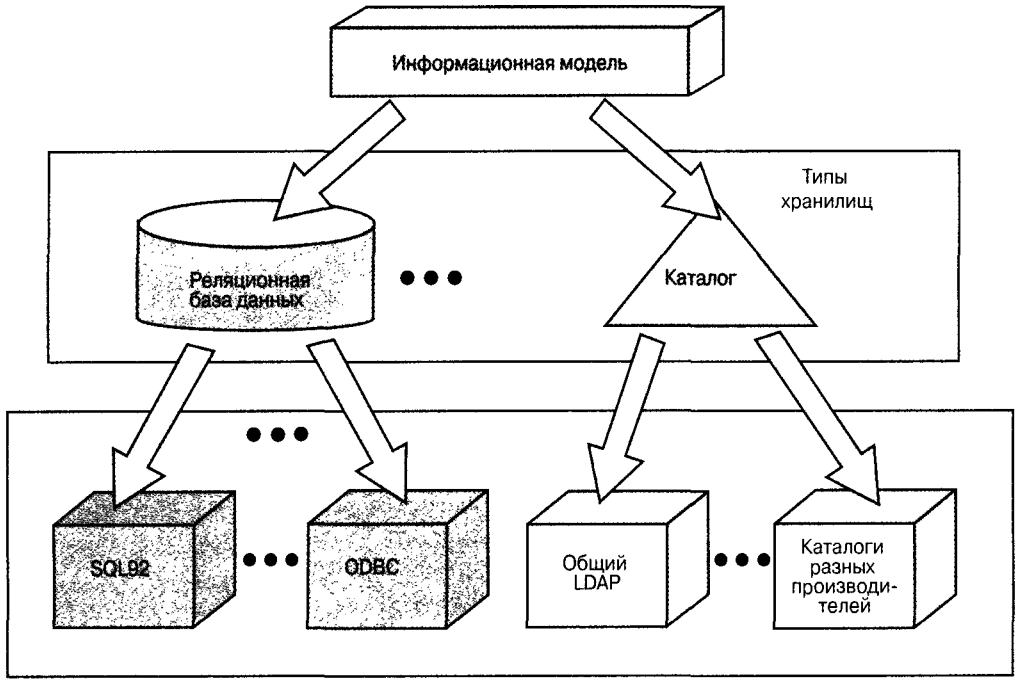


Рис. 53.1. Информационная модель, модели данных и схема

Основное назначение информационной модели — описание единого, универсального представления управляемых данных и объектов, не зависящее от технологий хранения и протоколов доступа. Информационная модель применяется для описания всех управляемых объектов среды и связей между ними.

Поскольку природа объектов и данных, описывающих эти объекты различны, естественно ожидать, что для представления этих объектов и связей между ними потребуются различные типы данных при хранении. Например, может быть разработана политика для изменения типа очередности на конкретном интерфейсе маршрутизатора доступа. Она может оказаться функцией числа отброшенных октетов и числа пользователей конкретных типов служб. Сохранение результатов счетчика протокола SNMP, регистрирующего все, связанное с числом отброшенных октетов, для каталога нецелесообразно, поскольку показания счетчика изменяются слишком быстро для того, чтобы каталог успевал их регистрировать. Однако определения пользователя, как и сама политика вполне целесообразно сохранять в каталоге, поскольку они могут воспользоваться механизмами репликации (дублирования), которые имеются в каталоге. Как будет показано далее в настоящей главе, каталоги весьма удобны в качестве механизмов репликации, а публикация данных в каталоге позволяет различным приложениям совместно использовать данные и обмениваться ими. Поэтому преимущество информационной модели состоит в возможности представления того, как эти различные типы данных и объектов связаны друг с другом единым согласованным образом не будучи обусловленными возможностями какого-либо конкретного хранилища. Иными словами, информационная модель задает *логическое хранилище*, которое описывает управляемые объекты и данные. Логическое хранилище преобразуется в некоторое множество *физических хранилищ* для данных. Конкретное множество храни-

лищ для данных, которое будет использоваться, зависит от нужд приложений, использующих эти хранилища. Это позволяет разработчику выбрать соответствующие хранилища для данных и протоколы, которые будут использоваться для данного приложения.

У разных приложений различные потребности, в силу чего им требуются различные способы хранения данных. Это не вызывает проблем, поскольку можно выполнить набор преобразований из одной информационной модели в несколько моделей, соответствующих используемым типам хранения данных. Вообще говоря, эти преобразования будут различными, поскольку каждый тип хранилища использует конкретную технологию хранения, которой соответствуют один или несколько конкретных протоколов доступа. Это приводит к тому, что одна информация будет отличаться от другой. Например, схема каталога принципиально отличается от схемы реляционной базы данных. Однако все полученные таким образом информационные элементы могут быть связаны друг с другом поскольку одни получены из одной информационной модели.

Модели данных в различных хранилищах

Модель данных описывает основные характеристики объекта или совокупности объектов способом, *характерным для определенного типа хранилища*. Например, объект "маршрутизатор" принципиально отличается от объекта "пользователь". Более того, представление объекта в каталоге отличается от его представления в реляционной базе данных, даже если это одна и та же информация.

Объект в каталоге представляет собой набор элементов с атрибутами, определенными в соответствии с синтаксическими правилами (такими, как типы данных и способы поиска информации), поддерживаемыми LDAP и в X.500. Кроме того, это улучшает локализацию каталога. *Локализацией* (containment) называют отношения подчинения между объектами в системе. В нашем примере объект "пользователь" обычно локализован, или принадлежит, объекту более высокого уровня, такому как группа или организационная единица (то, что в X.500 называется division — подразделение).

Структура объекта "пользователь" в реляционной базе данных отличается от структуры такого же объекта в каталоге. Например, данные, описывающие пользователя, будут находиться в одной или нескольких таблицах, а не в виде отдельных элементов, как в каталоге. Более того, они и структурированы будут несколько иначе, чтобы поддерживать различные информационные структуры и протоколы доступа, которые могут быть использованы в базе данных, но не в каталоге. Однако одним из главных различий между реляционной базой данных и каталогом является взаимосвязь с другими объектами, а не их локализация.

В объектно-ориентированной информационной модели используются объектно-ориентированные методы представления информации в виде некоторой совокупности объектов, существующих в управляемой среде. Главным отличием информационной модели является то, что кроме описания характеристик элементов в ней также описывается их поведение и взаимодействие. Впрочем, два последних свойства присущи не всем хранилищам. Таким образом, информационная модель описывает взаимосвязь между различными типами информации, независимо от типа их хранения. Выбор типа хранилища и вспомогательных средств для реализации тех аспектов информационной модели, которые не обеспечивает само хранилище, зависит от разработчика.

Поясним это на примере. Предположим, нужно принять решение об изменении условий, так как в сети появился некий дополнительный поток данных. Данное решение зависит от следующих факторов:

- количество отброшенных октетов на данном интерфейсе.
- соглашение об уровне обслуживания для данного пользователя или приложения.
- историческая и прочая информация.

Это три принципиально различных типа информации. Отдельное хранилище данных, каким бы оно ни было, очевидно, не является оптимальным для ее хранения из-за свойственных ему различий в объеме, частоте обновления, типах запросов и структурах для хранения и извлечения этих данных. Информационная модель описывает отношения между такими структурами данных, а также с другими объектами управляемой среды. Это позволяет разработчику проектировать оптимизированные хранилища для каждого типа информации, а затем комбинировать данные так, как это ему нужно.

Другим примером является использование различных моделей данных для моделирования интерфейса маршрутизатора, пользователей, различных служб и данных для приложений, предоставляемых разными пользователями. Однако модель данных не позволяет описать взаимодействие между этими объектами. Для этого применяется информационная модель. Отсюда следует, что для представления различных данных, описанных в информационной модели, применяются разные модели данных.

Таким образом, хотя каталоги — очень важный тип хранилищ информации о сетевых элементах и службах, они не являются единственно возможным типом хранилищ данных. Однако, поскольку в каталогах обычно содержатся данные о пользователях, приложениях и других ресурсах сети, они часто в той или иной степени используются всеми приложениями. Вот почему эта глава посвящена отображению DEN-информации в форме, позволяющей сохранять DEN-данные в каталоге и извлекать их оттуда.

Реализация информационной модели

В настоящее время развиваются две основные стандартные информационные модели: общая информационная модель (Common Information Model — CIM) и модель сетевых каталогов (Directory-Enabled Networks — DEN), которая является расширенной моделью CIM. Обе они в настоящее время находятся в ведении DMTF.

Модель CIM

Общая информационная модель (Common Information Model — CIM) представляет собой объектно-ориентированную информационную модель, которая описывает управление системой и ее компонентами. Она определяется стандартом рабочей группы по управлению развитием настольных вычислительных систем (Distributed Management Task Force — DMTF). Продолжение развития CIM является частью отраслевой инициативы, цель которой — единое управление средой, независимо от протоколов и форматов данных, поддерживаемых устройствами и приложениями. Многие разработчики сетевой инфраструктуры и управляющего ПО приняли CIM в качестве информационной модели для средств управления предприятием.

CIM является многоуровневой информационной моделью. Она состоит из нескольких подчиненных субмоделей, детализирующих сведения, представленные на внешних, более общих уровнях. В частности, в модели ядра (рис. 53.2) определен набор общих абстракций и функций, который затем уточняется посредством определения подчиненных

субмоделей, где описывается использование информации в этой модели ядра. Одним из таких уровней является сетевая модель, построенная на основе DEN.

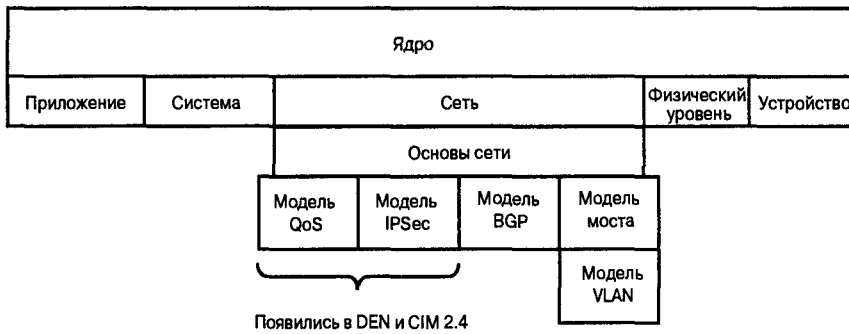


Рис. 53.2. Многоуровневая информационная модель CIM

CIM 2.2 состоит из модели ядра, где определены концепции информационной модели, применяемой во всех сферах управления. Она представляет собой набор классов, атрибутов, методов и взаимосвязей, описывающих общие концепции управления компьютерными системами и системными компонентами. Модель ядра является основой для наследования классов и иерархии взаимосвязей, а также для всех общих и расширенных моделей.

Общие модели являются сборниками классов, атрибутов, методов и взаимосвязей, дополняющих отдельные концепции в модели ядра. Например, в модели ядра определено понятие службы. Сетевая модель уточняет это понятие, описывая различные типы служб, характерных для сети, таких как перенаправление и маршрутизация потоков данных.

Проще всего представить себе общую модель как набор абстракций, часто встречающихся в определенной области управления. Существуют следующие общие модели.

- **Система.** Описывает основные компоненты системы: компьютерная система, операционная система, файл и др., а также отношения между ними.
- **Устройство.** Описывает аппаратное представление физических устройств и способы моделирования связей между устройствами, такими как хранилища данных, мультимедиа, датчики, принтеры и источники питания.
- **Приложение.** Описывает управление установкой программного обеспечения в компьютерной системе.
- **Сеть.** Описывает логические элементы иерархии классов, моделирующие сетевые элементы и службы.
- **Физическая модель.** Описывает физическую организацию, структуру, состав устройств и их соединение.
- **Пользователь.** Моделирует пользователей, группы и организации, показывает, как эти объекты взаимодействуют с другими компонентами управляемой системы.
- **Политика.** Основана на исходной модели политики, предложенной DEN, и обеспечивает общую структуру для представления и определения правил, условий и действий политики. Она также уточняет исходную модель политики с учетом особых требований, предъявляемых правилами, условиями и действиями политики QoS.

Сочетание модели ядра с одной или несколькими общими моделями служит основой для CIM- или DEN-совместимой схемы, которая может быть применена в конкретном случае.

DEN — расширение CIM

В DEN воплощены следующие две идеи.

- Расширение информационной модели, определенной в CIM и описывающей физические и логические характеристики сетевых элементов и служб, а также политик, определяющих правила предоставления и управления сетевыми элементами и службами.
- Отображение информации в формате, который может быть сохранен в каталоге с протоколом доступа (L)DAP.

Схемы сетевой интеграции, определенные в спецификациях DEN и CIM, дополняют друг друга. CIM главным образом касается управления отдельными компонентами в контексте предприятия. В DEN более подробно описаны сетевые компоненты системы с особым акцентом на среду, провайдера услуг или то и другое одновременно. Сюда входит описание не только сетевых элементов и служб, но и их предоставления и управления при помощи объектов политик.

Схема DEN, основанная на информационной модели DEN, объединяет в себе концепции X.500 и CIM для отображения данных в информационной модели DEN в форме, подходящей для реализации в каталоге.

Применение CIM определяется общими концепциями управляемых компонентов среды. DEN дополняет CIM информацией, касающейся непосредственно сети, более специализированной, чем та, что определена в CIM. Структура DEN представляет схему каталога, которая определяет его компоненты (а также другую информацию) и может быть добавлена к существующей схеме, описывающей сетевые элементы и службы. Она также определяет элементы, представляющие правила политики и другую информацию, касающуюся политик.

В информационной модели и схеме DEN также содержится информация рабочей группы IETF Policy Framework (и, вероятно, в будущем будет содержаться информация других рабочих групп), которая до сих пор не утверждена DMTF.

Основы теории каталогов

Современная управляемая вычислительная среда представляет собой не только компьютеры, но и соединяющие их сетевые устройства. Эффективное управление сетью требует множества данных, поступающих из самых разных источников — о различных потребностях пользователей сети и ее текущем состоянии. Более того, управление сетью должно быть распределенным, то есть осуществляться с нескольких точек. Часть этой информации может храниться в каталогах. В DEN предусмотрена методика моделирования сетевых элементов и служб таким образом, чтобы информация для их предоставления и управления могла быть помещена в хранилище любого типа. Как правило, это каталоги, но возможно использование и других типов хранилищ.

Служба каталогов представляет собой физически распределенное, но логически централизованное хранилище нечасто изменяемых данных, используемых для

управления всей средой. Каталоги обычно используются для хранения информации о пользователях, приложениях и сетевых ресурсах, таких как файловые серверы и принтеры. DEN определяет схему занесения информации в каталог. Фактически эта схема дополняет каталог, наделяя его возможностью хранения важной информации для моделирования сетевых элементов и служб, а также управляющих ими политик. Кроме того, DEN определяет схему, не зависящую от специфических реализаций каталогов.

Каталоги и службы каталогов

В этом разделе кратко описываются каталоги и службы каталогов.

Что такое каталог?

Каталог предназначен для хранения информации о принадлежности объектов группам, но не является универсальным хранилищем данных. Это скорее особый вид хранилища информации, основное назначение которого заключается в рациональном хранении и извлечении информации об объектах, имеющих отношение к определенному приложению или приложениям.

Информация в каталогах организована так, как показано на рис. 53.3. Группы объектов образуют иерархическую структуру, которая называется *информационным деревом каталога* (Directory Information Tree — DIT). DIT состоит из *объектов каталога*. Каждый такой объект соответствует элементу дерева каталога и может иметь один или несколько атрибутов. Каждый атрибут имеет по меньшей мере одно отличительное значение и, кроме того, может иметь неотличительные значения. Такая структура позволяет извлекать информацию либо по точному соответствию совокупности критериев, либо по более общей совокупности критериев, характеризующей нужную информацию.

Отличительные значения используются для вычисления относительных отличительных имен (Relative Distinguished Names — RDN) и определенных отличительных имен (Fully Qualified Distinguished Names — FQDN). FQDN элемента получается путем добавления RDN этого элемента к FQDN родительского элемента. Таким образом, FQDN на любом уровне представляет собой набор относительных отличительных имен, совокупность которых определяет путь от корня DIT к этому элементу каталога (рис. 53.4).

Модель любого предмета из реального мира может быть представлена в виде одного или нескольких элементов каталога. Каждый элемент каталога является объектом, имеющим ряд характеристик, описывающих информацию, которая содержится в этом объекте. Такие характеристики представлены в виде атрибутов элемента каталога. Например, атрибуты объекта User могут определять имя, фамилию, идентификационный номер сотрудника, его номер телефона и другие данные. Все эти атрибуты есть у любого объекта класса User, но значения по крайней мере некоторых из них различны, чтобы можно было отличать пользователей друг от друга.

Совокупность атрибутов элемента каталога определяется *объектным классом*, к которому принадлежит этот элемент. Объектный класс определяет обязательные атрибуты элемента (к примеру, значения, которые необходимо присвоить) и дополнительные атрибуты (например, определяемые схемой и не требующие явного присвоения значений). Полное множество объектных классов и атрибутов каталога определяется *схемой* каталога.

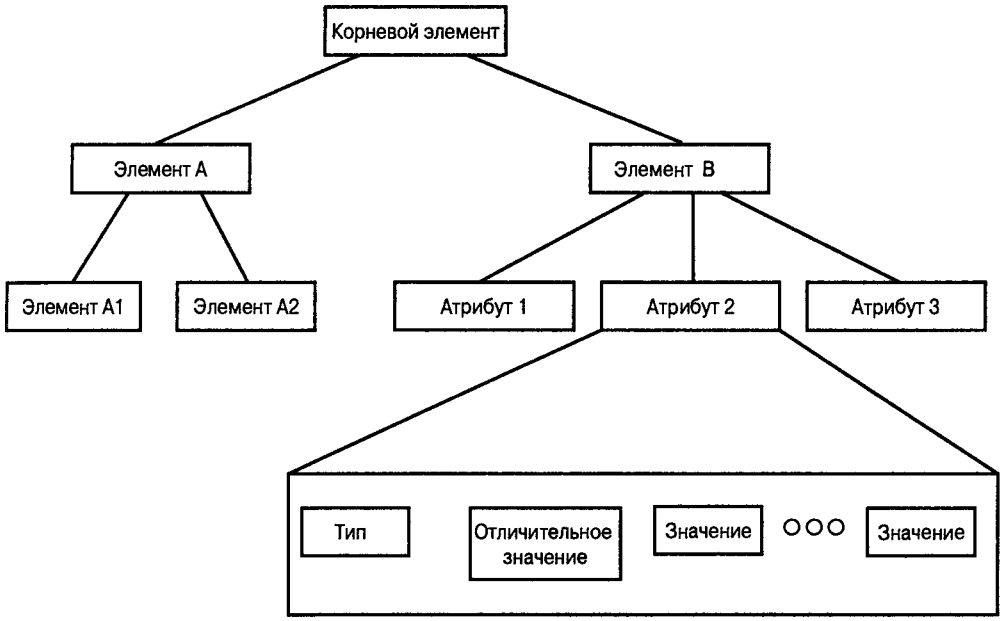


Рис. 53.3. Организация информации в каталоге

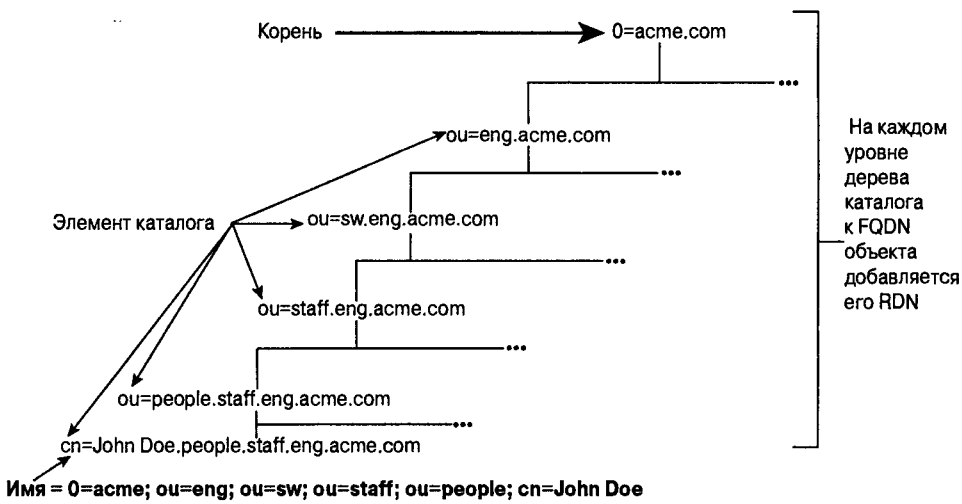


Рис. 53.4. Элементы каталога, их относительные и определенные отличительные имена

Каждый атрибут имеет специфический тип данных, который ограничивает круг присваиваемых атрибуту значений (в частности, буквенно-цифровая строка). Это называется *синтаксисом* атрибута. Кроме того, для каждого элемента определен набор правил, определяющих критерии совпадения каждого атрибута с поисковым запросом (например, игнорирование регистра символов в строке). Возможны и многозначные атрибуты. Наконец, все атрибуты имеют идентификаторы объекта, которые их однозначно определяют — *идентификаторы ASN.1*.

Свойства каталогов

Каталоги имеют пять основных свойств.

- Хранение информации оптимизируется из расчета, что чтение происходит гораздо чаще, чем запись.
- Информация организована в виде *иерархической структуры.*
- Информация в каталоге классифицируется в зависимости от *атрибутов.*
- Каталоги имеют *единое пространство имен* для всех ресурсов, информация о которых в них хранится.
- Каталоги позволяют эффективно распространять информацию в распределенной системе посредством репликации.

Первый пункт означает, что каталоги очень удобны для поиска в больших массивах информации (например, в адресной книге), но не для операций, связанных с частой записью (таких, как бронирование авиабилетов).

Второй и третий пункты в некоторой степени взаимосвязаны. Второй пункт означает, что информационная инфраструктура строится по принципу отношений "родитель-потомок". Основой хорошо структурированного каталога является вложенность, а не наследование. Третий пункт означает, что каталог состоит из набора объектов, каждый из которых имеет ряд атрибутов, содержащих информацию. Таким образом, информация хранится в атрибутах объектов, которые образуют инфраструктуру каталога.

Четвертый пункт очень важен. Он означает, что общая информация может быть размещена и использоваться различными клиентами каталога совместно, поскольку приложения могут использовать общий метод обращения к объекту. Единое пространство имен позволяет полностью интегрировать сетевые элементы и службы с другими типами информации, такими как данные пользователей, приложений и серверов.

Последний пункт является принципиальным для построения информационной инфраструктуры. Сервер каталога имеет возможность контролировать, какая информация, когда и в какие узлы системы распространяется.

Что такое служба каталогов?

Служба каталогов предназначена для хранения и извлечения информации из каталога для одного или нескольких авторизованных пользователей.

Службы каталогов созданы для предоставления определенных типов информации для приложений. Несколько служб каталогов могут совместно использовать один каталог. В качестве примера рассмотрим два телефонных справочника, один из которых построен по принципу "белых страниц", а второй — по принципу "желтых страниц". Оба справочника содержат номера телефонов, но в разной форме. Справочник "белых страниц" позволяет найти номер телефона нужного абонента, а справочник "желтых страниц" — получить номера телефонов нескольких организаций, принадлежащих к одной категории.

Каталог обеспечивает обе такие возможности. В рассмотренном примере каталог должен содержать модель данных, описывающую разные типы пользователей и служб. В действительности это должны быть две разные службы каталогов: одна — для доступа к данным по принципу "белых страниц", а вторая — по принципу "желтых страниц". Однако они могут использовать один и тот же каталог: модель данных для службы "желтых страниц" является просто расширенным вариантом модели "белых страниц", удовлетворяющим более сложным требованиям.

На этом примере видно, что службы каталогов обычно ограничены способом действия. Например, при помощи службы "белых страниц" нельзя (по крайней мере, непросто) узнать имя абонента по его номеру телефона.

Традиционное применение каталогов

Обычная служба каталогов предоставляет средства размещения и идентификации пользователей и доступных ресурсов в распределенной системе. Службы каталогов являются также основой для дополнения, изменения, удаления, переименования и управления системными компонентами без прерывания работы служб, предоставляемых другими системными компонентами. Современные службы каталогов применяются в следующих областях.

- Хранение информации о системных компонентах в распределенной среде. Каталог реплицируется на несколько серверов, так что пользователь или служба, нуждающиеся в доступе к каталогу, могут обратиться за информацией к локальному серверу.
- Общие функции поиска, такие как поиск по атрибуту (например, "найти телефонный номер Джеймса Смита") и по классификации (к примеру, "Найти все цветные принтеры на третьем этаже").
- Предоставление важной информации для единой регистрации пользователя при доступе к службам, ресурсам и приложениям.
- Независимое от расположения ресурса администрирование и управление. Следует отметить, что средства администрирования не обязаны располагаться и управляться централизованно.
- Репликация данных для устойчивого доступа. Изменения, вносимые в любую копию каталога, распространяются по всей сети так, что, после того как изменения распространены, на запрос приложения из любой точки сети выдается одна и та же информация.

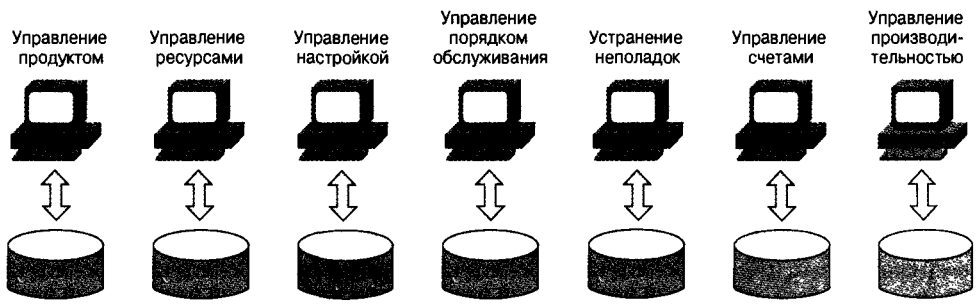
Причины применения DEN в интеллектуальных сетях

У серверов и служб каталогов, предшествующих DEN, есть две основные проблемы, которые препятствуют их использованию в интеллектуальных сетях. Первая проблема заключается в неспособности гетерогенных служб каталогов ко взаимному копированию информации. Дело в том, что протокол LDAP не предназначен для этого, и производители снабдили свои каталоги собственными средствами репликации. Некоторые производители служб каталогов используют форму синхронизации, когда информация считывается с сервера каталога другого производителя и преобразуется в формат, который может быть использован сервером, выполняющим синхронизацию.

Однако стандартов синхронизации не существует (каждый работает по-своему), и у каждого варианта есть свои ограничения. Следует отметить, что над этой проблемой сейчас работает группа по созданию протокола репликации и обновления (LDAP Duplication and Update Protocol — LDUP) при IETF. LDUP определяет информационную модель, использованную при разработке протокола репликации, который сейчас проходит синхронизацию. Эта работа должна завершить-

ся к концу 2000 г. Более подробную информацию о LDUP можно получить по адресу http://www.ietf.org/html.charters/ldup-charter.html.

Вторая проблема заключается в отсутствии стандарта на представление информации. Например, есть много способов представления общей информации о пользователе. Кроме того, существует тенденция разрабатывать приложения по принципу "дымохода". Такие приложения стремятся представить информацию в соответствии с набором соглашений об именовании и структурами, наиболее удобными в данном случае. Это выгодно для отдельного приложения, но создает трудности при совместном использовании и повторном использовании информации разными программами (рис. 53.5).



- Архитектурные проблемы:
  - Избыточность данных
  - Проблемы синхронизации
  - Проблемы авторизации приложений
  - "Закрытость" производителя и приложения
- Проблемы интеграции:
  - Изолированные хранилища данных
  - Сложность администрирования
  - Сложность интеграции и настройки
  - Сложность перехода от устаревших систем к новой, более гибкой операционной архитектуре

Рис. 53.5. Интеграция приложений, построенных по принципу "дымохода", весьма затруднена

Как видно из рис. 53.5, увеличение количества несовместимых баз данных, каждая из которых предназначена для обслуживания определенных потребностей приложений, значительно усложняет интеграцию. В первую очередь, проблема заключается в дальнейшем использовании хранилищ, ориентированных на конкретное приложение. Дело в том, что данные в таких хранилищах частично совпадают, но используются различные правила хранения и именования. Это вызывает проблемы синхронизации, поскольку теперь все копии данных должны обновляться одновременно; однако это не просто, так как они находятся в разных форматах и представлениях. Кроме того, одни и те же данные рассматриваются по-разному. Наконец, последним камнем преткновения является интеграция. Если все приложения станут использовать частные версии одной и той же модели данных, как они будут ими обмениваться? Обратите внимание, что это также ограничивает возможность совместного и повторного использования приложениями одних и тех же данных.

Но еще большей проблемой является то, что до DEN не существовало никакого стандарта на представление сетевых элементов и служб. По этой причине DEN имеет следующие важные преимущества.

- Сетевые элементы и службы представлены стандартным образом, что позволяет различным приложениям использовать одни и те же данные.
- Все элементы управляемой среды представлены в виде объектов. Это дает возможность одинаково обрабатывать различные элементы управляемой среды

и обеспечивает единый способ представления информации о различных элементах системы.

Как сейчас осуществляется, например, единое управление сетью? Иногда для управления различными элементами среды используют HP/Openview и одно или несколько приложений Cisco (предположим, что это Windows NT) для настройки устройств Cisco во всей сети. Возникает проблема: эти два типа приложений должны использовать одни и те же данные, но такое практически невозможно по следующим причинам.

- Разные приложения представляют одну и ту же информацию по-разному, поскольку имеют различную структуру.
- Приложения работают на различных платформах.
- Приложения написаны на разных языках.
- У каждого приложения свой пользовательский интерфейс.

Обратите внимание, что, как правило, интерфейсы API здесь не помогают. И дело не только в описанных ранее причинах, но и в том, что интерфейс API чаще всего отражает внутреннюю функциональность приложения. Поэтому разработчик, занимающийся интеграцией приложения, должен иметь доступ и быть знаком с его функционированием. А это обычно не так, и даже если бы это было так, все равно приходилось бы изменять интерфейс после каждого изменения интегрированного приложения.

DEN решает эту проблему, определяя стандартный способ представления информации. Используя такие технологии, как XML, разработчики могут закодировать данные, представленные в DEN, и передать их другому приложению или другой платформе. Затем это приложение декодирует данные DEN и использует их в своем интерфейсе. Это и в самом деле очень действенная концепция, и вот почему.

- Администратору достаточно изучить только одно приложение.
- При изменении одного из приложений нет необходимости перестраивать интерфейсы API.
- Приложения могут использовать данные совместно, что позволяет отобрать лучшие приложения и организовать их бесперебойную работу.

Таким образом, DEN обеспечивает обмен информацией между различными сетевыми элементами и приложениями, созданными разными производителями. Это позволяет эффективно использовать при построении сети системы и сетевые элементы различных типов.

Распределение интеллектуальных функций между сетевыми приложениями

Благодаря быстрому росту Internet за последние несколько лет возникла потребность в более устойчивых, масштабируемых и защищенных сетевых службах. Частные клиенты хотят иметь мультимедиа-службы с богатыми возможностями, такими как комбинированная передача данных и видео. Корпоративные клиенты требуют от телефонных компаний и провайдеров более широких возможностей за доступную цену. Пользователи хотят надежных, легких и удобных служб.

Произошел значительный сдвиг в сторону сетевых приложений, требующих широкой полосы пропускания и изохронной передачи. Проблемы обмена данными больше

не сводятся к размеру полосы пропускания. Все более важно понять потребности разных типов потоков данных, передаваемых по сети, и сконструировать сеть, удовлетворяющую эти потребности. Более того, если ресурсов становится недостаточно, необходим эффективный способ распределения таких ресурсов согласно принятыми в компании правилам ведения бизнеса.

DEN играет критически важную роль в решении этих проблем. Для описания функций и потребностей различных приложений, использующих сеть, применяется информационная модель. Она преобразуется в набор потоков данных, которые будут передаваться по сети. Для преобразования правил ведения бизнеса в аппаратно-независимую форму может быть использована модель политик DEN. Затем ее можно использовать для преобразования протоколов и алгоритмов, свойственных отдельным устройствам.

Модель политик DEN

Распределение ресурсов в соответствии с принятыми в компании правилами ведения бизнеса является критически важным требованием. Модель политик DEN определяет континуум политик, каждая из которых оптимизирована для представления различной информации. Например, цель деятельности предприятия может определяться администратором, что делает ее аппаратно и алгоритмически независимой. Рассмотрим в качестве примера следующее правило.

ЕСЛИ

Абонент подписан на "золотой" пакет услуг,

ТО

Разрешить использование NetMeeting и обеспечить первоочередное обслуживание

КОНЕЦ

Это полноценное производственное правило, но в нем не сказано, как настраивать устройства. Однако оно определяет, какие службы должны быть выделены.

Для того чтобы сеть поддерживала производственные политики организации, необходимо преобразовать это правило в правило настройки устройств. Преобразование может быть, например, таким:

ЕСЛИ

IP-адрес источника = 172.3.128.0/15

ТО

Присвоить речевым данным метку EF, а обычным данным — метку AF11

КОНЕЦ

Это правило аппаратно-независимо в том смысле, что может применяться к разным устройствам.

Следующий шаг — преобразовать правило таким образом, чтобы оно стало понятно для устройства. Это значит, что нужно привести предыдущее правило к виду, где идентифицируются механизмы устройства, которыми нужно управлять. Вот несколько вариантов такого правила, соответствующих различным действиям.

- Настроить компонент так, чтобы его можно было использовать для условной передачи потоков данных.
- Настроить компонент таким образом, чтобы он мог непосредственно влиять на потоки данных.

- Изменять действия компонента в зависимости от сетевых или системных событий (таких, как повреждение канала связи).

Теперь набор политик можно преобразовать, например, в набор команд CLI для конкретного устройства.

Преимущество такого подхода заключается в том, что он обеспечиввет многократно используемый шаблон. Вместо того чтобы пытаться выполнить преобразования для каждого интерфейса каждого сетевого устройства, можно разработать набор шаблонов, управляемых политиками, и отделить аппаратно-независимые правила от аппаратно-зависимых правил. Именно такой подход использует рабочая группа политик IETF для управления и подготовки QoS (см. http://www.ietf.org/html.charters/policy-charter.html).

Использование каталогов в интеллектуальной сети

Для хранения и извлечения большей части этой информации удобно использовать службу каталогов по следующим четырем причинам.

1. Каталог является естественной средой публикации, способной обеспечить многократное считывание и позволяющей хранить и извлекать практически любую информацию. Таким образом, отпадают ограничения, налагаемые собственно информацией. Каталогу свойственна расширяемость, позволяющая размещать в нем как дополнительную, так и новую информацию.
2. Каталоги фактически являются стандартом для хранения информации о пользователе и других типов информации. Приложения, ориентированные на использование каталогов, требуют интеграции информации о пользовательских, сетевых и других типах ресурсов. Преимущество каталогов заключается в том, что эта информация о ресурсах, элементах и службах сети не только расположена в одном месте, но и представлена в виде одинаковых объектов. Это позволяет различным приложениям совместно использовать информацию из единого хранилища, что намного упрощает структуру всей системы.
3. Каталоги упрощают поиск информации, если неизвестно точное расположение или имя объекта, где хранится нужная информация. Служба каталогов представляет собой нечто большее, чем просто служба имен, такая как DNS. Служба каталогов позволяет осуществлять как поиск, так и извлечение именованной информации.
4. Каталог может также ссылаться на другие системы, где содержится информация. Таким образом, он становится единой точкой, куда приложения обращаются за информацией.

Проблемы современных служб каталогов

Современные технологии служб каталогов не соответствуют стремительно растущим требованиям сегодняшних приложений для открытых и закрытых сетей. Это происходит потому, что большинство применяемых в настоящее время служб каталогов предназначено главным образом для администрирования. Каталоги, используемые таким образом, напоминают обычный склад, где находится только элементарная информация. Необходимо преобразовать каталог из склада в надежное, распределенное,

интеллектуальное хранилище информации для служб и приложений. С этой точки зрения каталог является одной из основ интеллектуальной инфраструктуры.

Сетевые приложения, требующие широкой полосы пропускания и изохронной передачи данных, нуждаются в том, чтобы устройства, расположенные на пути между источником и приемником, были правильно настроены. Эта настройка часто выполняется динамически, по требованию, когда определенный пользователь подключается к сети из одной из нескольких возможных точек. Полноценно управлять приложениями этого нового класса можно только при условии, что управляющая информация о пользователях, сетевых устройствах и службах находится в едином, надежном источнике.

Обзор DEN

В этом разделе описываются проблемные домены, информационная модель и использование интегрированных сетей со службами каталогов. Сеть со службами каталогов представляет собой конструкционная философия, использующая спецификацию DEN для моделирования компонентов в управляемой среде. Этими компонентами являются сетевые устройства, рабочие станции, операционные системы, средства управления и другие компоненты, подлежащие управлению. Все они используют службы каталогов для выполнения таких функций:

- публикация информации о себе;
- обнаружение других ресурсов;
- получение информации о других ресурсах.

DEN можно рассматривать с двух точек зрения:

1. расширение CIM;
2. преобразование информации в формат, пригодный для хранения в каталоге с протоколом доступа (L)DAP.

В следующих разделах представлена обзорная информация о построении функционально-совместимых сетевых систем и преимуществах DEN.

Сети и DEN

Административные потребности и обслуживающие их средства развивались как распределенные системы. Современные службы каталогов предназначены для централизованного управления системой защиты и контактной информацией в сети с довольно незначительным количеством сравнительно больших компьютеров. Управление сетью до сих пор осуществлялось специализированными средствами, у каждого из которых было собственное хранилище информации. Управлением приложениями занимались в последнюю очередь, если занимались вообще.

Добиться единства структуры и представления информации в хранилищах любого типа (не говоря уже о различных хранилищах информации, используемых в сети) было очень сложно. В результате получалась среда с преобладанием вертикального управления. Недостаток интеграции и явная сложность самих средств управления стали препятствием на пути ввода в действие новых приложений.

Администраторы требуют более высокого уровня управления сетями, чем доступен сегодня. Перед ними стоят такие небывало серьезные проблемы, как передача пото-

ковых мультимедийных данных, использование открытых сетей и обеспечение соответствующей безопасности.

Простого управления отдельными устройствами уже недостаточно. Сетевым администраторам приходится определять и управлять политиками, чтобы контролировать сеть и ее ресурсы распределенно, но логически централизованно. В общих словах, политики определяют, какие ресурсы доступны потребителю данного приложения или службы. Отсутствие простого способа управления политиками создает серьезный барьер для внедрения новейших распределенных приложений.

Потребитель представляет собой пользователь, приложение, служба или другой пользователь ресурсов.

Определение политик и управление ими требует общего хранилища четко определенной информации о сети и ее ресурсах — пользователях, приложениях, устройствах, протоколах и среде передачи — и взаимоотношениях между этими элементами. Это, а также традиционная информация, характеризующая сеть (например, таблицы маршрутизации), является информацией о сети. Где же хранить политики и другую информацию, распространяемую по компонентам таким образом, чтобы она была доступной широкому кругу потребителей?

Масштабируемая, защищенная служба каталогов, представляющая логически централизованную форму хранения физически распределенной информации является логическим хранилищем метаинформации, необходимым для создания и управления сетями следующего поколения. В спецификации интеграции службы каталогов и сетевых служб описываются информационная модель и схема, благодаря которым это становится возможным.

Вот только две перспективные возможности DEN:

- средства хранения данных в общем хранилище;
- способ доступа приложений к данным, управляемым другими приложениями.

Это принципиально новый взгляд на приложения управления сетью, а также на приложения, повышающие эффективность работы сети. Достаточно сравнить традиционное управление сетью и управление сетью с использованием DEN. В традиционной системе управлении сетью каждое устройство представлено один раз. Однако у каждого устройства есть подробная информация о конфигурации, которая хранится не в системе управления сетью, но в каждом из приложений в отдельности или в другом хранилище. Роль описателя устройств, возложенная на систему управления сетью, дает возможность пользователю запускать отдельные управляющие приложения, предназначенные для управления устройством в том или ином аспекте. Таким образом, система управления сетью является единой точкой представления устройств, но не хранит информацию о них. В результате интеграция приложений и совместный доступ к информации становятся сложной, если вообще выполнимой задачей.

В DEN применяется принципиально противоположный подход, основанный на каталогах. Главное назначение DEN — обеспечение общего, объединенного хранилища информации, используемого для хранения и совместного использования данных и информации о данных (таких, как метаданные) различными приложениями. Рассмотрим в качестве примера систему управления сетью с использованием HP/Openview под управлением HP/UX. Предположим, что в сети обнаружен новый маршрутизатор, не имеющий информации о внутренней базе данных системы. При отсутствии DEN единственным решением для сетевого администратора было приобретение еще одной

управляющей утилиты для поддержки нового маршрутизатора. Затем, каждый раз, когда требовалось управление маршрутизатором, сетевой администратор должен был переходить на другую консоль. И это только начало всех проблем, так как у новой утилиты, вероятно, свой пользовательский интерфейс, и она может работать на другой платформе.

При наличии DEN все может пройти практически безболезненно. Приведу пример из демонстрации HP и Cisco на шоу 1999 N+I в Атланте. HP и Cisco поддерживают DEN, что позволяет обмениваться некоторой общей управляющей информацией, определяемой стандартами CIM и DEN (следует отметить, что обмен более подробной информацией возможен посредством наследования этих стандартов и их использования как основы для представления специфических продуктов и услуг Cisco). Указанное было достигнуто путем обмена сообщениями между агентом HP/Openview и агентом управления Cisco, запрашивающим описание устройства в DEN. Эта информация находилась в формате XML и отправлялась HP/Openview по протоколу HTTP. Сочетание XML и HTTP обеспечило отсутствие межъязыковых и межплатформенных проблем.

Однако главным преимуществом является то, что *на экран HP/Openview выводятся собственные данные маршрутизатора Cisco.* Отсюда вытекает следующее.

- Администратору достаточно изучить только один пользовательский интерфейс.
- Система расширяема по своей природе. Поскольку ее общим интерфейсом является DEN, она может динамически приспосабливаться к новым продуктам, если только они описаны в DEN.
- Не нужны дополнительные сложные API.
- Новые продукты тоже могут получить совместный доступ к данным.

Служба каталогов и управление сетью

Элементы сети обычно характеризуются динамическим и долговременным состояниями. Для определения динамического состояния достаточно протоколов управления сетью. Однако стандартных способов описания и хранения долговременного состояния нет. Более того, существующий программный инструментарий и приложения направлены на управление не столько сетью в целом, сколько ее отдельными элементами. В спецификациях DEN и CIM определены стандартная схема хранения долговременного состояния и информационная модель для описания отношений между объектами, представляющими пользователей, приложения, элементы и службы сети (рис. 53.6). Для обращения к элементам сети применяются протоколы управления сетью (такие, как SNMP, CMIP и HMMP), а для обращения к элементам и службам сети — расширения сетевой схемы для службы каталогов.

Интеграция сетевой инфраструктуры со службой каталогов позволяет приложениям и пользователям обнаруживать устройства и связи между ними, отправив запрос службе каталогов, а не сопоставляя результаты обращения к отдельным устройствам. Представление элементов сети в каталоге расширяет возможности управления ими и использования их, одновременно снижая нагрузку на сеть. Пользователи и администраторы получают дополнительный опыт, поскольку черпают нужную информацию из единого, надежного источника.

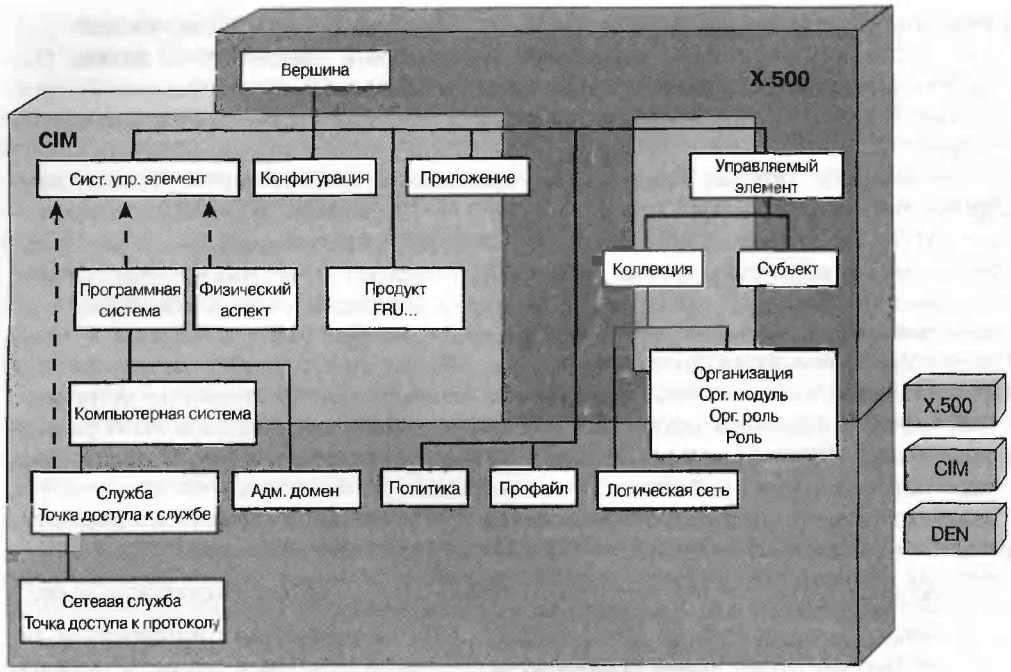


Рис. 53.6. Некоторые из основных классов схемы DEN

Расширенная схема и другие схемы устройств

Схемы, определенные в SNMP (MIB), DMTF CIM и т.п., предназначены главным образом для подробного описания отдельных устройств. Назначение интегрированных, расширенных схем — улучшить использование информации, предоставляемой существующими схемами и управляющими структурами, не заменяя последние. Более того, информационные модели CIM и DEN не зависят от вида хранилища. Это означает, что в устройствах, представленных в схеме DEN и управляемых ею, не обязательно должен быть реализован протокол LDAP.

Сетевые приложения, интегрированные с каталогом и другими сетевыми протоколами

Описанные выше схема и информационная модель расширяют существующие сетевые службы и их протоколы, в частности Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP) и RADIUS.

Каталог является общим хранилищем сетевой информации; взаимоотношения, которые могут возникать внутри каталога, описываются информационной моделью. Модель использования определяет, как существующие сетевые службы и протоколы работают с элементами информационной модели для достижения тех или иных целей, таких как координация выделения IP-адресов между несколькими DHCP-серверами, определение и распространение политики регистрации при удаленном доступе и т.п.

Преимущества DEN

Как правило, DEN используется по следующим трем причинам. Первая — упрощение настройки устройств. В последнее время конфигурация устройств становится все более сложной, что в основном объясняется следующим. Различные типы пользователей и приложений одновременно обращаются к ограниченным сетевым ресурсам. Проблема заключается не в недостатке пропускной способности, а скорее в так называемом смешивании потоков данных (то есть в необходимости мирного сосуществования в одной сети разных приложений, каждому из которых присущи свои требования). Это заставило производителей расширить функциональность сетевых устройств. Таким образом, от сетевых устройств требуется больше возможностей, что приводит к усложнению их конфигурации.

Второй причиной применения DEN является необходимость контроля управления и подготовки сетевых устройств к работе при помощи политик. Предприятия нуждаются в способе преобразования соглашений на уровне обслуживания и производственных правил к общему набору политик, которые бы *контролировали распределение сетевых ресурсов* в зависимости от поведения пользователей, ситуации в подсети, времени суток и других факторов. Но главное — они должны обеспечивать аппаратно-независимую реализацию служб. Разумеется, без стандартной информационной модели это невозможно.

Третьей причиной является возможность сообщать приложениям больше информации о сети, а сети — больше информации о приложениях. В информационной модели DEN это достигается путем представления сетевых элементов, служб и других компонентов управляемой среды в виде объектов. Если все объекты идентичны и обладают равными возможностями, они могут быть одинаково хорошо представлены, что обеспечивает обмен данными между ними.

Полезность служб DEN зависит от потребностей клиента.

Для частных лиц DEN обеспечивает единую регистрацию. При такой регистрации пользователь получает один и тот же набор прав доступа и привилегий вне зависимости от места, времени и способа подключения к сети (разумеется, в пределах, установленных политиками). Кроме того, DEN обеспечивает идентификацию и обслуживание пользователя в соответствии с его ролью в компании, контрактом и т.п. DEN позволяет вводить сложные корпоративные политики. Например, производственные правила могут запрещать передачу кодов программ по открытым каналам Internet. В таком случае, даже если пользователь успешно зарегистрируется при подключении по телефону, политика откажет ему в соединении с кодовым сервером, так как система распознает, что пользователь подключился через открытый канал Internet. В данном случае используются устойчивые уведомления DEN о службах и политиках и возможность связать их с пользователем или с устройством.

Провайдеры услуг заинтересованы в сетях с каталогами, поскольку им необходим способ предоставления дифференцированного обслуживания. Философия "все, что сможете съесть за $19.95" не позволяет покрыть даже расходы на новую сетевую инфраструктуру. Кроме того, сеть с каталогами нужна провайдерам для централизованного управления вновь вводимыми службами. Главным преимуществом здесь является возможность управления элементами и службами на базе политик, а также ограничения области применения новых служб.

Предприятия нуждаются в централизованной защите критически важных данных и в улучшении управления все более сложными конфигурациями устройств. Здесь важна возможность DEN объединять несколько потоков данных в одном приложении, а также организовать управление элементами и услугами сети на базе политик.

Разработчикам приложений предоставляются стандартные средства представления информации о сетевых элементах и службах, что позволяет расширить возможности сети. Возможность DEN описывать приложения, генерируемые ими потоки данных и способы управления этими потоками посредством политик позволяет достичь этой цели.

Использование DEN в продуктах Cisco

На рис. 53.7 показаны два уровня преобразования данных, свойственные DEN. Первый представляет собой преобразование из информационной модели к формату хранилища данного типа. Это преобразование определяет тип хранилища, который, в свою очередь, определяет способ хранения, структуры данных, протокол (протоколы) для их хранения и извлечения, а также другие факторы. Второй уровень преобразования иногда используется для оптимизации системы с учетом требований конкретного приложения или в случае, когда хранилища одного типа, но разных производителей имеют неодинаковые функции.

Рис. 53.7. Преобразования DEN

Cisco использует эту философию для стандартизации использования DEN. По сути, Cisco строит три модели. Первая представляет собой стандартное преобразование информационной модели DEN в нескольких реализациях, таких как CIM 2.2.

Вторая модель представляет собой набор расширений общего назначения для сетей Cisco, разрабатываемых группой инженеров Cisco, занимающихся совместимостью продуктов. Эта модель расширяет базовые концепции CIM и DEN до промежуточного аппаратно-независимого уровня. Например, в ней расширена концепция порта и связана со специфическими элементами и службами Cisco.

Третья модель представляет собой набор расширений для конкретных приложений, которые моделируют устройства и службы Cisco. Этот набор моделей основан на DEN и расширениях Cisco для DEN и позволяет моделировать устройства и службы Cisco на уровне, достаточном для информационной модели.

Следует отметить следующее: несмотря на то, что расширения для Cisco основаны на DEN, сетевые элементы и службы Cisco моделируются на основании открытых стандартов. Это гораздо лучше, чем если бы в основу разработок Cisco был заложен конкурирующий стандарт или, что еще хуже, если бы стандарта вообще не было.

В данном случае гарантируется достаточная функциональная совместимость и появляется возможность обмена с партнерами более подробной информацией. Это касается и расширений для конкретных приложений, основанных на расширениях Cisco.

Перспективы сетей со службами каталогов

Дальнейшее совершенствование сетей путем интеграции со службами каталогов заключается в предоставлении сетевым приложениям информации из каталога. Развитие интеллектуальных сетей подразумевает выполнение следующих условий :

- в основу сети должны закладываться надежные службы каталогов;
- сетевые элементы и службы должны моделироваться по схеме, основанной на открытых стандартах;
- в сети должны использоваться протоколы доступа, управления и манипулирования информацией в каталогах.

Разработка сетей, основанных на каталогах, должна преследовать следующие цели.

- Обеспечить поддержку приложений, которые могут улучшить сетевую инфраструктуру в соответствии с требованиями пользователей.
- Обеспечить надежную, расширяемую основу для построения приложений, ориентированных на сеть.
- Предоставить пользователям индивидуальное сквозное сетевое обслуживание.
- Обеспечить возможность создания и инициализации общесетевых служб.
- Предоставить возможность управления всей сетью.

Основное внимание уделяется управлению сетью как единой системой, а не как набором отдельных компонентов или индивидуальных интерфейсов. Такая возможность обеспечивается благодаря описанию отношений между сетевыми при помощи служб каталогов. Для того чтобы встроить эти службы в системы управления, производители используют открытые промышленные стандарты *де-факто*, такие как DNS и DHCP. Следующим таким стандартом является DEN.

Резюме

Эта глава содержит начальные сведения о сетях DEN. Сеть DEN характеризуется двумя очень важными свойствами. Первое и главное представляет собой объектно-ориентированная информационная модель для описания управляемых объектов в среде. Подобных моделей множество, но сеть DEN уникальна тем, что ее модель описания сетевых элементов, служб и других объектов, образующих управляемую среду, не привязана к хранилищу объектов. Второе важное свойство заключается в том, что DEN определяет отображение данных, описываемых информационной моделью DEN, в форме, которая может храниться и извлекаться из каталога (с протоколом доступа LDAP или X.500).

Кроме того, были кратко описаны основы объектно-ориентированного информационного моделирования и преимущества такого подхода. Этот метод позволяет создавать согласованные модели любых объектов управляемой среды. Каталоги являются одним из важных примеров отображения такой информации. Это вызвано тем, что в

каталогах уже содержится такая важная информация, как сведения о пользователях, принтерах и других сетевых ресурсах. Концептуально DEN расширяет тип данных, которые могут быть смоделированы в каталогах, и показывает, как эта информация связана с различными типами данных в других хранилищах.

DEN представляет собой основу интеллектуальных сетевых служб и управления системами посредством политик. DEN создает модель сети как провайдера интеллектуальных услуг и клиентов как пользователей этих услуг. Данная методология позволяет предоставить приложениям больше информации о сети, а сети — получать больше информации о потребностях различных приложений.

Наконец, были приведены примеры использования DEN в Cisco Systems для построения нового семейства интеллектуальных продуктов и решений.

Контрольные вопросы

1. Что такое DEN?
2. Требует ли DEN использования каталога?
3. Является ли DEN обычным средством моделирования сетевых устройств и служб?
4. Что такое объектно-ориентированная информационная модель?
5. Перечислите некоторые основные преимущества DEN.
6. Как DEN моделирует отношения между объектами?

Источники дополнительной информации

DEN и связанные с ним стандарты

Рабочая группа по управлению развитием настольных вычислительных систем (Desktop Management Task Force — DMTF), , является промышленным консорциумом, который занимается разработкой, сопровождением и развитием стандартов управления настольными вычислительными системами и продуктами для них, в том числе CIM и DEN. Более подробную информацию о ней см. по адресу http://www.dmtf.org.

Рабочие группы IETF

Информацию о рабочей группе по разработке политик (Policy Framework Working Group) при IETF можно получить по адресу http://www.ietf.org/html.charters/policy-charter.html.

Рабочая группа по расширениям LDAP (LDAPEXT) при IETF продолжает работы по созданию службы каталогов Internet. Она создает описания и стандартизирует расширения протокола LDAP 3, расширения для применения протокола LDAP в Internet и API для LDAP. Более подробную информацию можно получить по адресу http://www.ietf.org/html.charters/ldapext-charter.html.

Рабочая группа по протоколу репликации и обновления LDAP (LDAP Duplication and Update Protocol — LDUP) при IETF описывает дополнения (протокол и схемы) к протоколу LDAP, обеспечивающие возможность репликации между каталогами раз-

личных производителей. Более подробную информацию можно получить по адресу http://www.ietf.org/html.charters/ldup-charter.html.

Рабочая группа по политике доступа к RSVP (RSVP Admission Policy — RAP) при IETF занимается разработкой стандартов для масштабирования модели управления политиками, которая обеспечивает дифференцированное качество обслуживания в Internet с использованием явных сигнальных протоколов, таких как RSVP. Служба общей открытой политики (Common Open Policy Service — COPS) определяет протокол для передачи запросов и ответов политик. Более подробную информацию можно получить по адресу http://www.ietf.org/html.charters/rap-charter.html.

Простой протокол управления сетью (Simple Network Management Protocol — SNMP) является стандартом де-факто для управления IP-системами. Разработкой SNMP занимается несколько рабочих групп IETF. Информацию о некоторых из них можно найти по следующим адресам:

- http://www.ietf.org/html.charters/agentx-charter.html;
- http://www.ietf.org/html.charters/snmpv3-charter.html.

Целью первой из этих групп является повышение расширяемости SNMP Agent. Цель рабочей группы SNMP 3 — разработка протокола SNMP следующего поколения.

Информационная база мониторинга удаленных сетей (Remote Network Monitoring Management Information Base) существует в двух версиях и описана в следующих RFC:

- http://info.internet.isi.edu/in-notes/rfc/files/rfc1757.txt ("Remote Network Monitoring Management Information Base");
- http://info.internet.isi.edu/in-notes/rfc/files/rfc2021.txt ("Remote Network Monitoring Management Information Base v2 Using SMI v2");
- http://info.internet.isi.edu/in-notes/rfc/files/rfc2074.txt ("Remote Network Monitoring MIB Protocol Identifiers").

Протокол RSVP описан в нескольких RFC. Наиболее соответствующие теме этой книге перечислены ниже. Кроме того, рекомендуем обратиться к информации о рабочей группе RAP. По адресу http://info.internet.isi.edu/in-notes/rfc/files/ находятся следующие RFC:

- rfc2205.txt, "RSVP Functional Specification";
- rfc2206.txt, "RSVP Management Information Base Using SMIv2";
- rfc2207.txt, "RSVP Extensions for IPSec Data Flows";
- rfc2208.txt, "RSVP Applicability Statement";
- rfc2209.txt, "RSVP Message Processing Rules";
- rfc2210.txt, "The Use of RSVP with IETF Integrated Services".

Рабочая группа по дифференцированным службам при IETF определяет "относительно простые и приближенные методы дифференциации классов обслуживания потоков данных в сети Internet". Точнее, речь идет о ограниченном наборе "строительных блоков", позволяющем определять качество обслуживания в данном узле. Описание этой работы находится по адресу http://www.ietf.org/html.charters/diffserv-charter.html.

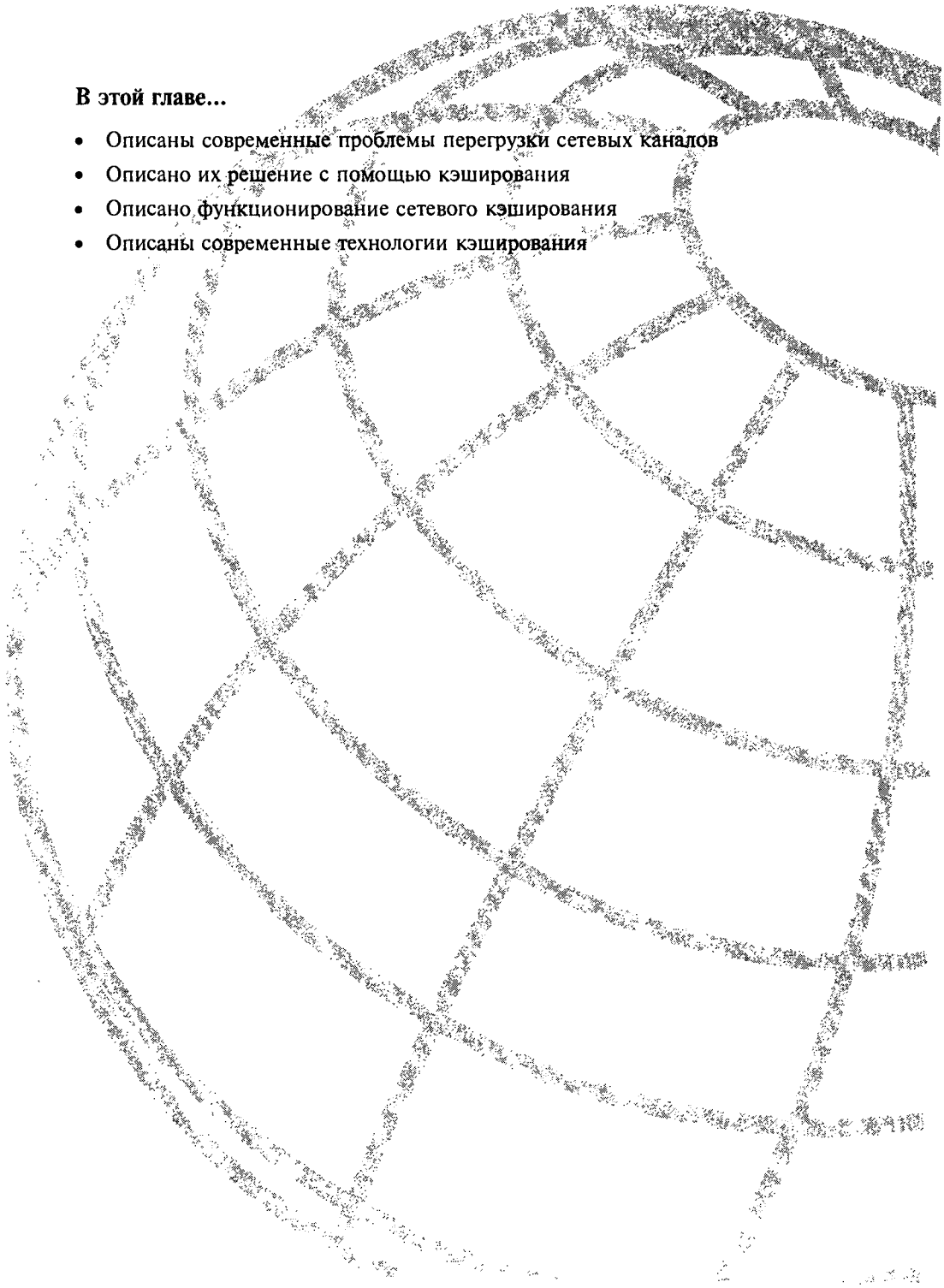
Рабочая группа по интегрированным службам при IETF Recent Experiments демонстрирует возможности протоколов пакетной коммутации по поддержке интегрированных служб — передачи аудио- и видеоданных, данных реального времени и "классических"

данных через единую сетевую инфраструктуру. Более подробную информацию можно получить по адресу http://www.ietf.org/html.charters/intserv-charter.html.

Каталоги

Вероятно, лучшим источником информации о каталогах являются упомянутые выше Web-узлы двух рабочих групп IETF — LDAPEXT и LDUP. Кроме того, прекрасными источниками информации о каталогах являются следующие:

- http://www.critical-angle.com/ldapworld/;
- http://www.kingsmountain.com/ldapRoadmap.shtml;
- Strassner J. *Directory Enabled Networks.* Indianapolis: Macmillan Technical Publishing, 1999.



В этой главе...

- Описаны современные проблемы перегрузки сетевых каналов
- Описано их решение с помощью кэширования
- Описано функционирование сетевого кэширования
- Описаны современные технологии кэширования

Глава 54

Технологии сетевого кэширования

Введение

Хотя объем Web-данных в Internet непостоянен, его значительную часть на любом Web-узле составляют обращения одних и тех же пользователей к одному и тому же содержимому. Это означает, что значительная часть инфраструктуры глобальной сети изо дня в день занята переносом одного и того же содержимого и одинаковых запросов на него. Благодаря ликвидации большинства повторяющихся операций по передаче данных предприятия и клиенты провайдеров экономят значительные средства.

При Web-кэшировании происходит локальное сохранение Web-содержимого. Это позволяет быстрее обслуживать повторные запросы пользователей, не пересылая запросы и получаемое в ответ содержимое по глобальной сети.

Сетевое кэширование

Сетевое кэширование представляет собой технологию хранения часто запрашиваемой информации поблизости от того, кто ее запрашивает. В *Web-кэше* Web-страницы и содержимое хранятся на накопителе, который физически или логически расположен ближе к пользователю и быстрее поставляет информацию, чем Web-ресурс. За счет сокращения потоков данных по глобальным каналам и через перегруженные Web-серверы кэширование позволяет добиться значительной экономии для провайдеров ISP, корпоративных и частных клиентов. Можно выделить два основных достоинства этой технологии.

- **Сокращение затрат за счет меньших требований к полосе пропускания глобальных каналов.** Internet-провайдеры могут разместить кэш-процессоры в стратегических точках своих сетей, за счет чего сократить время отклика и уменьшить требования к полосе пропускания магистрали. Провайдеры ISP могут устанавливать кэш-устройства в стратегических точках доступа к глобальной сети для того, чтобы Web-запросы обслуживались с локального диска, а не с удаленных или перегруженных Web-серверов.
- В корпоративных сетях значительное сокращение используемой полосы пропускания за счет Web-кэширования позволяет обслуживать ту же базу пользователей при помощи более узкополосного (и дешевого) WAN-соединения, увели-

чить количество пользователей или расширить спектр услуг за счет освободившейся пропускной способности существующего канала.

- **Повышение производительности труда пользователей.** Время отклика локального Web-кэша часто оказывается примерно в три раза быстрее, чем время загрузки того же содержимого по глобальной сети. Для пользователей значительно сокращается время отклика при предоставлении того же содержимого, что и по глобальной сети.

Среди других достоинств можно отметить следующие.

- **Надежный контроль доступа и мониторинг.** Кэш-процессор предоставляет сетевым администраторам простой, надежный метод соблюдения политики доступа ко всему Web-узлу путем URL-фильтрации.
- **Контроль действий посетителей.** Сетевые администраторы могут изучить количество обращений к различным URL, узнать, сколько запросов в секунду обслуживается кэшем, какая часть URL обслуживается кэшем, а также получить другую статистическую информацию.

Функционирование Web-кэширования

Web-кэширование функционирует следующим образом.

1. Пользователь обращается к Web-странице.
2. Сеть анализирует запрос и, в зависимости от его параметров, прозрачно перенаправляет его в кэш локальной сети.
3. Если у кэша нет Web-страницы, он генерирует собственный запрос на исходный Web-сервер.
4. Исходный Web-сервер предоставляет содержимое, которое заносится в кэш. Там оно сохраняется и передается клиенту. Таким образом, содержимое остается в кэше.
5. Впоследствии, когда другой пользователь запросит ту же Web-страницу, сеть проанализирует его запрос и, в зависимости от его параметров, прозрачно передаст его локальному сетевому кэшу.

Вместо того чтобы отправлять запрос по Internet и Intranet, сетевой кэш выполняет его локально, таким образом ускоряя доставку содержимого.

Возникает важная задача своевременного обновления данных, и она решается различными способами, в зависимости от структуры системы.

Достоинства локализации типов потоков данных

Кэширование позволяет локализовать типы потоков данных и решить проблему перегрузки сетевых каналов благодаря следующим факторам:

- ускорение доставки содержимого пользователям;
- более оптимальное использование полосы пропускания WAN-сети;
- упрощения наблюдения за потоками данных.

Интегрированный сетевой кэш

Первым шагом при организации интегрированного сетевого кэширования является локализация потоков данных путем маршрутизации содержимого на уровне системы и настройка параметров оптимизации потоков данных в сети. Примером технологии маршрутизации содержимого, поддерживающей локализацию потоков данных, является Cisco IOS ® Web Cache Communication Protocol (WCCP).

Если в основу сети заложена соответствующая технология, то в ее стратегических точках могут быть добавлены кэши.

Для интегрированного сетевого кэширования Cisco разрабатывает аппаратно-программные комплексы.

Системы интегрированного сетевого кэширования всегда обладают следующими тремя свойствами.

- Управление ими подобно управлению другим сетевым оборудованием, так что затраты на эксплуатацию минимальны.
- Поскольку это сетевые аппаратные средства с высокой степенью интеграции, они хорошо встраиваются в физическую сетевую инфраструктуру в качестве сетевых расширений и занимают мало места в стойке.
- Они прозрачно внедряются в сеть, что, с одной стороны, сокращает затраты на внедрение и эксплуатацию, а с другой, повышает доступность содержимого.

Современные системы кэширования

На сегодняшний день наиболее распространенными являются три типа кэшей: прокси-серверы, автономные кэши и кэши в броузере клиента.

Прокси-серверы

Прокси-сервер представляет собой программное обеспечение, работающее на обычном компьютере и под управлением обычной операционной системы. Прокси-сервер устанавливают на компьютере, физически расположенном между клиентским приложением, таким как Web-броузер, и Web-сервером. Прокси-сервер играет роль "привратника", который принимает все пакеты, предназначенные для Web-сервера и проверяет, может ли он выполнить запрос самостоятельно; если такой возможности у него нет, то он формулирует собственный запрос для Web-сервера. Прокси-серверы могут использоваться для фильтрации запросов, например, чтобы предотвратить доступ сотрудников к определенным Web-узлам.

К сожалению, прокси-серверы не оптимизированы для кэширования и их нельзя масштабировать при увеличении нагрузки на сеть. Кроме того, поскольку через прокси-сервер проходят все потоки данных пользователей, возникают две проблемы: для того, чтобы прокси-сервер мог проанализировать каждый пакет, передача всех данных замедляется, а аппаратный или программный сбой прокси-сервера лишает всех пользователей доступа к сети. Для компенсации низкой программной производительности и невозможности масштабирования прокси-серверов требуется дорогое оборудование.

Для использования прокси-сервера также необходима настройка каждого броузера пользователя в отдельности, что является дорогостоящей и немасштабируемой для провайдеров услуг и крупных предприятий управляющей процедурой. Кроме того,

иерархическая структура прокси-серверов создает дополнительную нагрузку на сеть, которая делает невозможными любые планы стратегического объединения несовместимых сетей в единую сеть.

Автономные кэши

Для компенсации недостатков прокси-серверов некоторые производители создали *автономные кэши*. Эти специализированные приложения и устройства для кэширования разработаны для повышения производительности путем применения более совершенного кэширующего программного обеспечения и устранения других свойств прокси-серверов, замедляющих передачу данных. Хотя автономные кэши являются шагом в правильном направлении, они, не будучи интегрированы в сеть, приводят к более высоким эксплуатационным расходам и поэтому малоприемлемы для крупномасштабного развертывания.

Кэширование в браузере клиента

Internet-браузеры позволяют кэшировать Web-страницы (изображения и текст в формате HTML) на локальном жестком диске пользователя. Пользователь сам выбирает размер дискового пространства для кэширования. На рис. 54.1 показано окно настройки кэша в Netscape Navigator.

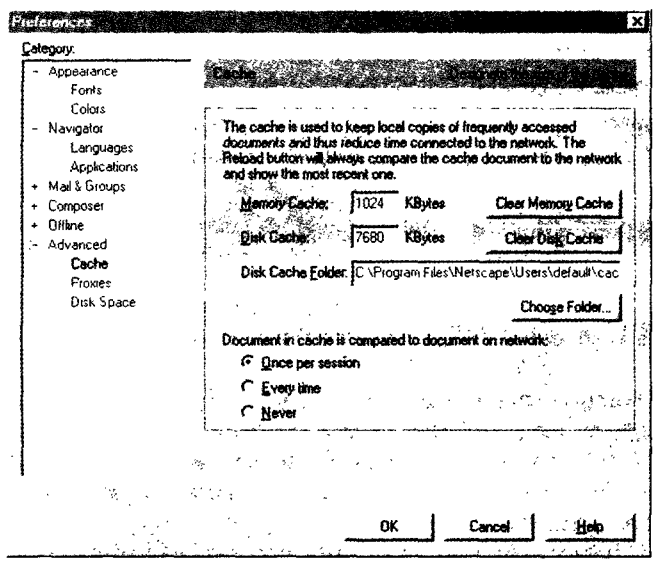


Рис. 54.1. Выбор размера дискового пространства для кэширования Web-страниц в Netscape Navigator

Такая настройка полезна в случаях, когда пользователь обращается к узлу несколько раз. Когда он просматривает Web-узел впервые, его содержимое сохраняется в виде файлов в каталоге на жестком диске компьютера. При следующем обращении пользователя к этому Web-узлу браузер получит содержимое из кэша, не обращаясь к сети. Пользователь заметит, что элементы Web-страницы — особенно графические, такие как кнопки, пиктограммы и изображения, появляются гораздо быстрее, чем когда он обращался к странице в первый раз.

Такой метод хорош для одного пользователя, однако не дает преимуществ другим пользователям той же сети, если они захотят обратиться к тому же Web-узлу. Как видно из рис. 54.2, то, что пользователь A кэшировал часто посещаемую страницу, никак не влияет на время загрузки этой страницы пользователями B и C.

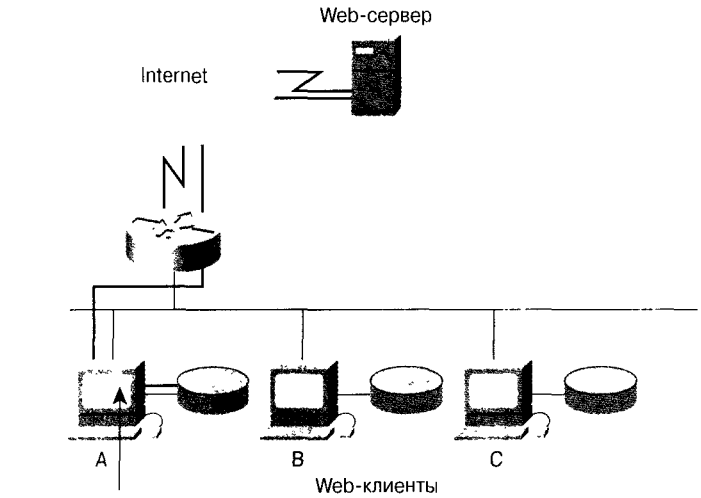


Рис. 54.2. Достоинства кэширования в браузере для одного узла

Сетевое кэширование по протоколу WCCP

В 1997 г. корпорация Cisco разработала протокол маршрутизации кэширования WCCP, который локализирует потоки данных в сети и обеспечивает интеллектуальное распределение нагрузки между несколькими сетевыми кэшами, что позволяет добиться максимальной скорости загрузки содержимого.

Кэш-компонент в этой разработке Cisco представляет собой кэш, интегрированный в сеть — Cisco Cache Engine 500 Series. Он интегрирован в сеть по следующим причинам.

- Обеспечивает те же возможности управления сетью, что и в традиционных сетевых устройствах Cisco (такие, как поддержка Cisco IOS CLI и RADIUS), что сводит к минимуму затраты на управление и эксплуатацию.
- Спроектирован и внедряется скорее как сетевое оборудование для кэширования, чем как автономные серверные платформы, приспособленные для кэширования. Таким образом, устройства высокой плотности Cisco Cache Engines конструктивно лучше интегрируются в инфраструктуру сети в качестве сетевых расширений, прозрачно встраиваемых в существующие сетевые структуры и приспосабливаемые к необычным режимам, что позволяет свести к минимуму затраты на внедрение и эксплуатацию, а также повысить доступность содержимого.

Совместное сетевое кэширование

Кэш-процессор с самого начала разрабатывался как слабосвязанная многоузловая сетевая система, оптимизированная для совместного сетевого кэширования. Кэш-

процессорная система состоит из протокола управления Web-кэшированием (Web Cache Control Protocol — WCCP), который является стандартной функцией программного обеспечения Cisco IOS, и одного или нескольких кэш-процессоров Cisco, сохраняющих данные в локальной сети. Обмен информацией между кэш-процессором и маршрутизатором происходит по протоколу WCCP. Согласно этому протоколу маршрутизатор направляет Web-запросы кэш-процессору (а не на соответствующий сервер). Маршрутизатор также определяет доступность кэш-процессора и перенаправляет запросы на новые кэш-процессоры по мере их ввода в действие.

Кэш-процессор Cisco представляет собой специализированное сетевое устройство для хранения и извлечения содержимого посредством высокооптимизированных алгоритмов кэширования и предоставления данных (рис. 54.3).

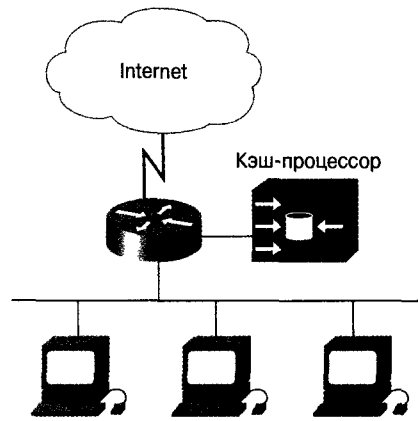


Рис. 54.3. Кэш-процессор Cisco, подключенный к маршрутизатору IOS Cisco

Прозрачное сетевое кэширование

Кэш-процессор выполняет прозрачное кэширование следующим образом (рис. 54.4).

1. Пользователь запрашивает из броузера Web-страницу.
2. WCCP-маршрутизатор анализирует запрос и определяет по номеру TCP-порта, нужно ли его прозрачно перенаправить кэш-процессору.
3. Если у кэш-процессора нет требуемого содержимого, он устанавливает отдельное TCP-соединение с сервером, откуда и получает нужное содержимое. Содержимое поступает на кэш-процессор и сохраняется там.
4. Кэш-процессор пересылает содержимое клиенту. Последующие запросы того же содержимого кэш-механизм выполняет прозрачно, используя данные из локального хранилища.

Поскольку WCCP-маршрутизатор перенаправляет пакеты, предназначенные для Web-серверов, кэш-процессору, последний является прозрачным для клиента. Клиентам не нужно настраивать свои броузеры на определенный прокси-сервер. Это является важным преимуществом для Internet-провайдеров и крупных предприятий, где сложно добиться единой конфигурации броузера. Кроме того, функционирование кэш-процессора прозрачно и для сети, поскольку маршрутизатор

функционирует в обычном режиме, как если бы перенаправления потоков данных не было.

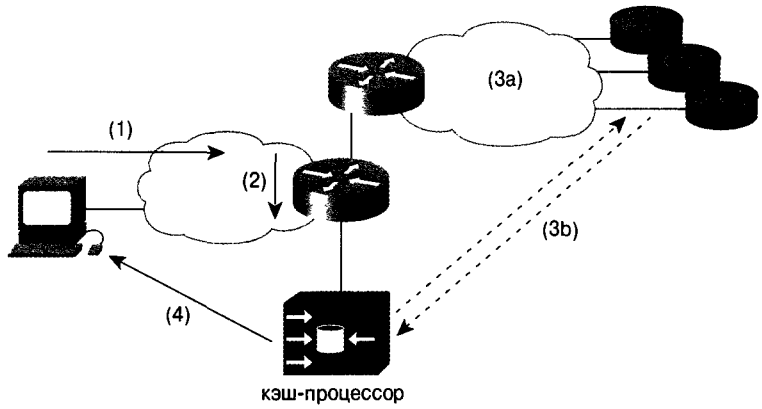


Рис. 54.4. Прозрачное сетевое кэширование

Иерархическое развертывание

Поскольку Cisco Cache Engine работает прозрачно для клиента и для сети, можно без труда установить кэш-процессоры в нескольких местах сети и объединить их в иерархическую структуру. Например, если в главной точке доступа к Internet ISP установит Cache Engine 590 (рис. 54.5), то от этого выиграют все его точки присутствия (Point Of Presence — POP). Запросы клиента поступают на Cisco Cache Engine 590 и удовлетворяются содержимым из его хранилища. Для дальнейшего улучшения обслуживания клиентов ISP-провайдер может установить в каждой точке присутствия Cache Engine 590 или 570. Тогда при обращении клиента к Internet запрос сначала перенаправляется в кэш точки присутствия. Если в кэше точки присутствия отсутствует содержимое, необходимое для выполнения запроса, то кэш направляет обычный Web-запрос конечному серверу. Этот запрос перенаправляется обратно на Cisco Cache Engine 590 в главной точке доступа к Internet. Если он выполняется Cisco Cache Engine 590, то поток данных не попадает на главный канал доступа к Internet, серверы-источники испытывают меньшую нагрузку, а клиент быстрее получает ответы от сети. Такую иерархическую прозрачную архитектуру можно использовать и для улучшения работы корпоративных сетей (рис. 54.6).

Масштабируемая кластеризация

Система кэширования Cisco предназначена для того, чтобы облегчить сетевым администраторам кластеризацию кэш-процессоров и распределение плотных потоков данных. Подход, примененный в этой разработке, обеспечивает линейное масштабирование производительности и объема кэша по мере добавления новых кэш-процессоров. Например, одно устройство Cisco Cache Engine 590 поддерживает канал WAN со скоростью передачи 45 Мбит/с и кэшем объемом 144 Гбайт; система из двух таких устройств поддерживает линию связи WAN со скоростью передачи 90 Мбит/с и кэшем объемом 288 Гбайт. В одной системе может быть до 32 кэш-процессоров.

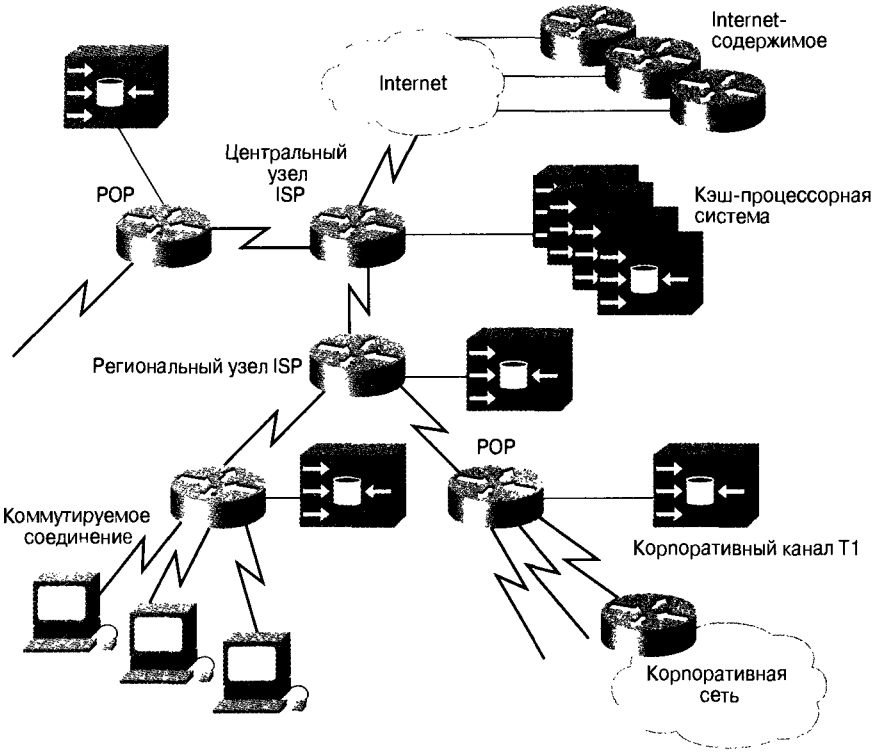


Рис. 54.5. Иерархическая реализация кэш-процессоров (ISP)

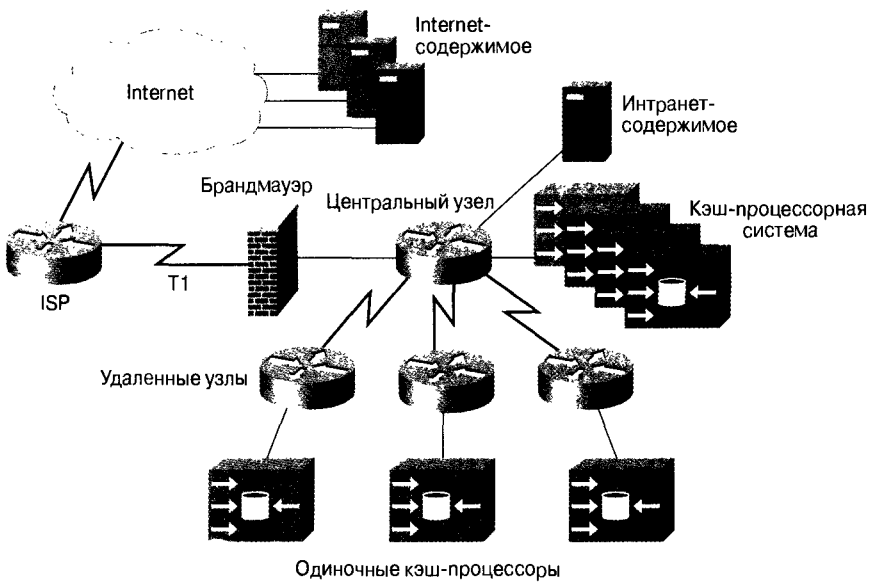


Рис. 54.6. Иерархическая реализация кэш-процессоров (корпоративная сеть)

Такая линейная масштабируемость достигается благодаря тому, что маршрутизаторы с функцией WCCP перенаправляют потоки данных на кэш-процессоры. WCCP-маршрутизаторы осуществляют хеширование по IP-адресу, указанному во входящем запросе, направляя запрос в одну из 256 дискретных ячеек. Эта хэш-функция распределяет входящие запросы статистически равномерно по всем ячейкам. Кроме того, эти ячейки равномерно распределены по всем кэш-процессорам. Благодаря WCCP-маршрутизаторам удается сделать так, чтобы каждый кэш-процессор обрабатывал запросы для определенного IP-адреса Internet. Эмпирически такой алгоритм обеспечивает равномерное распределение нагрузки на кластеры кэш-процессорной системы. Большинство известных Web-узлов имеют несколько IP-адресов, что препятствует неравномерному распределению загрузки.

Если добавить в кластер новый кэш-процессор, WCCP-маршрутизатор обнаруживает присутствие последнего и перераспределяет 256 ячеек, чтобы разместить в них дополнительный кэш-процессор. Например, в простейшей структуре из одного маршрутизатора и одного кэш-процессора все 256 ячеек назначаются одному кэш-процессору. Если добавить в систему еще один процессор, то WCCP-маршрутизатор равномерно распределит пакеты между двумя кэш-процессорами так, чтобы на каждое устройство приходилось по 128 ячеек. Если установить третий кэш-процессор, WCCP-маршрутизатор назначит каждому из трех устройств 85 или 86 ячеек.

Установка новых кэш-процессоров может осуществляться "на ходу", без отключения системы, когда кластеры работают на полной мощности. В этой ситуации WCCP-маршрутизатор автоматически перераспределяет ячейки между всеми членами кэш-кластера, включая вновь установленный кэш-процессор. Поскольку у нового кэш-процессора еще нет содержимого, в кэше будет часто не хватать данных для ответа на запрос до тех пор, пока в локальное хранилище не будет занесено достаточно содержимого. Для того чтобы смягчить период "раскачки", новый кэш-процессор на начальном этапе запрашивает необходимую информацию у других членов кэш-кластера. Если таковая обнаружена, то она передается новому кэш-процессору. Если новый кэш-процессор сочтет, что получил от членов кластера достаточно содержимого (согласно параметрам конфигурации), то при недостатке данных в кэше он начнет обращаться за содержимым непосредственно к конечному серверу, а не к другим кэш-процессорам кластера.

Отказоустойчивость и защита от сбоев

Если в каком-либо из кэш-процессоров кластера происходит сбой, то кластер восстанавливается автоматически. WCCP-маршрутизатор равномерно перераспределяет загрузку отказавшего кэш-процессора между остальными кэш-процессорами. Кэш-кластер продолжает работу, используя на один кэш-процессор меньше.

Система сетевого кэширования Cisco обеспечивает совместный доступ к кластеру кэш-процессоров пары маршрутизаторов, поддерживающих протокол WCCP и протокол мультигруппового маршрутизатора "горячего" резервирования (Multigroup Hot-Standby Router Protocol — MHSRP), что образует полностью избыточную систему кэширования, называемую множественной WCCP-адресацией (WCCP multihoming). В случае отказа WCCP-маршрутизатора начинают работать стандартные механизмы отказоустойчивости и восстановления Cisco IOS. Например, маршрутизатор "горячего" резервирования может динамически взять на себя перенаправление сетевых запросов кластеру кэша. Если откажет весь кэш-кластер, то WCCP-маршрутизатор автоматически прекращает перена-

правление потоков данных кэш-кластеру, посылая Web-запросы клиентов узлу-источнику традиционным способом. Для пользователей полный сбой кэш-кластера выразится только в увеличении времени загрузки Web-содержимого. Такая структурная отказоустойчивость достигается благодаря тому, что кэш-кластер не расположен на пути прохождения остальных потоков данных клиентов.

Поддержка многоадресных WCCP-маршрутизаторов

Как уже отмечалось, система сетевого кэширования Cisco позволяет подключать кэш-процессорный кластер к нескольким WCCP-маршрутизаторам для обеспечения избыточности. Таким образом, Web-данные от всех WCCP-маршрутизаторов перенаправляется кэш-кластеру. Например, кэш-процессорный кластер, подключенный к обоим маршрутизаторам MHSRP-пары, образует полностью избыточную систему кэширования, в которой нет одиночных точек отказа (рис. 54.7).

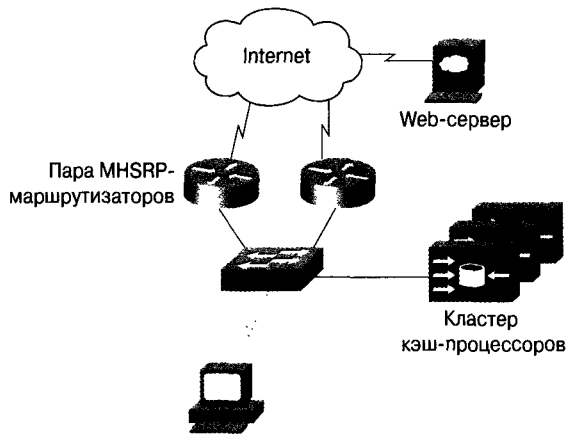


Рис. 54.7. Конфигурация полностью избыточного кэш-процессорного кластера

Снятие избыточной нагрузки

В случае внезапного всплеска потоков Web-данных на кэш-процессорном кластере может возникнуть перегрузка. Для того чтобы обойти эту ситуацию, в случае если кэш-процессор определяет, что кластер перегружен, то он отказывается от дополнительных запросов и передает их серверам-источникам. Последние отвечают непосредственно клиентам, поскольку переданные им запросы не были обработаны кэш-процессором (рис. 54.8).

Перегруженный кэш-процессор возобновит прием запросов, когда найдет достаточно ресурсов, чтобы сделать это без риска перегрузки в ближайшем будущем. Режим перегрузки автоматически включается и отключается центральным процессором и файловой системой. В критической ситуации, когда кэш-процессор настолько перегружен, что оказывается неспособным ответить на основные WCCP-сообщения проверки состояния от своего маршрутизатора, WCCP-маршрутизатор удаляет кэш-процессор из кластера и перераспределяет его ячейки.

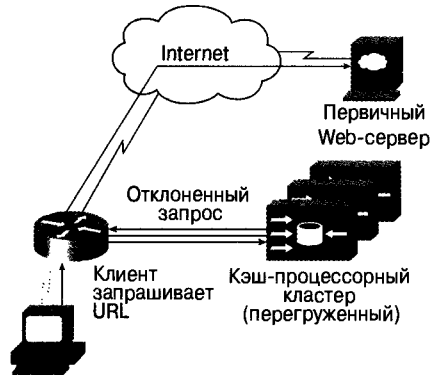


Рис. 54.8. Снятие избыточной нагрузки

Таким образом, режим снятия избыточной нагрузки гарантирует, что кэш-процессорный кластер не приведет к аномальным задержкам и сохранит доступ к сети даже при необычно интенсивном потоке данных.

Динамический сквозной пропуск клиентов

На некоторых Web-узлах требуется идентификация клиентов по IP-адресу. Однако если между клиентом и Web-сервером стоит сетевой кэш, то Web-сервер "видит" только IP-адрес кэша, но не адрес клиента.

Для решения этой и подобных проблем, в Cisco Cache Engine имеется функция динамического сквозного пропуска клиентов, которая позволяет последним при определенных условиях подключаться к Web-серверу непосредственно, в обход кэш-процессора. Cisco Cache Engine сохраняет существующие модели IP-идентификации и передает клиентам сообщения об ошибках с сервера. Поскольку кэш-процессор динамически адаптируется к ситуации, для обеспечения прозрачности кэша требуется меньше усилий.

Функция динамического сквозного пропуска клиентов

На рис. 54.9 показана ситуация, когда клиент посылает Web-запрос, который перенаправляется кэш-процессору. Если на кэш-процессоре нет соответствующего содержимого, то он пытается получить его с источника на Web-сервере.

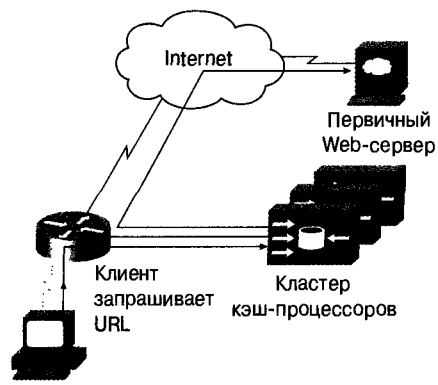


Рис. 54.9. Динамический сквозной пропуск клиента

На рис. 54.10 изображена ситуация, когда в ответ на запрос кэш-процессора сервер выдает код сообщения об ошибке HTTP (например, 401 — несанкционированный доступ, 403 — запрет доступа или 503 — недоступность службы). В этом случае кэш-процессор запускает систему динамического сквозного пропуска клиента. Он динамически сохраняет IP-адреса клиента и сервера, к которому он обращается, для того, чтобы пропускать все последующие пакеты, направляющиеся по этому пути. Кэш-процессор посылает броузеру клиента автоматически формируемое HTTP-сообщение о необходимости повторной попытки.

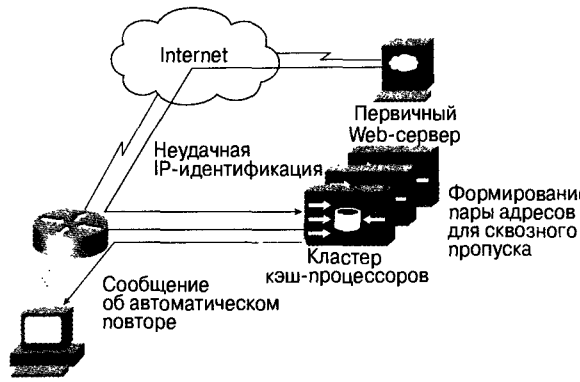


Рис. 54.10. Динамический сквозной пропуск клиента

На рис. 54.11 показана ситуация, когда броузер клиента автоматически производит перезагрузку. Запрос перенаправляется кэш-процессору. Однако после проверки таблицы сквозного пропуска и обнаружения записи, которой соответствует запрос, кэш-процессор отказывает в удовлетворении запроса и отправляет его напрямую серверу-источнику. Таким образом, сервер-источник получает IP-адрес клиента, идентифицирует его и отвечает непосредственно клиенту.

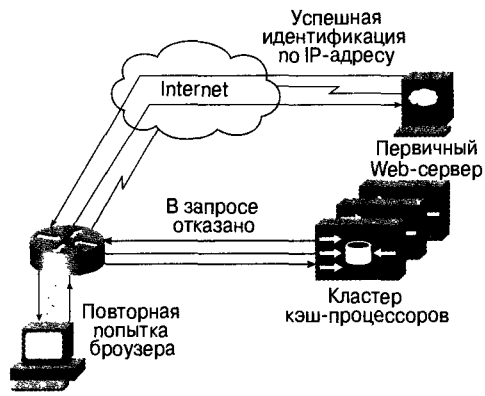


Рис. 54.11. Динамический сквозной пропуск клиента

Обратное прокси-кэширование

Кэш-процессоры часто размещают рядом с клиентами для ускорения реагирования сети и сокращения использования глобальных каналов связи. Таким образом, в кэши

заносится информация, к которой клиенты обращаются наиболее часто. Кроме того, кэш-процессоры иногда размещают перед многосерверными системами с целью повышения их пропускной способности и скорости работы Web-узла. Такая конфигурация называется *обратным прокси-кэшированием*, так как в кэш-процессоры попадает содержимое только с тех Web-серверов, перед входом на которые они установлены.

Такая возможность особенно полезна в том случае, когда кэш-процессоры устанавливаются на входе многосерверных систем, где некоторая информация используется гораздо чаще, чем другая. Использование обратного прокси-кэширования позволяет администраторам предупреждать влияние небольшого количества часто используемых URL на общую производительность сервера. Более того, это означает, что такие часто используемые URL не нуждаются в идентификации, ручной репликации, дублировании или специальном управлении, не применяемом к остальным URL.

Функция обратного прокси-кэширования

На рис. 54.12 каждый кэш-процессор привязан к WCCP-маршрутизаторам и WCCP-коммутаторам, обслуживающим многосерверные системы. Когда входящий Web-запрос достигает WCCP-маршрутизатора, последний хеширует IP-адрес и номер порта источника запроса, помещая запрос в одну из 256 ячеек. Эта функция хеширования распределяет входящие запросы статистически равномерно по всем ячейкам. Кроме того, эти ячейки равномерно распределяются по всем кэш-процессорам кластера.

Поскольку функция хеширования основана на обработке IP-адреса и номера порта источника, а не получателя запроса, Web-объект может храниться в нескольких кэш-процессорах кластера. Распределяя часто запрашиваемую информацию по всему кэш-кластеру, функция обратного прокси-кэширования позволяет обслуживать такие запросы нескольким кэш-процессорам. Таким образом, установка в кластере дополнительных кэш-процессоров приводит к повышению скорости доступа к популярным Web-узлам и сокращению времени загрузки содержимого.

Следует обратить внимание на то, что хеширование по конечному IP-адресу также обеспечило бы обратное прокси-кэширование. Но в этом случае все запросы имели бы один и тот же конечный IP-адрес и переадресовывались бы на один и тот же кэш-процессор. Такой метод приемлем, если не требуется использовать несколько кэш-процессоров на входе многосерверной системы.

Обновление содержимого

Любая система кэширования должна гарантировать, что пользователи получат из сетевого кеша то же содержание, что и с Web-сервера. Любая Web-страница состоит из нескольких Web-объектов, и каждый такой объект имеет собственные параметры кэширования, определяемые его авторами и стандартами HTTP. Таким образом, даже на Web-странице с объектами, изменяющимися в реальном времени, обычно есть много других объектов, подлежащих кэшированию. Обычно не кэшируются анимированные баннеры и отклики, CGI (Common Gateway Interface). Кэшированию подлежат такие объекты, как панели инструментов, полосы прокрутки, изображения в форматах GIF и JPEG. Таким образом, остается получить с сервера-источника только некоторые динамические объекты Web-страницы, а статические объекты могут обрабатываться локально.

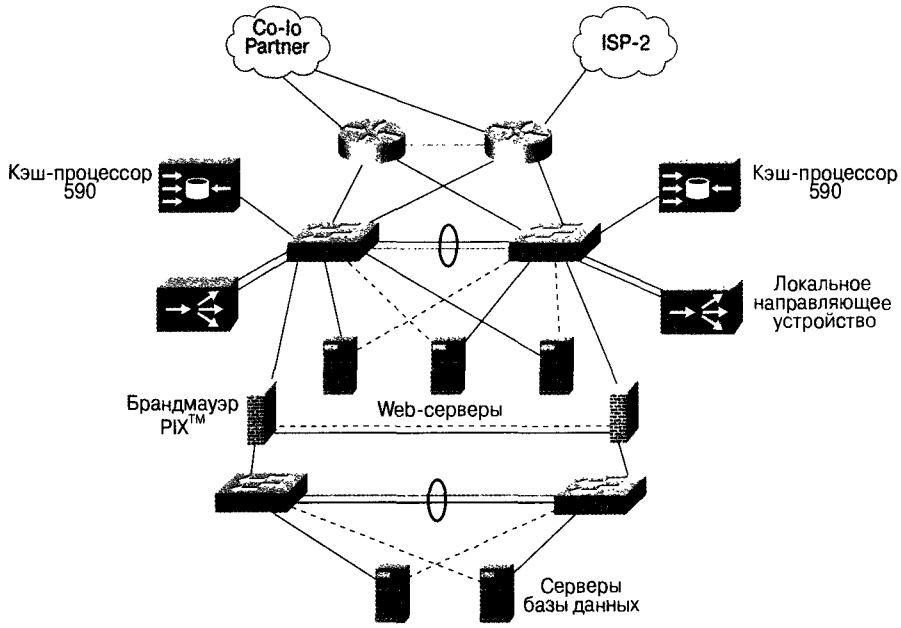


Рис. 54.12. Обратное прокси-кэширование

Продукты Cisco Cache Engine обеспечивают обновление содержимого согласно HTTP-стандартам кэширования и позволяют кэш-администраторам управлять обновлением информации, получаемой с серверов-источников.

Стандарты HTTP-кэширования

Параметры кэширования объектов на Web-странице определяются стандартами кэширования HTTP 1.0 и 1.1.

Стандарт HTTP 1.0 позволяет отключить кэширование любого объекта в поле заголовка псевдокомментария (pragma) и хранить содержимое в кэше в течение неопределенного времени.

Стандарт HTTP 1.1 позволяет определить срок хранения содержимого в кэше. Для каждого объекта Web-страницы можно выбрать один из следующих режимов кэширования.

- не кэшировать;
- кэшировать;
- явно указать срок хранения в кэше.

В HTTP 1.1 предусмотрен механизм проверки данных на устаревание, называемый IMS (If-Modified-Since, "если изменен не позже..."). При получении запроса на хранящееся в кэше, но устаревшее содержимое или IMS-запроса от клиента, где кэшируемое содержимое устарело, кэш-процессор направляет Web-серверу упрощенный IMS-запрос. Если на сервере объект не изменялся со времени кэширования, сервер ответит упрощенным сообщением с разрешением кэш-процессору предоставить клиентам кэшированную копию. Если со времени кэширования объект изменился, сервер сообщит об этом кэш-процессору. Если клиент направил IMS-запрос, а содержимое еще не устарело, содержимое будет получено из кэша без проверки.

Средства контроля устаревания содержимого в кэш-процессоре

Администраторы могут управлять обновлением Web-объектов, хранящихся в кэш-процессоре, при помощи параметра, называемого *коэффициентом устаревания* (freshness factor) и определяющего скорость устаревания содержимого кэша. Когда объект помещается в кэш, его время существования (Time-To-Live — TTL) вычисляется по следующей формуле:

TTL = (текущая дата − дата последнего изменения) * заданный коэффициент устаревания.

Когда поступает следующий запрос на объект, срок годности которого в соответствии со значением TTL истек, кэш-процессор направляет IMS-запрос. Более подробная информация об IMS приведена в разделе "Стандарты HTTP-кэширования".

Если администратор предпочитает консервативную политику обновления, то он может выбрать низкий коэффициент устаревания (например, 0,05), с тем чтобы срок годности объектов истекал быстрее. Однако в этом случае станут более частыми IMS-запросы, а это означает дополнительную нагрузку на канал. Если администратор займет либеральную позицию, он может установить больший коэффициент устаревания для того, чтобы продлить срок годности объектов. В этом случае можно избежать лишней нагрузки на канал, вызванной запросами IMS.

Средства контроля устаревания в броузере

Наконец, клиенты всегда могут явно обновить содержимое окна броузера при помощи кнопки перезагрузки страницы.

Перезагрузка страницы представляет собой команду броузера, запрашивающая обновление данных. Перезагрузка страницы вызывает серию IMS-запросов, требующих получения только измененных данных. Использование кнопки перезагрузки совместно с клавишей <Shift> приводит к расширенной перезагрузке страницы. В правильно работающих броузерах по этой команде вместо IMS-запроса всегда выполняется полная загрузка страницы с сервера-источника, а кэш-процессоры не используются.

Резюме

Большая часть потоков Web-данных избыточна. Одни и те же пользователи зачастую многократно обращаются к одному и тому же содержимому. Зная это можно значительно сократить объем передачи данных по глобальным сетям, что обеспечивает большую экономию для предприятий и провайдеров.

Кэширование представляет собой метод хранения часто запрашиваемой информации в месте, близком к источнику запросов. У кэширования есть два основных преимущества:

- стоимость;
- удобство использования.

Внедрение технологий кэширования ускоряет доставку данных, оптимизирует пропускную способность глобальных сетей и позволяет производить мониторинг содержимого.

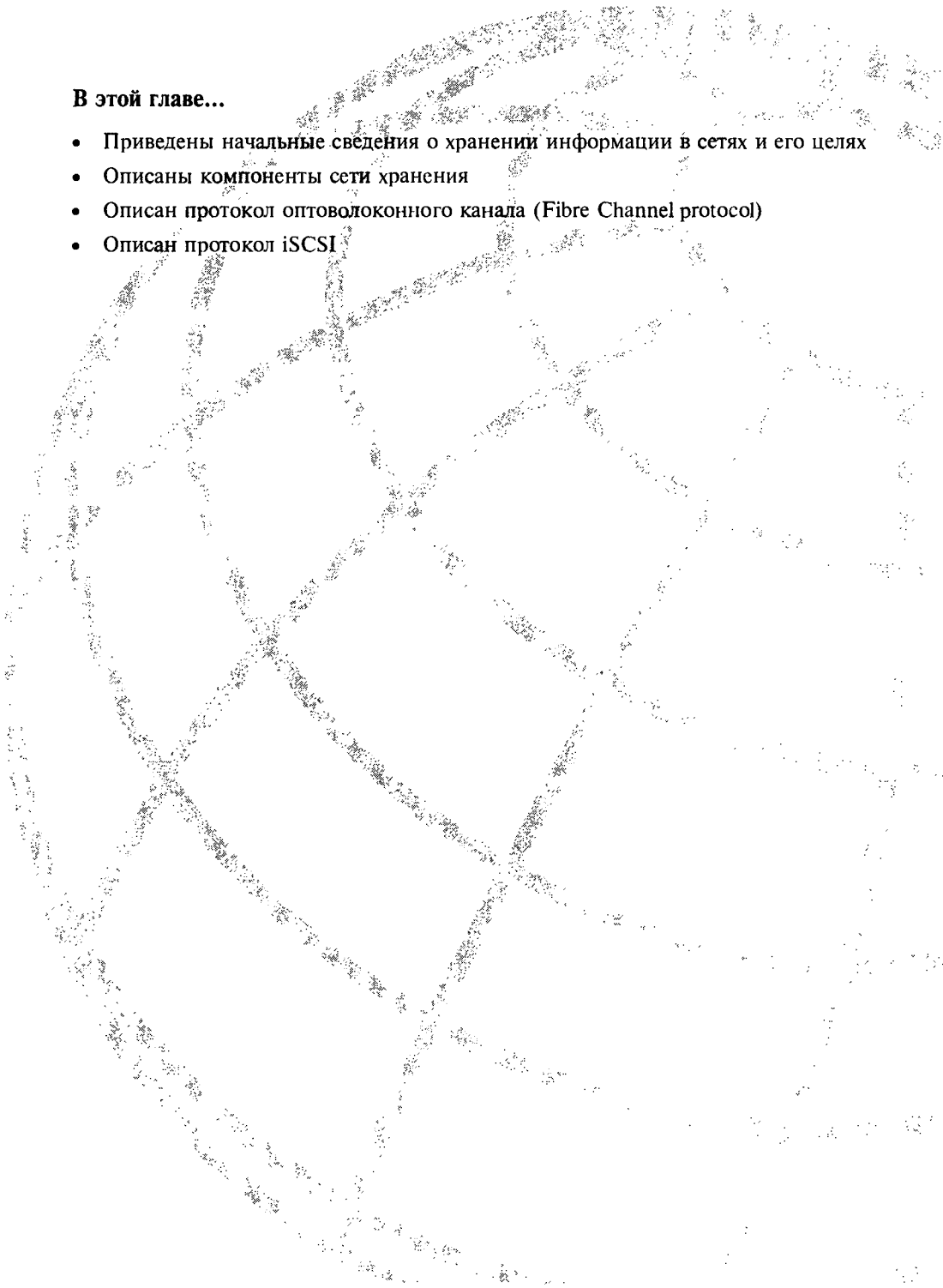
Корпорация Cisco разработала аппаратно-программный кэш-процессор, интегрированный в сеть и работающий на системном уровне.

Контрольные вопросы

1. Какая концепция лежит в основе сетевого кэширования?
2. Назовите два дополнительных преимущества от внедрения технологии кэширования.
3. Дайте краткое описание технологии интегрированного сетевого кэширования.
4. Как с помощью кэш-процессоров Cisco гарантировать обновление Web-страниц?
5. Приведите пример объекта, который можно сохранить в кэш-памяти, и объекта, который нельзя в ней сохранить.

В этой главе...

- Приведены начальные сведения о хранении информации в сетях и его целях
- Описаны компоненты сети хранения
- Описан протокол оптоволоконного канала (Fibre Channel protocol)
- Описан протокол iSCSI



Глава 55

Сети для хранения информации

В современном автоматизированном мире организации, связанные с информационными технологиями, продолжают искать новые методы, позволяющие оптимизировать производственные процессы в уже существующих технологиях и уменьшить общие затраты. Прошли те дни, когда приходилось лично посещать банковского кассира и регистрировать сделки в гроссбухе. Вместо этого все большее количество коммерческих операций передаются компьютерным приложениям, что обеспечивает ускорение обслуживания, экономию средств, большую доступность и уменьшение операционных расходов. В настоящее время клиент может выполнять свои банковские операции через ATM-сеть, через Web-браузер, по телефону и даже через PDA. Однако постоянное развитие и реализация компьютерных приложений, особенно Internet-приложений, с головокружительной скоростью приводят к созданию огромных объемов данных. Кроме того, требования к доступности данных и скорости их передачи постоянно возрастают. Сталкиваясь с необходимостью размещения и управления огромными количествами хранимых данных, IT-организации постоянно изменяют способы размещения хранимых данных, поддержки и доступа к ним.

В прошлом хранимые данные непосредственно закреплялись за серверами, на которых установлены приложения, которым требуются эти данные (модель хранения с непосредственным закреплением (direct-attached storage [DAS] model). Такое закрепление осуществлялось, как правило, через параллельное SCSI-соединение, хотя в некоторых сравнительно новых системах могли использоваться непосредственные ("точка-точка") петлевые соединения протокола Fibre Channel. Однако DAS-модель обладает недостаточной эффективностью в отношении производительности, гибкости и стоимости. По своей природе она предназначена для исключительного использования сервером приложений, к которому она присоединена. Это затрудняло повышение пропускной способности или перераспределение неиспользуемой. Кроме того, DAS-модель требовала дополнительных затрат, связанных с управлением многочисленными и часто качественно различными устройствами хранения, размещенными по всему центру данных. В заключение следует сказать, что полоса пропускания параллельного петлевого соединения SCSI или оптоволоконного канала (Fibre Channel) совместно использовалась всеми устройствами шины или петли. Модель совместного использования полосы пропускания ограничивала количество доступных устройств хранения и общую доступную полосу пропускания.

Осознавая неизбежность предстоящих проблем, связанных с хранением данных, многие IT-организации переходят от DAS-модели к модели сетей с зонами хранения

(Storage Area Network — SAN). Применение открытых сетевых блоков в качестве устройств хранения с серверами приложений предоставляет различные преимущества. Использование модели SAN расширяет возможности хранения, включая более специализированное обеспечение и модель перемещения. Это позволяет быстрее реализовать сеть хранения информации и/или модифицировать ее, а также добиться более эффективного ее использования. Система SAN также представляет собой централизованную точку, в которой консолидированные ресурсы, включая дисковые и ленточные накопители, могут управляться более эффективно. На рис. 55.1 показаны компоненты типичной сети хранения и их расположение. Как видно из рисунка, сеть хранения состоит из локального центра данных и удаленных соединений, осуществляемых через распределенные сети (Wide-Area Network — WAN) или через сети городского масштаба (Metro-Area Network — MAN).

Рис. 55.1. Модель сети хранения

Что представляет собой система SAN?

Система хранения и доступа к информации SAN представляет собой коммуникационную сеть, используемую для соединения между собой компьютерных устройств, таких как конечные станции приложений, с устройствами хранения, такими как дисковые и ленточные накопители. В обычной терминологии сетей хранения, сложившейся на основе протокола SCSI, пользователи хранимых данных называются *инициаторами (initiators)*, а блоки устройств хранения называются *целевыми устройствами (target)*. Двумя основными коммуникационными протоколами, используемыми для построения сети SAN, являются протоколы Fibre Channel и SCSI, работающие совместно с протоколом TCP/IP или протокол iSCSI. Чаще используется протокол Fibre Channel,

поскольку в его применении уже накоплен определенный опыт. Однако протокол iSCSI, ныне являющийся стандартом IETF, позволяет построить сеть SAN, используя менее дорогостоящую инфраструктуру Ethernet. На рис. 55.2 показана коммуникационная модель *инициатор-целевое устройство (initiator-target)* сетей SAN на базе протоколов Fibre Channel и iSCSI. В случае использования протокола iSCSI реализация сети, как правило, включает в себя мостовое соединение между Ethernet-инфраструктурой протокола iSCSI и инфраструктурой протокола Fibre Channel. Применение такой гибридной инфраструктуры объясняется относительной нехваткой целевых устройств, изначально поддерживающих протокол iSCI. В настоящей главе основное внимание уделяется протоколу Fiber Channel, хотя приведены также и начальные сведения о протоколе iCSCI.

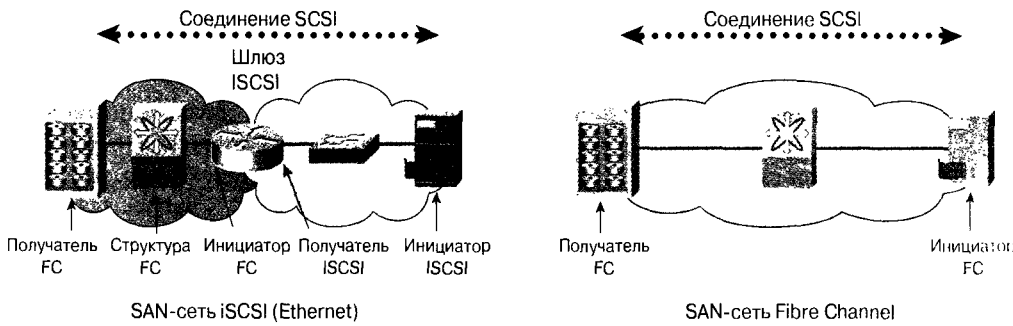


Рис. 55.2. Коммуникационная модель iSCSI

Сеть SAN представляет собой ряд коммутаторов Fibre Channel или Ethernet, объединенных в сети с различной топологией, из которых, в свою очередь создаются более крупные сети, имеющие большую плотность портов. В протоколе Fibre Channel отдельные коммутаторы называются *структурами (fabric)*, соединенные группы таких коммутаторов также называются *структурами*. Термин *Ethernet-структура* часто используется по отношению к сетям Ethernet, из которых строятся SAN-сети протокола iSCSI. В настоящей главе термин *структура* используется по отношению к группе соединенных между собой коммутаторов сети SAN.

Целью создания и использования SAN-сети является предоставление гибкого и централизованного средства связи, позволяющего большому количеству инициаторов получать доступ к большому количеству целевых устройств. Такая модель сети имеет больше общего с моделью "клиент/сервер", чем с моделью сети, состоящей из одноранговых устройств. Сети SAN во многом аналогичны обычным коммуникационным сетям передачи данных, включая IP-сети, поскольку обладают рядом сходных с ними характеристик, описанных ниже.

- **Возможность использования нескольких протоколов**. Хотя наиболее часто используется протокол Fibre Channel, существуют и другие протоколы хранения данных, такие, как созданные корпорацией IBM протоколы ESCON, FICON и SSA. Протокол iSCSI является новичком в семействе протоколов хранения, предоставляющим значительные преимущества в отношении стоимости инфраструктуры и управляемости.
- **Возможность использования различных типов соединений**. В сети хранения могут быть использованы различные типы соединений, выбор которых зависит от

типа используемой линии (выделенной или совместного использования), от скорости канала, длины линии и используемой среды. Например, при использовании протокола Fibre Channel соединение может быть создано методом конкурентной петли (линия совместного использования), методом соединения структур (выделенная линия), с использованием медного провода или оптоволоконного кабеля, со скоростью 1 или 2 Гбит/с.

- **Иерархическая схема адресации.** В сетях хранения, независимо от того, какой из протоколов используется (Fibre Channel или iSCSI) для маршрутизации фреймов данных и их пересылки между конечными узлами, используется иерархическая схема адресации. Кроме того, в сетях SAN используются протоколы динамической маршрутизации, например, в протоколе Fibre Channel используется протокол выбора кратчайшего пути в структуре (Fabric Shortest Path First — FSPF). Такие протоколы в сети SAN динамически строят предпочтительные маршруты и в случае сбоя в канале выполняется альтернативная маршрутизация.
- **Интегрированная безопасность в сети.** Сети хранения, как и другие коммуникационные сети, обладают функциями, позволяющими избирательно ограничивать видимость или связь между отдельными парами устройств, находящихся в одной физической сети. В сетях хранения протокола Fibre Channel для ограничения видимости или связи используется *принцип использования зон (zoning)*, который позволяет видеть друг друга и устанавливать связь только устройствам, относящимся к одной и той же зоне. В SAN-сетях протокола iSCSI для обеспечения безопасности могут использоваться также механизмы протокола IP, такие как списки доступа.
- **Управление потоками на основе характеристик сети.** Как и для любой другой сети, частью проектирования сети хранения является реализация механизма избыточной подписки (oversubscription). Он всегда присутствует, поскольку его ликвидация была бы слишком дорогостоящей. Следует также отметить, что поскольку предполагается, что вся связь происходит между инициаторами и целевыми устройствами, весьма маловероятно, что все целевые устройства смогут поддержать тот объем ввода/вывода (I/O), который может быть сгенерирован всеми инициаторами в пиковом режиме. Вследствие этого сети хранения проектируются с избыточной подпиской, обычно унаследованной от выбранной модели проектирования "база-граница" (core-edge). Однако бывают случаи, когда переполнение происходит в точках консолидации, таких как восходящие каналы от базового устройства к граничному. Сети хранения, использующие протокол Fibre Channel, как и другие сети, имеют механизмы управления потоками, использующие механизм буферного кредита, который может замедлить скорость передачи конечных устройств для того, чтобы помочь ликвидировать точки переполнения.
- **Служба назначения в сети приоритетов.** В некоторых случаях желательно обеспечить приоритетное обслуживание некоторых потоков данных. Такое обслуживание часто применяется в моменты переполнения, когда следует обеспечить приоритетную передачу данных от некоторых приложений или станций. Как и в сетях протокола IP, в сетях хранения Fibre Channel имеются возможности обеспечения качества обслуживания (QoS), осуществляющего приоритетную установку в очередь фреймов на основе их тегов, что минимизирует влияние переполнения на потоки данных от выбранных станций.

- **Гибридная модель связи**. В сетях передачи данных используются две основных модели связи. Одной из них является *дейтаграммная модель*, в которой фреймы данных просто передаются по сети, без каких-либо гарантий того, что они дойдут до места назначения или гарантий наличия в сети адекватных ресурсов для обработки отправленных фреймов. На всем пути от отправителя до получателя на каждом отдельном переходе принимаются независимые решения об отправке. При использовании второй, *канальной* модели коммуникации, на пути от источника к получателю создается выделенный канал для которого резервируются ресурсы. В действительности многие протоколы используют гибрид этих двух моделей. Протокол Fibre Channel, как и протокол TCP/IP, представляет собой гибридную модель, в которой с использованием процедуры `login` устанавливается канал от источника к получателю, однако для него не выделяются специальные ресурсы. В сети протокола Fibre Channel, как и в IP-сети, на каждом переходе принимаются независимые решения.

Следует, однако, отметить некоторые различия между сетями протокола Fibre Channel и традиционными IP-сетями передачи данных.

- **Чувствительность к задержке**. Транзакции, проходящие по сетям хранения, чувствительны к величине задержки. Эти транзакции, в первую очередь состоящие из команд SCSI, таких как **`read`** и **`write`**, представляют собой синхронные транзакции, которые упорядочены и часто требуют завершения выполнения предыдущей команды перед началом выполнения следующей. Вследствие высокой скорости операций ввода/вывода (I/O), возможной в сетях хранения, любая возможная избыточная задержка способна значительно повлиять на эффективность работы сети. Вследствие этого одной из задач сети SAN является минимизация задержки путем уменьшения количества переходов между источником и получателем и первоочередная обработка в точках переполнения данных с высоким приоритетом. Это может быть выполнено в сетях хранения как протокола Fibre Channel, так и протокола IP путем соответствующего проектирования сети и ее настройки.
- **Требование доставки фреймов в правильном порядке**. Общим требованием в сетях хранения является доставка фреймов от источника к получателю, насколько это возможно, в правильном порядке. Хотя фреймы упорядочены путем нумерации, некоторые устройства сети хранения могут оказаться неспособными переупорядочить фреймы или испытывают сбой при получении фреймов, порядок которых не соответствует требуемому. В любом случае переупорядочивание фреймов вызывает дополнительную задержку. Вследствие этого при проектировании сети хранения или перераспределении нагрузки важно обеспечить прохождение фреймов, ассоциированных с одним и тем же обменом SCSI, по одному и тому же маршруту.
- **Вход в структуру по процедуре `Log in`.** Перед тем как между инициаторами и целевыми устройствами начнется передача обменов, все устройства должны выполнить процедуру `log in` входа в сеть. В сетях Fibre Channel этот вход по процедуре `login` происходит в двух местах. Сначала устройство должно выполнить процедуру `login` для входа в сеть, а затем с другим устройством перед каждым обменом данными с ним.
- **Управление потоком, основанное на разрешениях**. Уникальной характеристикой сетей хранения Fibre Channel является управление потоком, основанное

на разрешениях. Перед тем как устройства смогут передавать фреймы, они должны получить разрешение или *кредит (credit)* от своего соседнего устройства, которым может быть устройство или сама сеть. Это разрешение имеет форму *буферного кредита (buffer credit)*, иначе называемого *упорядоченным набором готовности получателя (receiver-ready (R_RDY) ordered set)*, получаемого от структуры. Механизм *буферного кредита (buffer credit)* позволяет в случаях переполнения в структуре плавно уменьшать скорость передачи потоков данных.

В последующих двух разделах приведено подробное описание протоколов Fibre Channel и iSCSI.

Протокол Fibre Channel

Работа над стандартами протокола Fibre Channel началась еще в 1988 году. Первый стандарт американского института стандартов (American National Standards Institute — ANSI) был одобрен в 1994 году и назван стандартом FC-PH (ANSI X3.230:1994). Протокол Fibre Channel в качестве транспортного протокола первоначально разрабатывался для того, чтобы устранить недостатки современной параллельной инфрастуктуры Small Computer System Interface (SCSI), а также обеспечить более высокую скорость и большие возможности масштабирования. Хотя по протоколу Fibre Channel могут передаваться и данные других протоколов более высоких уровней, включая протоколы Intelligent Peripheral Interface (IPI), High-Performance Parallel Interface (HIPPI), IP и IEEE 802.2, однако в настоящее время он используется в первую очередь для передачи наборов команд и данных протокола SCSI. Организацией стандартов ANSI T11 протокол Fibre Channel определяется как протокол, использующий модель уровневых служб. Спецификация ANSI *FC-PH Physical and Signaling Interface* определяет модель уровневых служб протокола Fibre Channel как показано на рис. 55.3.

Рис. 55.3. Модель уровневых служб

Каждый уровень этой модели определяет некоторый набор служб, каждый из которых опирается на работу нижнего по отношению к нему уровня и обслуживает вышележащий уровень. Из рисунка также видно, что протокол Fibre Channel разработан

для поддержки нескольких протоколов верхнего уровня. Однако в настоящее время он в первую очередь используется в качестве транспортного протокола для передачи данных протокола SCSI-3.

В приведенном ниже списке описаны все уровни, показанные на рис. 55.3.

- **FC-0.** Уровень FC-0 определяет спецификации физического интерфейса для различных сред передачи и связанных с ними приемников и передатчиков. В качестве передающих сред используются различные типы медных и оптоволоконных кабелей, а также поддерживаемые ими скорости передачи. На уровне FC-0 определяются также виды разъемов (штекеры и розетки), типы кабелей, уровни сигнализации носителя и соответствующие скорости.
- **FC-1.** На этом уровне определяются три первичные функции. Первая из них состоит в кодировании и декодировании потоков данных. На уровне FC-1 определена схема кодирования 8B/10B, которая связывает между собой символы данных и соответствующие биты синхронизации. Второй функцией уровня FC-1 является управление упорядоченными наборами. Упорядоченные наборы представляют собой уникальные слова передачи, которые поддерживают синхронизацию канала и управляющие протоколы. Примером упорядоченных наборов, управляемых уровнем FC-1, являются ограничители фреймов. Третьей функцией уровня FC-1 является управление протоколами канального уровня и состояниями, такими как активное состояние, состояние отключения от сети (offline), сбой в канале и состояние восстановления канала.
- **FC-2.** Уровень FC-2 является ответственным за выполнение функций, связанных с установкой и поддержкой связи между двумя портами. Эти функции включают в себя выполнение процедуры `login` для порта, проведение сеанса обмена (коммуникационный элемент в SAN-сетях протокола Fibre Channel) и связанных с ним процедур упорядочивания фреймов, управление потоками, а также обнаружение ошибок и их устранение. Все эти функции будут более подробно описаны ниже. Уровень FC-2 также определяет все используемые в протоколе Fibre Channel форматы фреймов данных и управляющих фреймов.
- **FC-3.**Уровень FC-3, уровень общих служб (Common Services), в целом является базой для будущих усовершенствованных служб, общих для нескольких портов узла. Такие службы FC-3 (некоторые из которых уже были разработаны, но пока редко используются) включают в себя службы многоадресатной рассылки, сжатие и стековую организацию службы запроса соединения.
- **FC-4.** Уровень FC-4 определяет, каким образом данные различных протоколов преобразуются в форматы протокола Fibre Channel. Эти протоколы более высокого уровня включают в себя протоколы SCSI-3, IP, протокол виртуального интерфейса (virtual interface — VI) и некоторые другие. Команды, данные и состояния каждого из этих протоколов преобразуются в информационные блоки, передаваемые по протоколу Fibre Channel.

В целом описанные выше уровни можно считать аналогами уровней эталонной модели OSI. Они предназначены для отражения структуры протокола, что облегчает его понимание и реализацию.

В следующем разделе протокол Fibre Channel рассматривается более подробно.

Топологии протокола Fibre Channel

SAN-сеть протокола Fibre Channel может состоять из нескольких сетей с различными топологиями, такими как топология коммутируемых структур, топология конкурентной петли или сеть с соединениями типа "точка-точка". Каждая из этих топологий определяет связанные с ней режимы портов Fibre Channel, которые должны поддерживаться находящимся в ней устройствами.

Топология сети с соединениями типа "точка-точка"

Топология типа "точка-точка" используется в первую очередь для непосредственного подсоединения станции к дисковому или ленточному накопителю. Она обеспечивает большую полосу пропускания, чем параллельное соединение SCSI, но ее применение ограничено связью между двумя устройствами. Эта топология уступает место другим, более ориентированным на сетевое применение топологиям, позволяющим соединить несколько устройств в сеть или объединить их в структуру.

Топология конкурентной петли

Широко применяемой, но постепенно устаревающей является топология конкурентной петли. *Конкурентная петля (arbitrated loop)* представляет собой логическую петлю, включающую в себя до 126 устройств Fibre Channel, которые оспаривают между собой право на передачу данных. Такая петля обычно реализуется с использованием концентратора Fibre Channel для кабельного управления, в результате чего образуется физическая звездообразная топология. Все устройства такой петли совместно используют доступную полосу пропускания. Например, дисковые накопители Fibre Channel обычно объединяются в небольшие конкурентные петли в подсистемах дисковых накопителей большего размера. Преимуществом конкурентной петли является возможность соединения между собой нескольких устройств.

Частные петли

Прежние типичные топологии в целом называются *топологиями частной петли (private-loop topologies)*, поскольку все устройства такой петли понимают только 8-битовый логический адрес других устройств данной локальной петли. Такая схема адресации не позволяет устройствам петли обращаться к устройствам других петель. Более современные реализации петель, называемые публичными петлями, поддерживают полные 24-битовые иерархические адреса, что позволяет устройствам одной петли осуществлять связь с устройствами других петель. Вследствие этого при реализации публичной петли несколько конкурентных петель могут быть соединены между собой с использованием коммутируемой структуры.

Топология коммутируемых структур

В настоящее время предпочтительной топологией в сетях Fibre Channel является *топология коммутируемых структур (switched-fabric topology.)*.Она объединяет лучшие качетсва прежних топологий в отношении количества соединений и доступной полосы пропускания. Топология коммутируемых структур предоставляет возможности, аналогичные тем, которые имеются в коммутируемых сетях Ethernet/IP.

Коммутаторы Fibre Channel объединяются в структуры и используют 24-битовый идентификатор Fibre Channel ID (FC_ID) для маршрутизации (пересылки) фреймов внутри структур от одного коммутатора к другому. Структура протокола Fibre Channel может включать в себя до 239 коммутаторов, каждый из которых может иметь порты до 64 Кбит/с. Каждый из портов коммутатора Fibre Channel может предоставлять каждому подсоединенному устройству полосу пропускания шириной до 1 или 2 Гбит/с. Коммутируемая структура также включает в себя ряд распределенных служб, таких как службы маршрутизации структур, службы имен и службы безопасности. На рис. 55.4 показаны три из описанных выше четырех топологий.

Типы портов протокола Fibre Channel

Fibre Channel представляет собой ориентированный на соединение протокол. Это означает, что *узлы (nodes)* перед обменом данными должны установить между собой канал связи посредством процедуры `login`. Соединение устанавливается между *логическими элементами (logical elements)*, иначе называемыми *портами (ports)*, которые логически связываются с существующими физическими устройствами. Порты могут принадлежать к различным типам, в зависимости от физического устройства и топологии соединений.

Тип порта определяется в результате автоматического обсуждения того, к какому устройству или топологии они принадлежат. Однако пользователь может ограничить возможные режимы портов, которые будут обсуждаться.

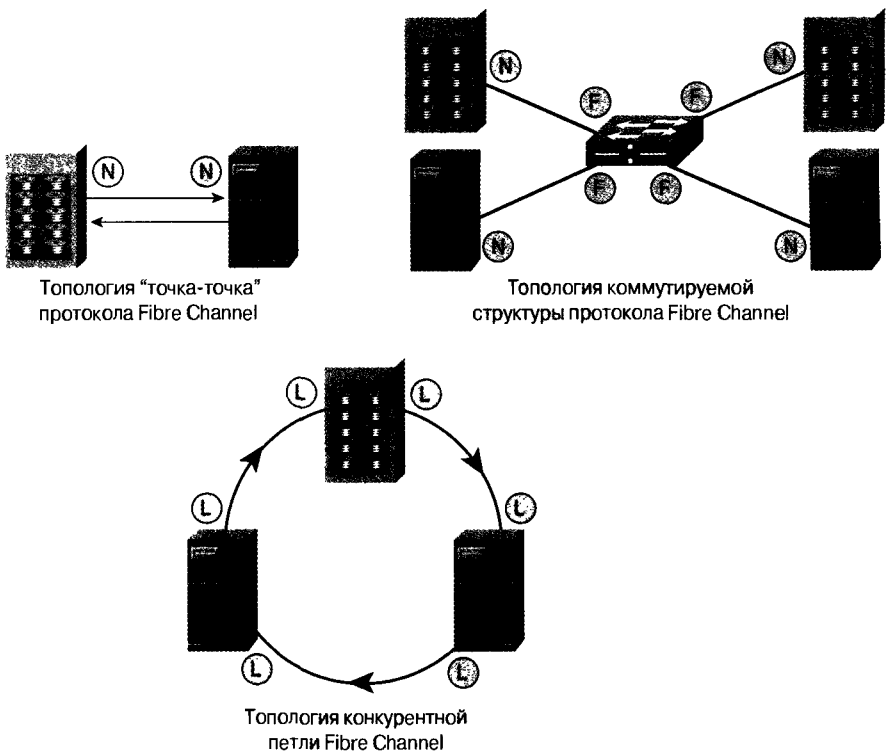


Рис. 55.4. Топологии протокола Fibre Channel

В приводимом ниже списке перечислены все стандартные и некоторые нестандартные типы портов, используемые в SAN-сетях протокола Fibre Channel.

- **N_Port.** Базовым типом порта является N_Port, или порт узла. Все обмены данными в сетях Fibre Channel происходят между портами типов N_Port или NL_Port. Порт N_Port находится на конечном устройстве, подсоединенном к сети с топологией "точка-точка" или с топологией коммутируемой структуры. На одном физическом устройстве могут существовать несколько портов N_Ports.
- **NL_Port.** Порты узлов, находящиеся в конечных устройствах, подсоединенных к сети конкурентной петли, называются портами узловой петли или портами NL_Port.
- **F_Port.** В коммутируемой структуре порты коммутатора, непосредственно подсоединенные к конечным устройствам (порты N_Port), называются портами структур или портами F_Port.
- **FL_Port.** Порты в коммутируемой структуре, подсоединенные к публичной конкурентной петле, называются портами структурной петли или портами FL_Port. Используя порты типа FL_Port публичные конкурентные петли могут быть соединены между собой с образованием топологии коммутируемой структуры. Порты FL_Port подсоединяются к петлям портов NL_Ports.
- **E_Port.** При соединении двух коммутаторов протокола Fibre Channel результирующий режим порта становится портом расширения или портом типа E_Port. Образовавшийся канал между двумя коммутаторами называется межкоммутаторным каналом (Inter-Switch Link — ISL). Порты E_Ports подсоединяются только к аналогичным портам E_Port.
- **B_Port.** Мостовой порт или B_Port не является типовым портом. Такой порт расширяет межкоммутаторный канал Fibre Channel ISL через порт иного типа, чем порт Fibre Channel. Порты типа B_Ports подсоединяются только к портам E_Ports и принимают участие только в базовом наборе канальных служб. Расширители каналов на IP-сети обычно используют интерфейс портов B_Port для расширения канала Fibre Channel ISL на IP-сеть.
- **TE_Port.** Специальным режимом порта, обсуждаемым между двумя многоуровневыми коммутаторами Cisco MDS 9000, является порт магистрального расширения или TE_Port. Такой порт является надстройкой или расширением порта типа E_Port; это означает, что специальный теговый механизм поддерживает способность виртуальной SAN-сети создавать многочисленные логические структуры поверх общей физической структуры. Порты TE_Port могут быть подсоединены только к аналогичным портам TE_Ports.
- **TL_Port.** Порты трансляционной петли или порты TL_Port соединяют частные петли с публичными петлями или с коммутируемыми структурами. Порт TL_Port выполняет функции адресного прокси-сервера для устройств конкурентной петли. Функция трансляционной петли полезна при использовании прежних устройств протокола Fibre Channel, которые не поддерживают публичную адресацию.
- **GL_Port.** Порт общей петли или порт GL_Port в действительности не является обсуждаемым режимом, а скорее отражает возможность порта. Порт, который может обсуждать режимы портов типов F_Port, FL_Port и E_Port называется портом GL_Port.

На рис. 55.5 показаны режимы соединений и возможности их использования.

Коммуникационная модель протокола Fibre Channel

В протоколе Fibre Channel используется методология соединения, которая требует, чтобы перед обменом данными между двумя устройствами между ними был установлен канал. Процесс установки канала включает в себя несколько этапов. После того, как канал установлен, обмен данными между конечными устройствами происходит согласно иерархической модели. Ниже приведены основные этапы установки связи между двумя устройствами, принадлежащими к различным топологиям протокола Fibre Channel. Для простоты некоторые несложные этапы опущены.

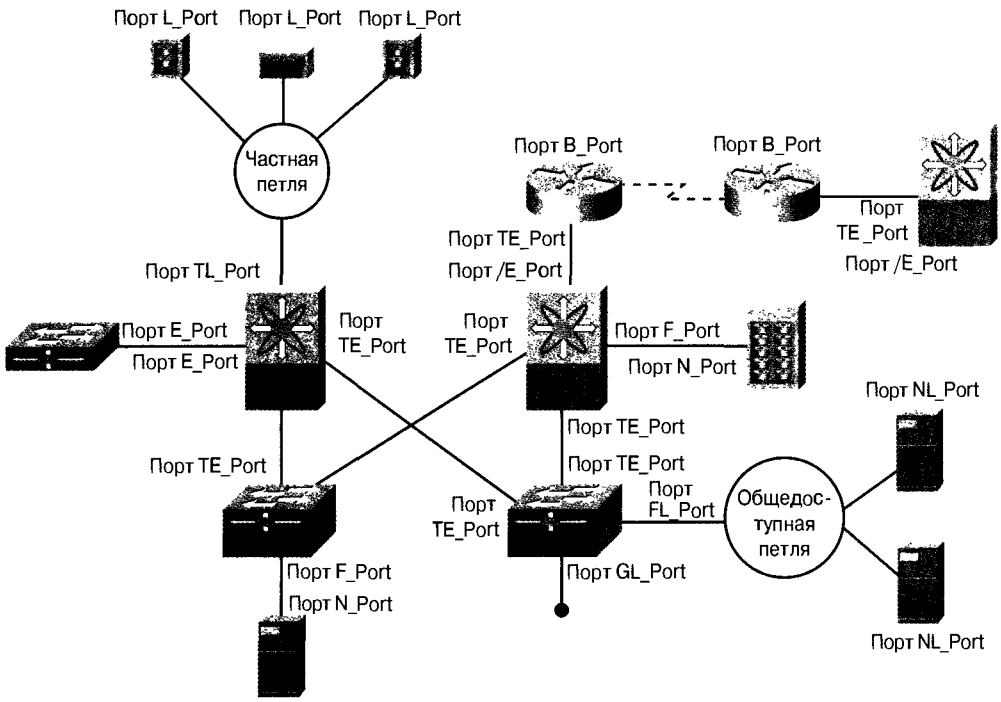


Рис. 55.5 Режимы соединений протокола Fibre Channel

Для соединений типа "точка-точка":

Этап 1. Устройства, принадлежащие сети с конфигурацией типа "точка-точка", ведут себя как два устройства, принадлежащие к частной конкурентной петле. Такие устройства сначала должны выполнить процелуру инициализации петли (loop initialization procedure — LIP) для определения того, принадлежат ли они к сети с конфигурацией типа "точка-точка" или к сети конкурентной петли.

Этап 2. Один порт NL_Port открывает канал к другому порту NL_Port.

Этап 3. Порты могут обмениваться данными.

Для конкурентной петли:

Этап 1. Устройства, подсоединенные к конкурентной петле, должны выполнить процедуру LIP для получения физического адреса конкурентной петли (Arbitrated Loop Physical Address — AL_PA), т.е. 8-битового адреса, используемого для коммуни-

кации с другими устройствами сети. Во время этого процесса порт NL_Port выясняет, имеется ли в петле порт типа FL_Port, присутствие которого делает ее публичной петлей. Если порт FL_Port отсутствует, то петля является частной.

Этап 2. Один порт типа NL_Port конкурирует за доступ к петле для осуществления связи с другим портом NL_Port.

Этап 3. После того, как получено право на доступ, порт NL_Port открывает соединение с другим портом NL_Port (или с портом FL_Port, если осуществляется связь с устройством коммутируемой структуры).

Этап 4. Порты могут начать обмен данными друг с другом.

Для коммутируемой структуры:

Этап 1 Устройства, подсоединенные к коммутируемой структуре, должны выполнить процедуру `login` входа в структуру (fabric login procedure — FLOGI) для получения адреса протокола Fibre Channel (Fibre Channel address (FC_ID), представляющего собой 24-битовый адрес, используемый для связи с другими устройствами коммутируемой сети.

Этап 2. Один порт N_Port должен выполнить процедуру `log in` для получения доступа к другому порту N_Port или порту NL_Port, с которым он будет осуществлять связь. Выполнение портом этой процедуры (port login procedure — PLOGI) выполняется для установки канала с целевым устройством.

Этап 3. Порты могут осуществлять взаимный обмен данными.

Сразу после установки канала связи между двумя устройствами протокол Fibre Channel строго следует коммуникационной модели, включающей в себя иерархию структур данных. На вершине этой иерархии находится обмен. Как правило, обмен протокола Fibre Channel преобразуется в команду протокола более высокого уровня, такую, например, как команда `read` протокола SCSI-3. Каждый обмен состоит из ряда однонаправленных предложений. В свою очередь каждое предложение состоит из нескольких пронумерованных фреймов, которые перемещаются от источника к получателю. Между двумя устройствами могут быть открыты несколько обменов, каждый из которых имеет свой набор идентификаторов ID инициатора обмена (originator exchange ID — OX_ID) и идентификаторов ID ответчика обмена (responder exchange ID — RX_ID). На рис. 55.6 показана эта иерархическая связь и приведен пример простого обмена по протоколу SCSI-3.

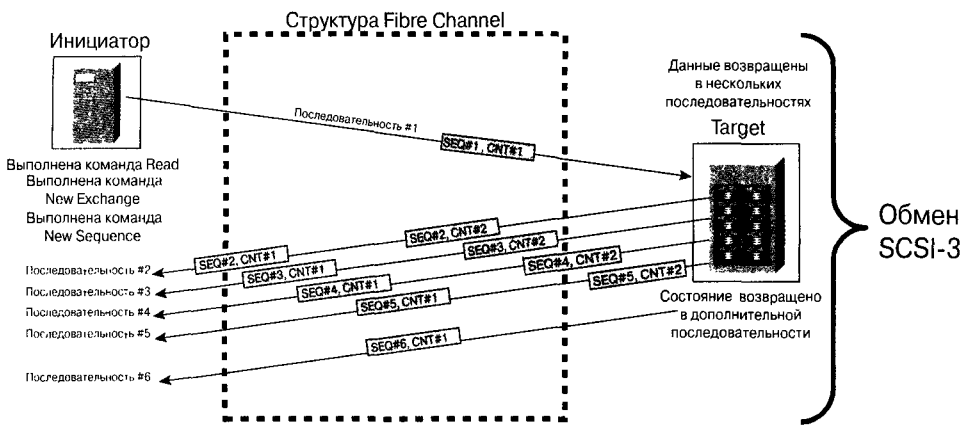


Рис. 55.6. Пример SCSI-обмена в сети протокола Fibre Channel

Адресация протокола Fibre Channel

В протоколе Fibre Channel имеется два типа адресов, которые используются для идентификации устройства или порта коммутатора. Первым типом является уникальный глобально назначаемый адрес, называемый мировым именем *(worldwide name — WWN)*. Адрес WWN назначается производителем и его глобальная уникальность гарантирована. Эта ситуация аналогична использованию MAC-адресов Ethernet-устройств.

Вторым типом адреса, используемым в протоколе Fibre Channel, является динамически назначаемый иерархический адрес, который позволяет целенаправленно пересылать фрейм от одного устройства к другому. Этот адрес называется идентификатором протокола Fibre Channel (Fibre Channel ID — FC_ID). В сети Fibre Channel идентификатор FC_ID преобразуется в адрес WWN, так что инициаторы могут использовать WWN для контакта с устройством, а затем этот адрес транслируется в FC_ID для осуществления связи. Адрес FC_ID, назначаемый устройству, зависит от типа топологии.

- **Топология "точка-точка".** Соединения "точка-точка" в действительности реализуются как частная петля между двумя устройствами. Поскольку устройства находятся в частной петле, они используют только 8-битовый адрес AL_PA. Этот адрес находится в диапазоне от 0x000001h to 0x0000Efh.
- **Конкурентная петля.** Конкурентные петли могут быть реализованы как частные или публичные петли, чем и определяется тип используемого адреса. В топологии частной петли стандартный адрес AL_PA назначается аналогично тому, как это делается в топологии "точка-точка". Каждому устройству частной петли назначается адрес из диапазона от 0x000001h до 0x0000Efh (однако в одной конкурентной группе могут находиться не более 126 устройств).
- **Публичная петля.** Публичная петля содержит один или более портов FL_Ports, которые действуют как шлюзы в коммутируемую структуру. Как таковой, назначенный устройству публичной петли адрес содержит полный 24-битовый адрес. Первый октет представляет собой идентификатор домена Domain_ID, назначенный коммутатору. Второй октет идентифицирует конкретную петлю на коммутаторе. Третий октет используется для адреса AL_PA, назначаемого устройствам этой петли. Порт FL_Port всегда имеет адрес AL_PA, равный 0x00h. Следовательно, реальный диапазон адресов для устройств публичной конкурентной петли представляется в виде *0xddllaa*, где *dd* — идентификатор Domain_ID подсоединенного коммутатора из диапазона от 0x01h до 0xEFh (от 1 до 239), *ll* — идентификатор петли из диапазона от 0x00h до 0xFF, а *aa* — адрес AL_PA из диапазона от 0x01h до 0xEFh, где адрес 0x00h зарезервирован для порта FL_Port.
- **Коммутируемая структура.** Адрес коммутируемой структуры основан на идентификаторе FC_ID, который использует полный 24-битовый адрес. Каждому коммутатору в коммутируемой структур назначается один или более идентификаторов Domain_ID. Этот Domain_ID можно рассматривать как префикс маршрутизации, который используется коммутатором для пересылки фреймов устройствам, подсоединенным к другим коммутаторам. Первым октетом идентификатора FC_ID является Domain_ID. Он находится в диапазоне от 0x01h до 0xEFh. Второй и третий октеты FC_ID коммутируемой структуры называются идентификаторами зоны Area_ID и порта Port_ID, соответственно. Эти компоненты FC_ID должны быть локально уникальными для каждого коммутатора.

Однако при идентификации устройств конечной структуры они используются по разному различными производителями коммутаторов. Некоторые производители располагают эти компоненты на основе физического порта, к которому подсоединено конечное устройство. Другие производители располагают их по принципу "первым пришел — первым обслужили". Стандарт не определяет правила размещения этих компонент адреса. Однако диапазоном действительности для этих адресов является диапазон от 0x0000h до 0xFFFFh.

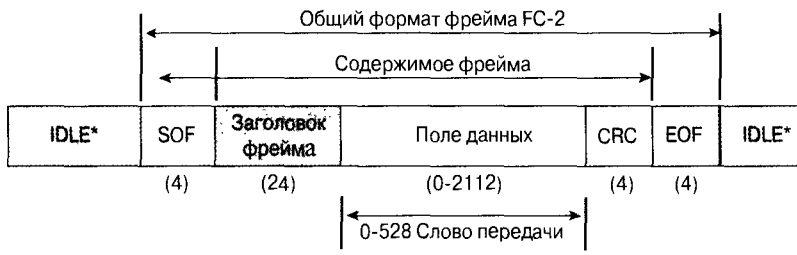
В табл. 55.1 обобщены различные модели FC_ID, их диапазоны адресов и ограничения.

Табл. 55.1. Модели и ограничения идентификатора FC_ID

	8 битов	8 битов	8 битов
Модель топологии коммутатора	Домен (01-EF)	Зона (00-FF)	Устройство (00-FF)
Модель адреса устройства частной петли	00	00	Физический адрес конкурентной петли (AL_PA) (01-EF)
Модель адреса устройства общедоступной петли	Домен (01-EF)	Зона (00-FF)	Физический адрес конкурентной петли (AL_PA) (00-EF)

Формат фрейма протокола Fibre Channel

Фрейм протокола Fibre Channel имеет стандартную структуру, показанную на рис. 55.7.



* 6 слов IDLE (24 байта), требуемых TX
2 слова IDLE (8 байт), гарантируемых для RX

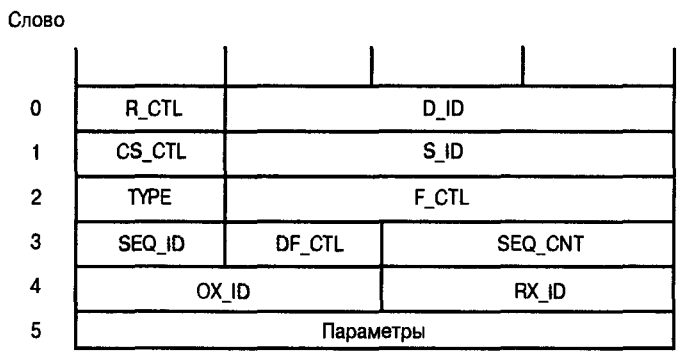
Рис. 55.7. Формат фрейма в протоколе Fibre Channel

Размер фрейма Fibre Channel находится в диапазоне от 36 до 2148 байтов, в зависимости от размера полезной нагрузки. Ниже приведено описание основных полей фрейма Fibre Channel.

- **Поле IDLE** IDLE используется для синхронизации и выравнивания слов у передатчика и приемника. Поля IDLE указывают на готовность к передаче и постоянно передаются, если другие данные для передачи отсутствуют. IDLE фактически представляет собой 4-байтовый *упорядоченный набор (ordered set)*, который передается от одного устроиства другому. В соответствии со стандартами Fibre Channel каждый передаваемый фрейм должен содержать шесть упорядоченных наборов, которые часто имеют поле IDLE, расположенное во фрейме

последним. Каждый получаемый фрейм должен быть заполнен как минимум двумя упорядоченными наборами.

- **Поле SOF** Поле начала фрейма (Start of Frame) представляет собой 4-байтовый *упорядоченный набор (ordered set)*, который непосредственно предшествует контенту (полезной нагрузке) фрейма. Поле SOF также указывает класс принимаемого фрейма.
- **Frame header (заголовок фрейма)** Заголовок фрейма имеет размер 24 байта и состоит из нескольких управляющих (контрольных) полей. Заголовок фрейма включает в себя такие поля, как FC_ID источника, FC_ID получателя, ID обменов, управление маршрутизацией и несколько других параметров. Полностью структура заголовка фрейма в протоколе Fibre Channel показана на рис. 55.8.
- **Data field (Поле данных)** Поле данных состоит из реальных данных протокола более высокого уровня. Оно может иметь длину от 0 до 2112 байтов.
- **CRC (Cyclical Redundancy Check)** Циклический контроль избыточности. Это поле имеет длину 4 байта и используется для проверки целостности фрейма. При вычислении значения этого поля используются только заголовок фрейма и поле данных (Data field).
- **EOF (End of Frame)** Поле конца фрейма представляет собой 4-байтовый упорядоченный набор, который непосредственно предшествует содержимому фрейма. Поле EOF также указывает классс фрейма Fibre Channel.



Формат заголовка фрейма протокола Fibre Channel

Рис. 55.8 Формат заголовка фрейма Fibre Channel

Ниже приводится краткое описание всех полей заголовка фрейма Fibre Channel.

- **R_CTL (Routing Control)** Поле управления маршрутизацией содержит два 4-битовых подполя: подполе типа маршрутизации и информационное подполе. Биты маршрутизации дифференцируют фреймы в соответствии с функцией или службой, например, фреймы данных отличаются от фреймов управления каналом, содержащих команды или состояния.
- **D_ID Fibre Channel ID (FC_ID)** Идентификатор Fibre Channel получателя (3 байта)
- **CS_CTL (Class-Specific Control)** Поле управления в зависимости от класса (Class-Specific Control), размером 1 байт, используется только в классах 1 и 4 (Class 1 или Class 4). Классы протокола Fibre Channel более подробно обсуждаются в следующем разделе.

- **S_ID** FC_Идентификатор ID источника Fibre Channel (3 байта).
- **Type** Поле типа (1 байт) указывает протокол верхнего уровня, данные которого пересылаются в поле полезной нагрузки.
- **F_CTL** Поле управления фреймом Frame Control (3 байта) содержит ряд флагов, которые управляют потоком в последовательности.
- **SEQ_ID (Sequence Identifier)** Поле идентификатора последовательности (1 байт) уникальным образом идентифицирует данную последовательность в контексте одного обмена. Каждый фрейм идентифицируется своим SEQ_ID.
- **DF_CTL (Data Field Control)** Поле управления полем данных (1 байт) указывает на наличие необязательных заголовков в начале поля данных (Data Field) для фреймов Device_Data Video_Data. Биты DF_CTL для фреймов Link_Control и Basic Link Service значения не имеют.
- **SEQ_CNT (Sequence Count)** Поле отсчета в последовательности (2 байта) указывает порядок передачи фреймов в последовательности. Оно используется получателем последовательности для учета всех передаваемых фреймов.
- **OX_ID (Originator Exchange ID)** Идентификатор инициатора обмена (2 байта) идентифицирует индивидуальный обмен. Эта идентификация выполняется инициатором обмена.
- **RX_ID (Responder Exchange ID)** Идентификатор ответчика обмена (2 байта) идентифицирует индивидуальный обмен. Эта идентификация выполняется ответчиком обмена.
- **Parameters** Поле параметров (Parameters) (4 байта) зависит от типа конкретного фрейма, задаваемого полем R_CTL.

Классы обслуживания протокола Fibre Channel

В протоколе Fibre Channel определены несколько классов обслуживания, хотя на практике, как правило, используются лишь два. Эти классы отличаются друг от друга тем, как в них реализуются механизмы подтверждения, управления потоком и резервирования каналов.

- Класс 1 представляет собой ориентированную на соединение службу с подтверждением доставки или уведомлением о том, что доставка не произошла. Перед тем как произойдет соединение, между источником и получателем должен быть установлен канал.
- Класс 2 представляет собой службу без установки соединения между портами с подтверждением доставки или уведомлением о том, что доставка не произошла.
- Класс 3 представляет собой службу без установки соединения между портами, без подтверждения доставки и без уведомления о том, что доставка не произошла. В настоящее время этот класс на практике используется наиболее часто.
- Класс 4 представляет собой ориентированную на соединение службу, которая обеспечивает виртуальный канал между портами N_Port с подтверждением доставки или уведомлением о том, что доставка не произошла, и гарантированной шириной полосы пропускания.

- Класс 6 представляет собой вариант класса 1 для многоадресатной рассылки (по схеме "один-со многими") с подтверждением доставки или уведомлением о том, что доставка не произошла.

В табл. 55.2 приведен обзор характеристик всех классов обслуживания. В современных SAN-сетях чаще всего используется класс 3. Большинство структур также поддерживают класс 2. Все остальные классы в настоящее время используются редко.

Табл. 55.2. Классы обслуживания протокола Fibre Channel

Атрибут	Класс 1	Класс 2	Класс 3	Класс 4	Класс 6
Ориентация на соединение	Да	Нет	Нет	Да	Да
Резервирование полосы пропускания	100%	Нет	Нет	Частичное	100%
Гарантированный максимум задержки	Да	Нет	Нет	Да (QoS)	Да
Гарантированный порядок доставки	Да	Нет	Нет	Да	Да
Подтверждение доставки	Да	Да	Нет	Да	Да
Мультиплексирование фреймов на портах	Нет	Да	Да	Нет	Нет
Сквозной контроль поток	Да	Да	Нет	Да	Да
Контроль потока на канальном уровне	SOFc1	Да	Да	Да	SOFc1

Маршрутизация в структуре протокола Fibre Channel

В топологии коммутируемой структуры для маршрутизации фреймов в связанной соединениями структуре используется динамический протокол маршрутизации, называемый протоколом выбора кратчайшего пути по структуре (Fabric Shortest Path First — FSPF).

Протокол FSPF в основном базируется на протоколе IP-маршрутизации выбора кратчайшего пути (Open Shortest Path First — OSPF). Протокол FSPF представляет собой протокол канального уровня, который требует, чтобы все коммутаторы обменивались друг с другом информацией канального уровня, включая информацию об операционном состоянии и метрику маршрутизации для каждого непосредственно подсоединенного канала ISL. Используя эту информацию, которая хранится в локальной базе данных, каждый коммутатор выполняет общеизвестный алгоритм Дейкстра для вычисления кратчайшего пути ко всем остальным доменам Domain_ID.

В случае, когда к некоторому домену существуют несколько маршрутов с равными оценками, выполняется функция балансирования нагрузки между этими маршрутами. В случае изменения состояния на канальном уровне, такого как изменение метрики или сбой какого-либо канала, рассылаются изменения канального уровня (link-state updates — LSU) и маршруты пересчитываются на основе полученной новой информации. В сети Fibre Channel настройкой метрики канала можно перераспределять потоки и восстанавливать маршруты.

Управление потоками в сети Fibre Channel

Одним из наиболее эффективных механизмов протокола Fibre Channel является возможность управления потоками. Управление потоками базируется на системе разрешений, которая заключается в том, что устройство или порт не могут передавать данные до тех пор, пока они не получат кредит. В протоколе Fibre Channel имеются два механизма управления потоками: *сквозной (end-to-end)* и *межбуферный (buffer-to-buffer)*.

Сквозной контроль используется для контроля скорости передачи между двумя конечными устройствами и применяется редко. Межбуферный контроль потоков происходит между всеми парами портов соседних устройств на всем протяжении конкретного маршрута по сети Fibre Channel и между всеми парами устройств конкурентной петли.

Понятие *буферных кредитов (buffer credits)* относится к количеству входных буферов, имеющихся на смежных соединенных портах. При выполнении процедуры login смежные устройства обмениваются информацией о количестве имеющихся буферных кредитов. Буферные кредиты пополняются, когда у соседнего устройства освобождается входной буфер. В этом случае генерируется 4-байтовая команда R_RDY и посылается соседнему устройству, в результате чего там появляется новый кредит. Важность межбуферного контроля потока увеличивается по мере того, как возрастает расстояние между смежными портами. По мере возрастания этого расстояния также возрастает транзитная отсрочка или задержка. Возрастание задержки увеличивает время, которое требуется для того, чтобы получить обратное сообщение R_RDY от удаленного устройства. Если кредитов недостаточно, то соседнее устройство может оказаться неспособным поддерживать скорость передачи по каналу между этими устройствами, поскольку при отсутствии буферных кредитов передача замедляется. Этот сценарий лежит в основе планового эксперимента при расширении SAN-сети Fibre Channel посредством добавления оптической сети (SONET/SDH) с целью дублирования данных в случае аварии, и, таким образом, восстановления передачи. Основным правилом в такой ситуации является то, что для поддержки 1 Гбит/с на каждых 2 км требуется один BB_Credit. Например, для поддержки линии 1 Гбит/с на оптическом канале длиной 100 км на каждом конце необходимо поддерживать 50 кредитов. Любая дополнительная задержка, вызываемая такими факторами, как преобразование данных между различными протоколами, сжатие или шифрование, требует увеличения количества кредитов. На рис. 55.9 показана модель межбуферного контроля потоков в применении к связи между станцией и дисковым накопителем в структуре.

Распределенные службы коммутируемых структур протокола Fibre Channel

Коммутируемая структура протокола Fibre Channel предоставляет ряд распределенных служб, которые облегчают управление, конфигурирование и повышают уровень безопасности в структурах протокола Fibre Channel. В настоящем разделе описаны некоторые из этих служб.

Службы каталогов

Структуры протокола Fibre Channel поддерживают распределенную службу каталогов, часто называемую *сервером имен (name server)*. Поскольку назначение адресов FC_ID в протоколе Fibre Channel осуществляется динамически, служба каталогов

помогает преобразовывать статический WWN устройства в FC_ID, который используется для маршрутизации. Когда устройство выполняет процедуру `log in` входа в структуру, оно автоматически регистрируется на *сервере имен* вместе с некоторыми своими атрибутами. Эта информация впоследствии может быть запрошена любым конечным устройством для нахождения конкретного устройства или устройств с какими-либо конкретными характеристиками.

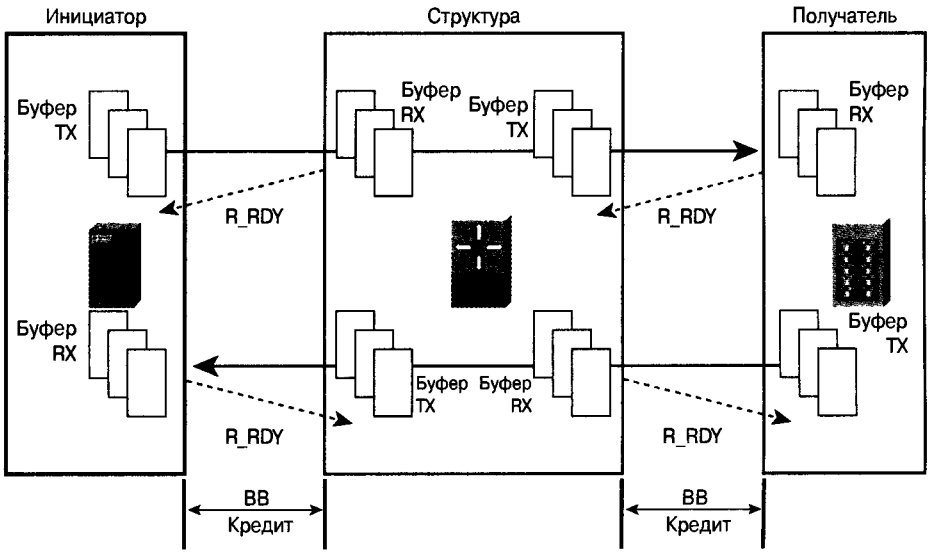


Рис. 55.9. Межбуферный контроль потоков в сети протокола Fibre Channel

Службы зон

Для того, чтобы обеспечить некоторую степень защиты в структуре протокола Fibre Channel, *службы зон (zone services)* ограничивают возможности связи между некоторыми подсоединенными устройствами. Под *зоной* в протоколе Fibre Channel понимается логическая группа устройств, которым разрешено вступать в связь и обмениваться данными. Поскольку эти устройства могут оказаться подсоединенными к разным коммутаторам, конфигурация зон распространяется на все коммутаторы структур. Зоны могут быть созданы с помощью ряда идентификаторов, включая FC_ID, индексы физических портов коммутаторов или наиболее общих адресов WWN. Существует два типа зон: *твердые или строгие зоны (hard zoning)* и *мягкие зоны или нестрогие (soft zoning)*. В строгих зонах конфигурация зоны обеспечивает фильтрацию фреймов в аппаратном обеспечении. Такой способ обеспечивает наибольшую степень безопасности. При использовании нестрогих зон фильтруются только запросы к службе каталогов, в результате чего видны только определенные устройства. Нестрогие зоны не дают полной безопасности, поскольку конечное устройство должно знать FC_ID устройства на другом конце канала, для того чтобы обойти зону и вступить в связь с конечным устройством.

Службы управления

Другой весьма полезной службой, основанной на стандарте ANSI T11 (Generic Services Standard (FC-GS и FC-GS-3), является распределенная служба управления.

Она позволяет восстанавливать в структуре атрибуты устройств и информацию о конфигурации. Эта информация может включать в себя такие атрибуты, как версия программного обеспечения, возможности устройств, логические имена устройств и IP-адреса устройств управления. Кроме того, возможен сбор информации о подсоединенных портах и соседних устройствах. Хотя эта информация весьма полезна для целей управления, многие производители не торопятся использовать эту возможность. Однако все большее количество производителей планируют такую поддержку для следующей версии, получившей название FC-GS-4, которая позволит восстанавливать из структур еще больший объем информации о конфигурации.

Службы уведомления об изменениях в состоянии

В большинстве традиционных сетей передачи данных информация о сбоях в сети передавалась другим сетевым элементам, таким как коммутаторы и маршрутизаторы. Однако протокол Fibre Channel расширяет эту службу до конечных устройств. Используя службу уведомления об изменениях в состоянии сети (State Change Notifcation Service), а позднее зарегистрированную службу уведомления об изменениях в состоянии сети (Registered State Change Notifcation Service — RSCN), конечные устройства могут зарегистрироваться для получения уведомлений о событиях в структуре. В случае, если в сети происходит событие, случайное или намеренно созданное, генерируются сообщения службы RSCN для уведомления о нем других устройств сети. Используя службу RSCN, устройства могут реагировать на сбои в сети значительно быстрее, чем если бы они ожидали истечения времени таймеров.

Протокол iSCSI

Протокол iSCSI позволяет создать SAN-сеть, в которой данные SCSI передаются поверх протокола TCP/IP. Протокол iSCSI может использовать любой транспорт IP, однако в первую очередь предназначен для SAN-сетей, основанных на технологии Ethernet. Используя протокол iSCSI, SAN-проектировщики могут строить экономически более эффективные SAN-сети, особенно для соединения серверов среднего уровня с хранилищами информации.

Коммуникационная модель протокола iSCSI

Протокол iSCSI использует стек протоколов TCP/IP для установки сеансов аналогично тому, как это делается в протоколе Fibre Channel. Однако в отличие от Fibre Channel узлам протокола iSCSI для установки связи не требуется выполнять процедуру `log in` для входа в Ethernet-структуру. Сеансы связи устанавливаются между инициаторами iSCSI (станциями или узлами) и целевыми устройствами iSCSI и могут состоять из нескольких соединений протокола TCP/IP. Однако каждый конкретный обмен SCSI (команда) должен быть выполнен по одному соединению TCP. Для всех iSCSI-соединений протокол iSCSI использует общеизвестный номер порта TCP/3260. Целевое устройство iSCSI может быть шлюзом iSCSI/Fibre Channel или реальным набором дисковых или ленточных накопителей с функциями iSCSI. На рис. 55.10 показана коммуникационная модель протокола iSCSI.

Перед передачей каких-либо команд SCSI инициатор iSCSI должен выполнить процедуру `log in` для входа в какое-либо целевое устройство iSCSI. Во время этой

login-фазы обнаруживаются целевые устройства iSCSI и преобразуются в блоковые устройства в рабочей станции. На рис. 55.11 проиллюстрировано выполнение процедуры **login**.

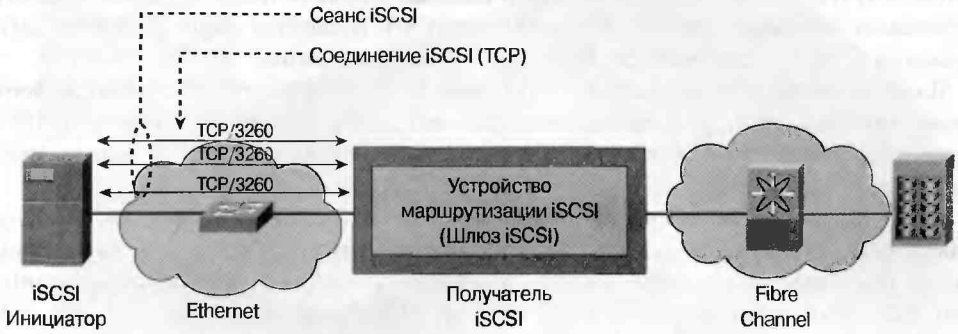


Рис. 55.10. Коммуникационная модель протокола iSCSI

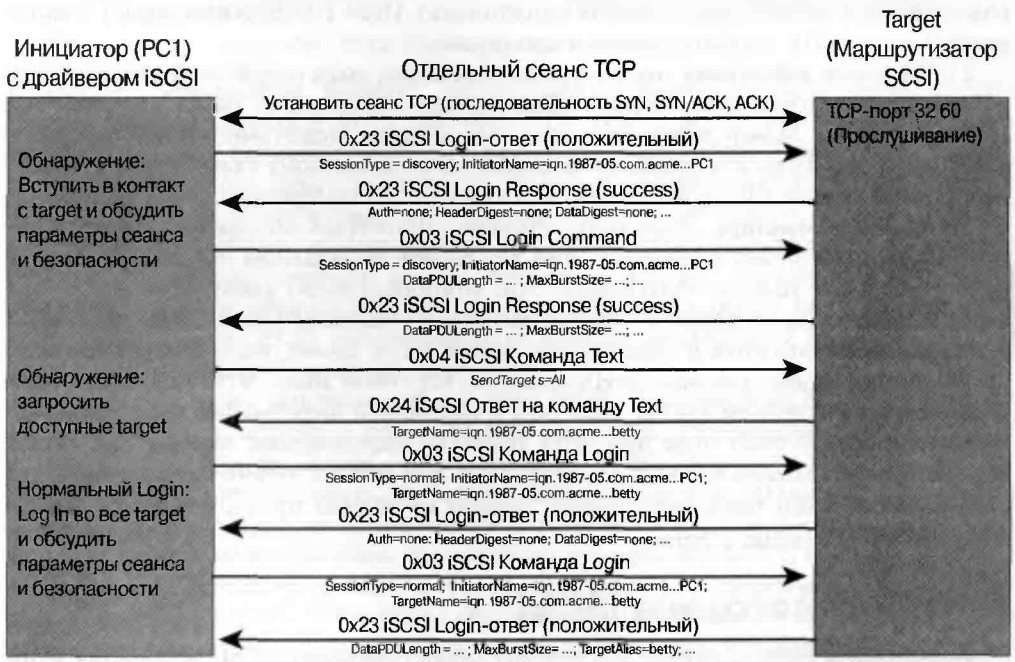


*Рис. 55.11. Выполнение процедуры **login** протокола iSCSI*

Формат фрейма протокола iSCSI

Протокол iSCSI использует TCP в качестве транспортного протокола. Однако для управления сеансом используется специфический заголовок протокола iSCSI. На рис. 55.12 показан заголовок протокола iSCSI и различные его компоненты. Ниже приводится более подробное описание отдельных полей.

Opcode Поле кода операции Opcode (1 байт) указывает тип модуля PDU iSCSI, который инкапсулирует заголовок. Имеется два типа кодов операции: код инициатора и код целевого устройства. Коды операции инициатора находятся в модулях PDU, посылаемых инициатором (PDU запроса), а коды операции целевых устройств находятся в модулях PDU, посылаемых целевыми устройствами (ответные PDU). Процедура `login` протокола iSCSI и команда SCSI представляют собой два примера кодов операции.

Поля конкретного кода операции Это поле (3 байта) имеет различные значения в зависимости от типа кода операции. Например, код операции для процедуры iSCSI `login` использует эту область для хранения номера версии iSCSI и управляющих флагов процедуры `login`.

AHS Len Это поле указывает длину всех дополнительных сегментов заголовка (additional header segments — AHS), выраженную в 4-байтовых словах, включая заполнитель (padding), если таковой имеется. Поле общей длины (TotalAHSLength) длиной один байт используется только в тех модулях PDU, которые имеют сегменты AHS. Во всех остальных PDU это поле равно нулю.

Длина поля данных (Data Field) В этом поле содержится значение длины сегмента полезной нагрузки в байтах (включая заполнитель). Поле DataSegmentLength (3 байта) равно 0 если в PDU сегмент данных отсутствует.

LUN или поля конкретных кодов операций Некоторые коды операций функционируют на конкретных логических блоках. Поле номера логического блока (Logical Unit Number — LUN) задает логический блок, на котором будет выполняться операция с данным кодом. Если код операции не относится к логическому блоку, то это поле игнорируется или может быть использовано определяемым конкретным кодом операции.

Тег задачи инициатора. Инициатор назначает некоторый тег каждой задаче iSCSI. До тех пор, пока задача существует, этот тег должен уникальным образом идентифицировать задачу в течение всего сеанса. Этот компонент имеет длину 4 байта.

AHS Поле сегмента дополнительного заголовка (Additional Header Segment — AHS) не является обязательным и используется только в том случае, когда требуется дополнительный заголовок команды. AHS представляет собой мини-заголовок, состоящий из значения собственной длины, кода типа и командной информации.

Поле данных В этом поле находятся реальные передаваемые данные. Ими могут быть данные протокола SCSI из команды `read` или данные аутентификации команде `login`. Длина этого поля непостоянна, однако не должна превышать длину максимального MTU фрейма Ethernet.

Службы протокола iSCSI

В настоящем разделе описан ряд сетевых служб протокола iSCSI, реализация которых являются частью общей задачи создания SAN-сети протокола iSCSI.

Службы каталогов

Инициаторы протокола iSCSI могут использовать различные способы для обнаружения целевых устройств протокола iSCSI. Большинство современных реализаций просто используют статическое преобразование в IP-адрес iSCSI-сервера, который осуществляет хостинг ряда целевых устройств. Однако существуют два механизма, которые могут находить целевые устройства протокола iSCSI автоматически. Они определены как проекты IETF.

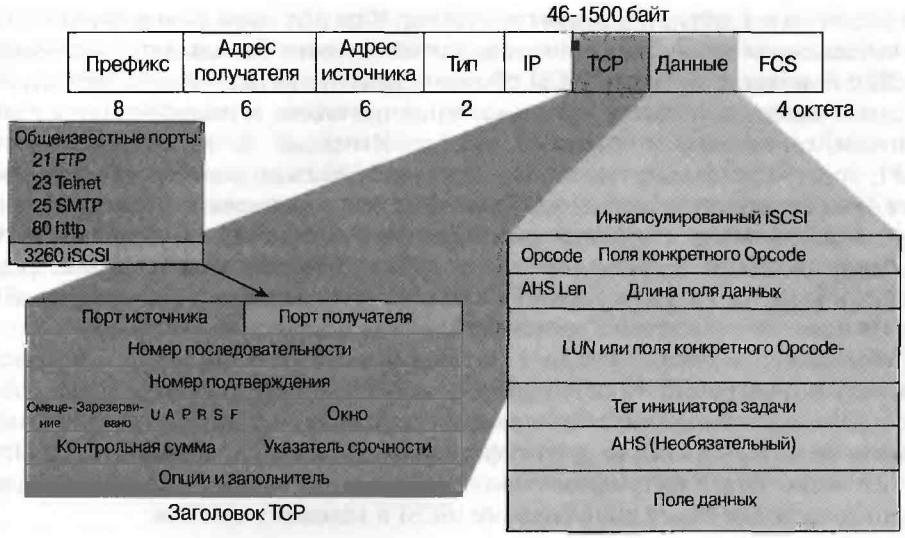


Рис. 55.12. Формат фрейма протокола iSCSI

Первым механизмом является использование протокола нахождения службы (Service Location Protocol — SLP). Протокол SLP требует, чтобы серверы iSCSI регистрировали все свои целевые устройства с использованием набора адресов URL службы, по одному на каждый адрес, по которому можно получить доступ к целевому устройству. Инициаторы обнаруживают эти целевые устройства используя служебные запросы SLP, которые обычно являются собой многоадресатными. Серверы iSCSI, которые слышат SLP-запросы, отвечают на них списком доступных целевых устройств. Агент централизованного каталога (directory agent — DA) также может использоваться для того, чтобы серверы iSCSI зарегистрировали целевые устройства, а инициаторы iSCSI получили информацию о целевых устройствах.

Второй механизм, используемый для того, чтобы инициатор iSCSI мог обнаружить целевые устройств, состоит в использовании протокола, называемого Internet-службой хранения имен (Internet Storage Name Service — iSNS). Используя iSNS, инициаторы протокола iSCSI могут находить друг друга с помощью сервера каталога. Протокол iSNS облегчает конфигурирование и управление устройствами iSCSI в IP-сети путем предоставления набора служб каталогов, похожего на аналогичный набор, доступный в сетях Fibre Channel. Используя протокол iSNS, устройства iSCSI автоматически регистрируют свои атрибуты на сервере iSNS. Таким образом, сервер iSNS служит консолидированной конфигурационной точкой, при посредстве которой станции управления могут конфигурировать и управлять всей сетью хранения iSCSI. Кроме того, сервер iSNS может посылать уведомления об устройствах iSCSI или о событиях в сети заинтересованным устройствам, или тем устройствам, которые затронуты этими событиями.

Службы аутентификации

Одним из достоинств протокола iSCSI является то, что в нем службы аутентификации включены в процесс выполнения процедуры `login`. Когда узел iSCSI выполняет процедуру `log in` с целевым устройством iSCSI, (которым обычно является шлюз iSCSI), может быть выполнена аутентификация с инициатором iSCSI, до того как

будет предоставлен доступ к целевому устройству. Хотя для такой аутентификации могут быть использованы несколько протоколов, для обеспечения безопасного соединения узла iSCSI с целевым устройством iSCSI обычно используются два основных метода.

Первый метод заключается в использовании протокола аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol — CHAP), требуемого стандартом iSCSI, и является типовым механизмом, используемым в IP-соединениях удаленного доступа. При использовании протокола CHAP целевые устройств могут запросить идентификационные данные у инициатора iSCSI и наоборот. Удобной реализацией этого метода является использование сервера RADIUS в качестве централизованного средства аутентификации для шлюзов iSCSI. RADIUS является стандартным протоколом, используемым для этих целей.

Вторым методом аутентификации является использование протокола безопасного удаленного пароля (Secure Remote Password — SRP). SRP представляет собой протокол обмена ключами и основанной на пароле аутентификации, обеспечивающий аутентификацию (возможна взаимная аутентификация) и обсуждение ключа сеанса. Протокол SRP также может быть использован для открытия безопасного аутентифицированного соединения между инициаторами iSCSI и целевых устройств.

Службы загрузки протокола iSCSI

Многие пользователи, не имеющие жестких дисков, конфигурируются для загрузки с удаленных устройств SCSI. Такая возможность существует также и для пользователей, не имеющих жестких дисков и выполняющих загрузку вне устройств протокола Fibre Channel. Такие бездисковые устройства имеют малый вес, компактны, обладают функциями энергосбережения и становятся все более популярными при использовании в различных средах. Используя вышеупомянутые службы удаленной загрузки можно быстро вставить новый процессор CPU для увеличения мощности или для замены вышедшего из строя CPU. Эти новые устройства заменяют уже существующие и начинают работать сразу после перезагрузки, используя прежнего образа.

Рабочая группа IP-хранения IETF внесла предложение о поддержке удаленной iSCSI-загрузки под названием *draft-ietf-ips-iscsi-boot*. В этом проекте описан механизм, позволяющий пользователям выполнить загрузку самостоятельно, используя протокол iSCSI. Целью этого стандарта является предоставление пользователям протокола iSCSI, осуществляющим перезагрузку, получать информацию для открытия сеанса iSCSI с загрузочного сервера iSCSI.

Резюме

Настоящая глава представляет собой краткое описание технологии хранения данных с использованием сетей. Сети SAN быстро становятся критически важными компонентами инфраструктуры сетевых сред современных предприятий. Постоянный рост требований к организации хранения данных быстро вызывает повышение соответствующих требований к сетям хранения. В главе представлен краткий обзор движущих мотивов развития SAN-технологий и описаны соответствующие решения. Основной целью применения SAN-сетей является получение доступа к информационным хранилищам предприятия и их использование. Эти сети также помогают решать многие задачи, связанные с хранением информации, путем реализации более гибкого и менее подверженного сбоям способа ее сохранения.

В главе описана типовая SAN-архитектура, включающая в себя такие компоненты SAN-сети, как станции, дисковые и ленточные накопители, а также разнообразные сетевые устройства. Кроме того, представлена функциональная модель, в которой узлы SAN-сети выступают в качестве инициаторов или целевых устройств. Эти роли непосредственно вытекают из протокола SCSI, являющегося основным протоколом, данные которого передаются по SAN-сетям.

Более подробно в главе представлен протокол Fibre Channel. Рассмотрены многие его структурные атрибуты, такие как схемы адресации, протоколы маршрутизации, управление потоками, типы соединений, сетевые топологии и распределенные службы.

В заключение приведено краткое введение в работу протокола iSCSI. Этот протокол вызывает огромный интерес профессиональных IT-организаций, поскольку он предоставляет способ использовать существующие Ethernet-инфраструктуры для реализации сети SAN. В главе представлен обзор протокола iSCSI, который описывается как альтернативный транспортный протокол для соединений протокола SCSI. Также подробно представлены архитектурные компоненты протокола iSCSI, такие как его коммуникационная модель, формат фрейма и ассоциированные сетевые службы.

Контрольные вопросы

1. Что представляет собой сеть зон хранения (SAN)?
2. Какие два основных транспортных протокола используются в SAN-сетях?
3. Данные какого коммуникационного протокола обычно передаются по сетям SAN?
4. Каковы две основных роли устройств протокола SCSI?
5. Какие три протокола верхнего уровня кроме SCSI были адаптированы для передачи их данных по протоколу Fibre Channel?
6. Какой управляющий орган руководит разработкой проектов и стандартов протокола Fibre Channel?
7. Когда был принят первый стандарт протокола Fibre Channel и как он назывался?
8. Какой уровень протокола Fibre Channel отвечает за установку связи между двумя портами в сети SAN?
9. Каковы три основных топологии сети Fibre Channel?
10. Сколько устройств может поддерживать топология конкурентной петли?
11. В чем состоит разница между топологиями частной конкурентной петли и публичной конкурентной петли?
12. Что понимается под обозначением "B_Port"?
13. Как называется основной протокол маршрутизации протокола Fibre Channel и какую часть идентификатора FC_ID он использует для принятия решений о маршрутизации?
14. Что представляет собой IDLE протокола Fibre Channel и для чего он используется?
15. Какой класс обслуживания протокола Fibre Channel не обеспечивает подтверждения доставки?
16. Каково основное правило определения количества буферных кредитов, требуемых для поддержки скорости передачи 1 Гбит/с по каналу протокола Fibre Channel?

17. Какие зоны называются "мягкими"?
18. Верно ли утверждение: "индивидуальный iSCSI-обмен может происходить по нескольким TCP-соединениям"?
19. Какой стандартный номер порта используется для протокола iSCSI?
20. Какие два механизма используются для аутентификации инициатора протокола iSCSI?

Дополнительные источники

Книги

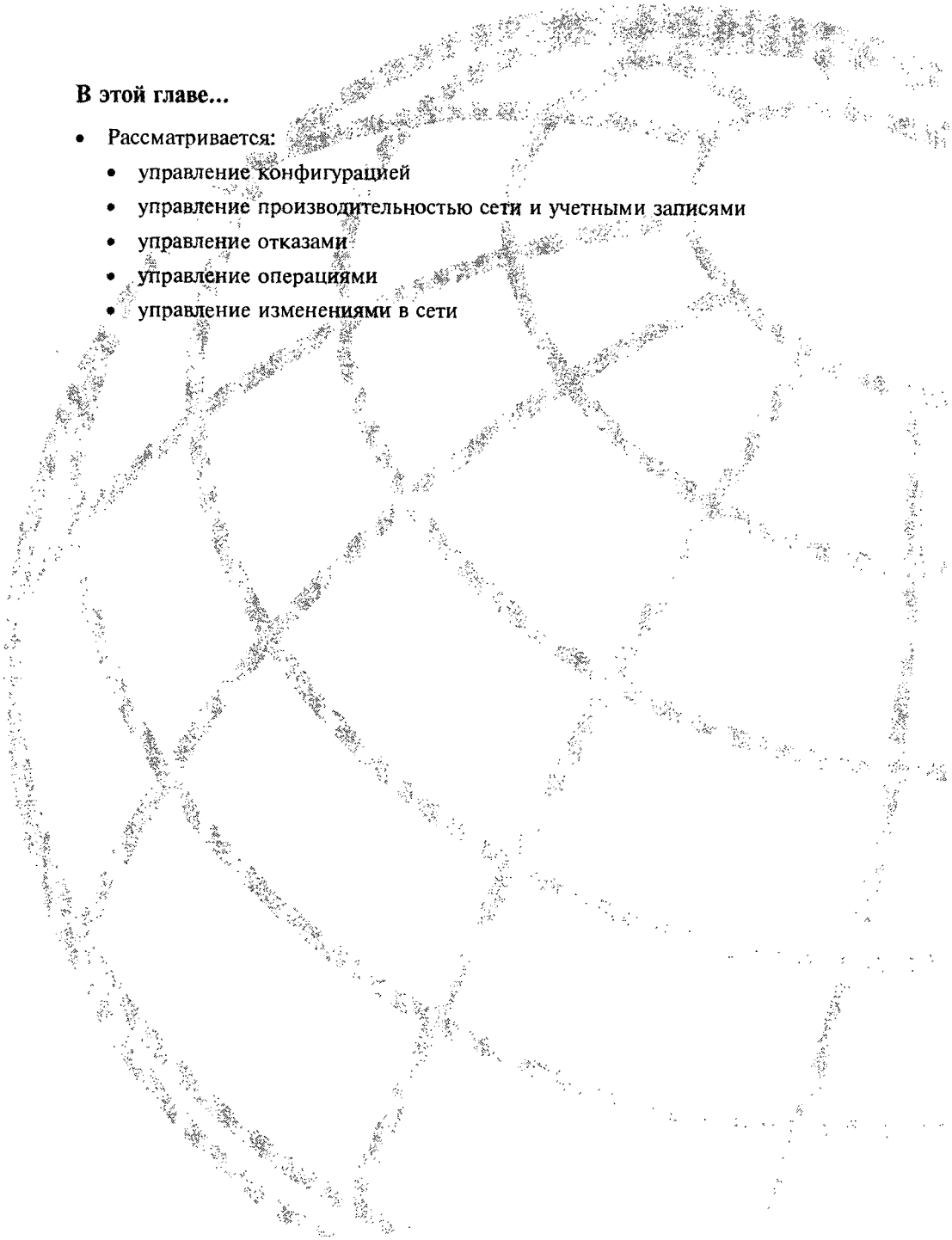
- Kembel, Robert W. Fibre Channel: *A Comprehensive Introduction*. Tucson: Northwest Learning Associates, Inc., 2000.

URL-адреса

- www..brealliance.org
- www.ietf.org/html.charters/ips-charter.html
- www.searchstorage.com
- www.snia.org

В этой главе...

- Рассматривается:
  - управление конфигурацией
  - управление производительностью сети и учетными записями
  - управление отказами
  - управление операциями
  - управление изменениями в сети



Глава 56

Управление сетями IBM

Введение

Системой управления сетями IBM называют любую архитектуру для управления сетями, использующую системную сетевую архитектуру IBM (Systems Network Architecture — SNA) или усовершенствованный протокол одноранговых сетей (Advanced Peer-to-Peer Networking — APPN). Управление сетями IBM является частью открытой сетевой архитектуры IBM (Open Network Architecture — ONA) и выполняется централизованно с использованием таких управляющих платформ, как NetView и другие. Управление сетями IBM включает в себя пять функций, аналогичных функциям сетевого управления, определенным в эталонной модели OSI. В настоящей главе описываются функциональные области управления сетями IBM, архитектура ONA системы управления сетью и управляющие платформы. На рис. 56.1 показана типичная управляемая сеть IBM.

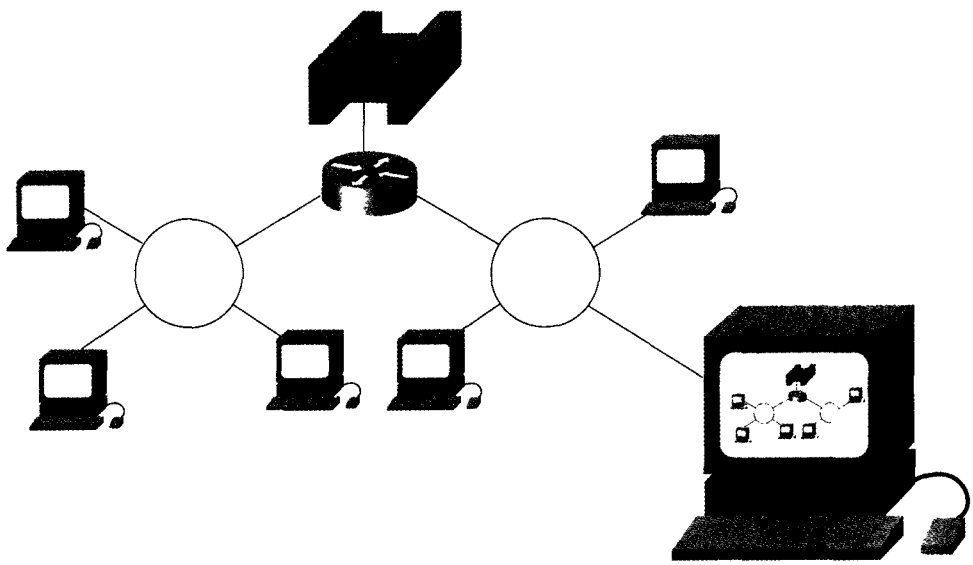


Рис. 56.1. Система сетевого управления IBM управляет сетями SNA и APPN

Функциональные области управления сетями IBM

Сетевое управление IBM включает в себя следующие пять функций: управление конфигурацией, управление производительностью и учетными записями, управление отказами, управление операциями и управление изменениями.

Управление конфигурацией IBM

Система управления конфигурацией IBM контролирует информацию, описывающую физические и логические характеристики сетевых ресурсов, а также взаимосвязь между этими ресурсами. Центральная система управления хранит данные в базах управления конфигурацией. Эти данные могут включать в себя информацию о версиях системного программного обеспечения или микрокода, серийные номера устройств и программного обеспечения, физическое расположение сетевых устройств, имена, адреса, телефоны и другую информацию о пользователях. Вполне естественно, что управление конфигурацией IBM практически соответствует управлению конфигурацией эталонной модели OSI.

Функции управления конфигурацией осуществляют ведение реестра сетевых ресурсов и отображение изменений конфигурации сети в базах данных управления конфигурацией. Система управления конфигурацией также предоставляет информацию системам, управляющим отказами и изменениями. В системах управления отказами эта информация используется для сравнения версий и обнаружения, идентификации и проверки параметров сетевых ресурсов. В системах управления изменениями такая информация используется для анализа влияния изменений в сети на ее работу и для планирования изменений на время минимальной загрузки сети.

Управление производительностью и учетными записями

Системы управления производительностью и учетными записями IBM предоставляют информацию о производительности сетевых ресурсов. В число функций управления производительностью и учетными записями входят мониторинг времени отклика систем, определение доступности ресурсов, измерение интенсивности использования ресурсов, а также настройка, наблюдение и контроль производительности сети. Информация, полученная при помощи функций управления производительностью и учетными записями, может быть полезна для ответа на вопрос: достигаются ли требуемые показатели производительности и нужно ли запускать процедуру поиска отказов, исходя из зарегистрированных параметров производительности. Функции систем управления производительностью и учетными записями IBM подобны аналогичным функциям OSI.

Управление отказами

Система управления отказами в сети IBM аналогична системе управления сбоями эталонной модели OSI в том, что рассматривает условия возникновения ошибок,

которые приводят к тому, что пользователи теряют полный доступ к функциям сетевого ресурса. Управление отказами включает в себя пять этапов: выявление отказа, диагностика отказа, блокировка отказа и восстановление работы, устранение отказа, поиск причин и контроль возникновения новых отказов.

Выявление отказа заключается в обнаружении отказа и выполнении действий по его начальной диагностике, таких как изоляция отказавшего участка в виде особой подсистемы. На этапе диагностики отказа определяется точная причина проблемы и действия, которые необходимо выполнить для ее устранения. Блокировка отказа и восстановление работы включает в себя попытки частично или полностью блокировать отказавший участок. Однако это лишь временное решение до тех пор, пока проблема не будет устранена полностью. Устранение отказа означает действия, направленные на полное решение проблемы. К нему обычно приступают по окончании диагностики отказа и для этого выполняются корректирующие действия, такие как замена поврежденного оборудования или программного обеспечения. Затем производится поиск причин и контроль возникновения новых отказов. Необходимая информация, характеризующая отказ, хранится в базе данных отказов.

Управление операциями

Управление операциями IBM заключается в управлении распределенными ресурсами сети с центрального узла с использованием двух наборов функций: служб управления и служб общих операций. Службы управления обеспечивают возможность централизованного управления удаленными ресурсами с использованием таких функций, как активация и деактивация ресурса, отмена команды и запуск по таймеру. Службы управления операциями могут запускаться автоматически в ответ на уведомление об определенных системных проблемах.

Службы общих операций обеспечивают управление ресурсами, не управляемыми явным образом другими системами управления. Для этого используется специализированный обмен данными посредством специальных приложений. В число служб общих операций входят две важные службы: команда **execute** и служба управления ресурсами. Команда **execute** является стандартным средством выполнения удаленных команд. Служба управления ресурсами обеспечивает контекстно-независимую передачу информации.

Управление изменениями

Система управления изменениями IBM наблюдает за изменениями в сети и поддерживает файлы регистрации изменений в удаленных узлах. Сетевые изменения происходят в основном по двум причинам: изменение требований пользователей и необходимость обойти возникшую проблему. Изменения требований пользователей связаны с обновлением программного обеспечения и аппаратных средств, с появлением новых приложений и служб, и с другими изменениями в сети, вызванными постоянно изменяющимися потребностями пользователей. Обход проблемы необходим для продолжения работы, несмотря на непредвиденные изменения, вызванные сбоем программного обеспечения, аппаратных средств или других сетевых компонентов. Система управления изменениями пытается свести к минимуму возникающие проблемы, выполняя регулярные изменения и внося изменения в файлы, в которых регистрируются сетевые изменения. Система управления изменениями IBM аналогична системе управления учетными записями OSI.

Архитектуры сетевого управления IBM

Наиболее известными архитектурами сетевого управления IBM являются открытая сетевая архитектура и SystemView.

Открытая сетевая архитектура

Открытая сетевая архитектура (Open-Network Architecture — ONA) представляет собой обобщенную архитектуру сетевого управления, которая определяет четыре ключевых элемента управления: фокусную точку, точку сбора, точку входа и точку доступа к службе.

Фокусная точка (focal point) представляет собой объект управления, поддерживающий операции централизованного управления сетью. Она реагирует на предупреждения конечных станций, управляет базами данных и предоставляет пользовательский интерфейс для оператора по управлению сетью. Существует три вида фокусных точек: первичные, вторичные и вложенные. Первичные фокусные точки выполняют все функции фокусных точек. Вторичные фокусные точки служат резервными для первичных фокусных точек и используются в том случае, если первичные выходят из строя. Вложенные фокусные точки обеспечивают распределенное управление в больших сетях и предназначены для передачи критически важной информации глобальным фокусным точкам.

Точки сбора (collection point) передают информацию из автономных подсетей SNA в фокусные точки. Точки сбора обычно используются для передачи данных из одноранговых сетей IBM в иерархические сети ONA.

Точка входа (entry point) представляет собой SNA-устройство, реализующее архитектуру ONA для себя и для других устройств. Точками входа могут быть большинство стандартных SNA-устройств.

Точка доступа к службе (service point) представляет собой систему, которая обеспечивает доступ к архитектуре ONA для устройств, несовместимых с SNA, и фактически является шлюзом архитектуры ONA. Точки доступа к службе могут посылать управляющую информацию о системах, несовместимых с SNA, в фокусные точки, принимать команды от фокусных точек, преобразовывать команды в формат, приемлемый для устройств, несовместимых с SNA, и передавать команды таким устройствам для выполнения.

Взаимосвязь между различными объектами управления ONA показана на рис. 56.2.

SystemView

SystemView представляет собой проект создания управляющих приложений, способных управлять неоднородными информационными системами. SystemView описывает взаимодействие приложений, управляющих разнородными сетями, с другими системами управления. Этот проект является официальной стратегией системного управления архитектуры системных приложений IBM (IBM Systems Application Architecture).

Платформы управления сетями IBM

Существует несколько платформ для управления сетями IBM. В их число входят NetView, LAN Network Manager (LNM), и простой протокол управления сетью (Simple Network Management Protocol — SNMP).

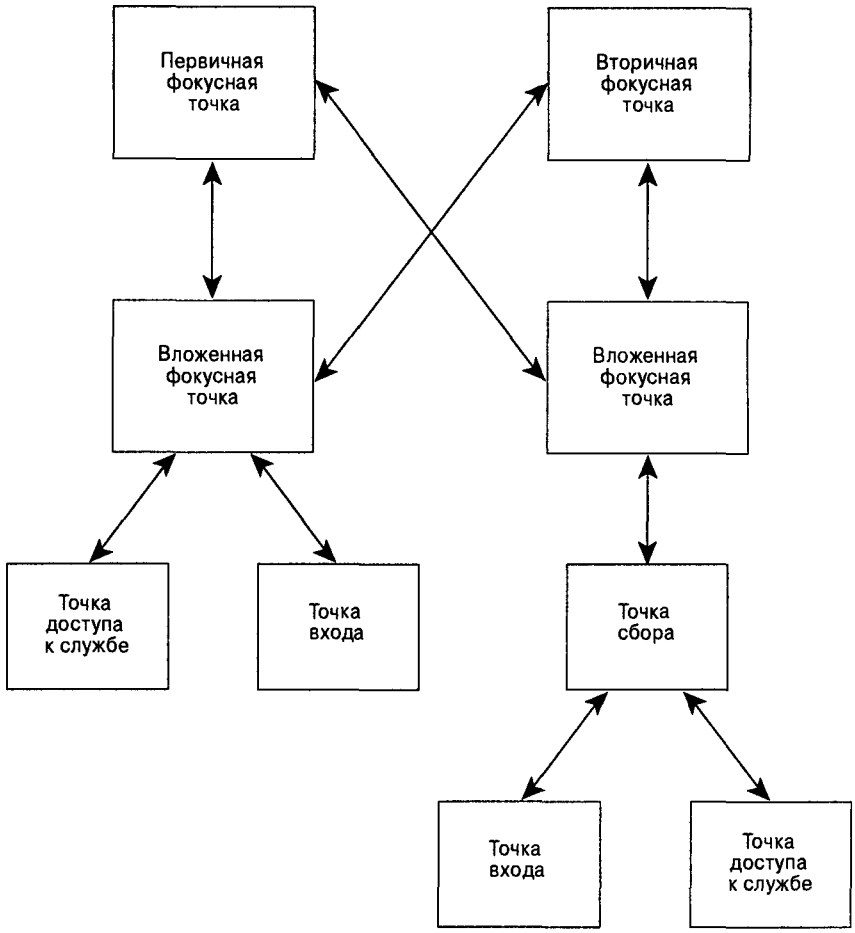


Рис. 56.2. Четыре типа фокусных точек и их взаимосвязь в среде архитектуры ONA

NetView

NetView представляет собой единую промышленную платформу управления сетями IBM, предоставляющую централизованные службы управления сетями SNA. Она используется в мэйнфреймах IBM и является составной частью архитектуры ONA. В состав NetView входят средство управления, монитор аппаратных средств, монитор сеансов, монитор состояния, монитор производительности, менеджер распространения, а также справочная система.

Средство управления осуществляет управление сетью при помощи основных операторов и команд файлового доступа к приложениям VTAM (Virtual Telecommunications Access Method), контроллерам, операционным системам и устройствам NetView/PC (интерфейс между устройствами NetView и устройствами, не поддерживающими SNA). Монитор аппаратных средств осуществляет наблюдение за сетью и автоматически информирует сетевого оператора об ошибках оборудования. Монитор сеансов действует как монитор производительности VTAM, выявляет программные

ошибки и ошибки управления конфигурацией. Справочная система предоставляет помощь пользователям NetView и состоит из функции просмотра, справочной панели и библиотеки типичных ситуаций, возникающих в сети. Монитор состояния собирает и предоставляет информацию о состоянии сети. Монитор производительности следит за производительностью препроцессоров (front-end processors — FEP), программы, контролирующей сеть (Network Control Program — NCP), и других смежных ресурсов. Менеджер распределения планирует, распределяет и направляет данные, программы и микрокоманды в средах SNA.

LAN Network Manager

Менеджер локальной сети (LAN Network Manager — LNM) представляет собой приложение для управления локальными сетями IBM Token Ring из центрального узла поддержки. LNM представляет собой продукт, основанный на OS/2 Extended Edition, взаимодействующий с IBM NetView (которому сообщается о таких действиях LNM, как аварийные предупреждения) и с другим управляющим программным обеспечением IBM.

Протокол SNMP

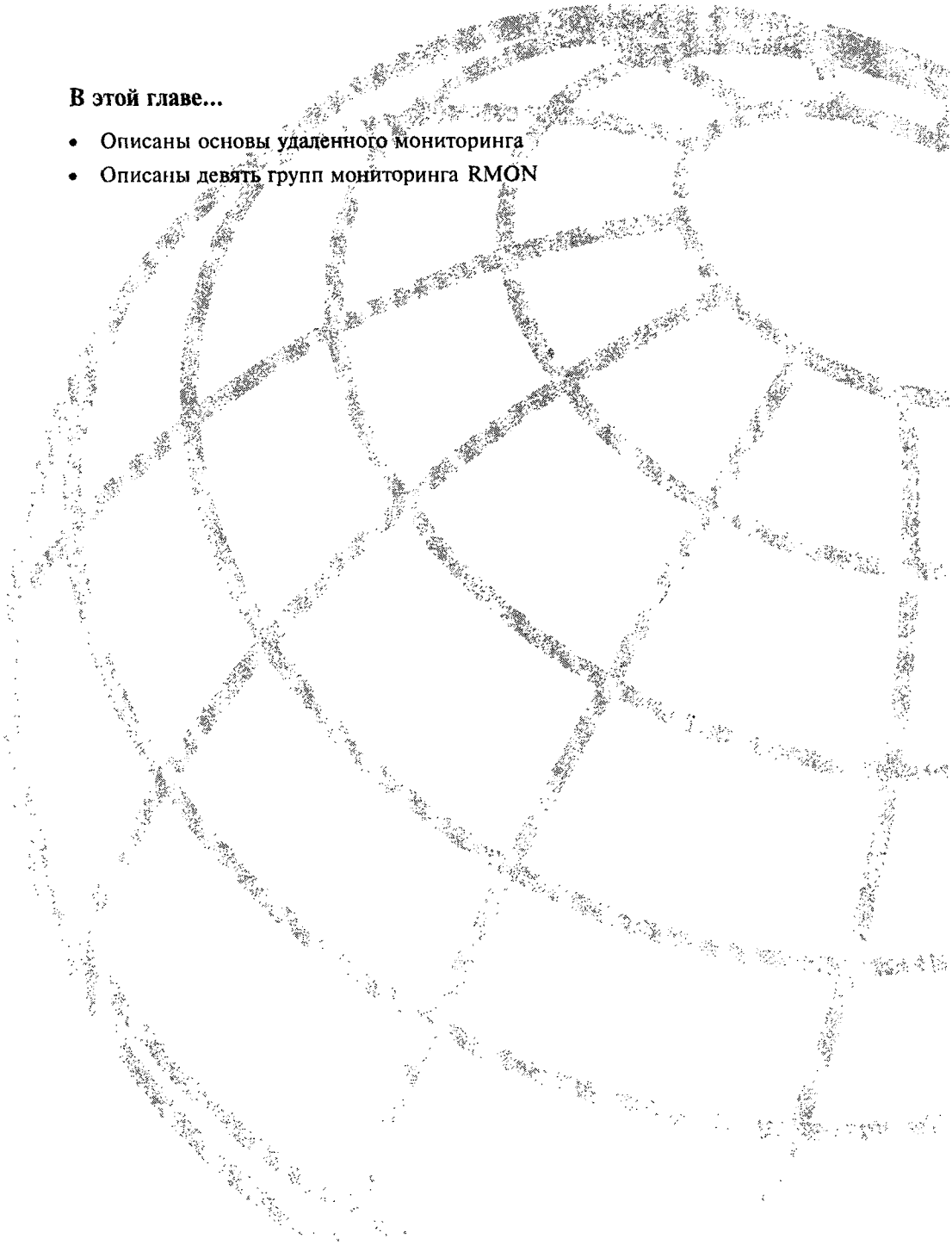
Управление сетями IBM может быть реализовано с помощью простого протокола управления сетями (Simple Network Management Protocol — SNMP). Более подробное описание этого протокола приведено в главе 58, "Протокол SNMP".

Контрольные вопросы

1. Каковы пять этапов устранения сетевых отказов?
2. Как работает средство управления программы NetView?
3. Что требуется для активизации и деактивизации ресурсов, отмены команд и синхронизации удаленных систем?

В этой главе...

- Описаны основы удаленного мониторинга
- Описаны девять групп мониторинга RMON



Глава 57

Удаленный мониторинг

Введение

Удаленный мониторинг (Remote Monitoring — RMON) представляет собой спецификацию стандартных средств мониторинга, позволяющую различным сетевым контрольным устройствам и консольным системам обмениваться данными мониторинга сети. Благодаря RMON у сетевых администраторов появляется больше свободы в выборе датчиков и консолей для сетевого мониторинга с функциями, отвечающими особенностям организации конкретной сети. В настоящей главе приводится краткий обзор спецификации RMON и уделяется особое внимание группам RMON.

Спецификация RMON определяет набор статистических характеристик и функций, которые могут распространяться между администраторами RMON-совместимых консолей и сетевыми датчиками. В целом RMON обеспечивает администраторов сети комплексной информацией по диагностике неисправностей, планированию и настройке производительности сети.

RMON был сформулирован сообществом пользователей с помощью IETF. В 1992 г. он был предложен как стандарт RFC 1271 (для Ethernet). В 1995 г. RMON стал временным стандартом RFC 1757, более эффективным, чем устаревший RFC 1271.

На рис. 57.1 показан датчик RMON, способный осуществлять мониторинг сегмента сети Ethernet и передавать статистическую информацию назад на RMON-совместимую консоль.

Группы RMON

RMON поставляет информацию в девять групп элементов мониторинга RMON, каждая из которых поддерживает отдельный набор данных, удовлетворяющий общим требованиям мониторинга сети. Группы не являются обязательными, так что производителям нет необходимости поддерживать их все в рамках базы управляющей информации (Management Information Base — MIB). Некоторые группы RMON для правильного функционирования требуют поддержки других групп RMON. В табл. 57.1 описаны девять групп мониторинга, определенных в RFC 1757 Ethernet RMON MIB.

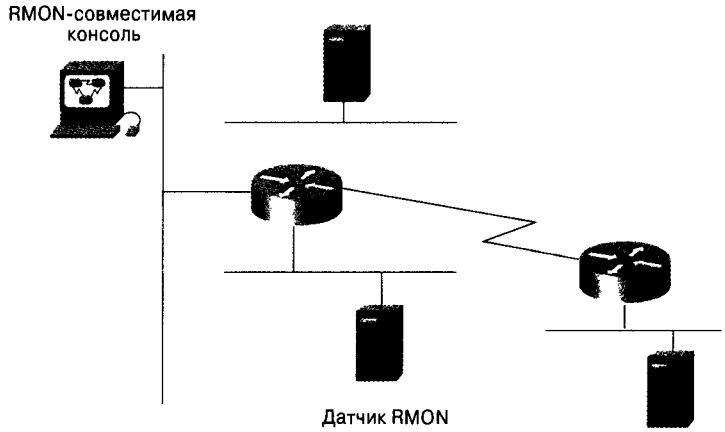


Рис. 57.1. Датчик RMON посылает статистическую информацию на RMON-консоль

Таблица 57.1. Группы мониторинга RMON

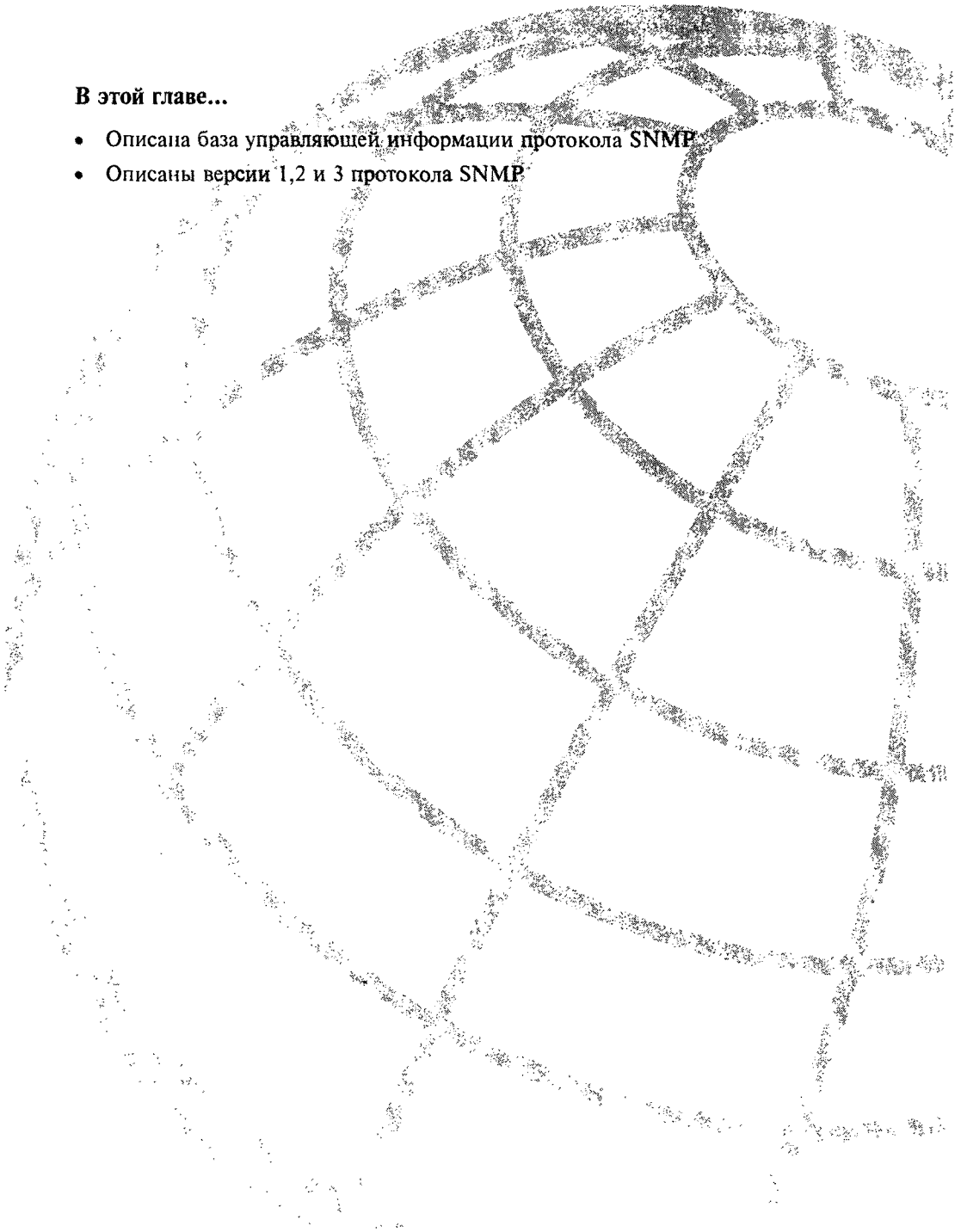
Группа RMON	Функция	Элементы
Statistics	Содержит статистические данные, измеренные датчиком на каждом интерфейсе устройства, для которого проводится мониторинг	Отброшенные пакеты, отправленные пакеты, отправленные байты (октеты), широковещательные пакеты, многоадресные пакеты, ошибки СКС, карликовые (runts) и гигантские (giants) пакеты, фрагменты, "мусор", коллизии и счетчики пакетов размером 64–128, 128–256, 256–512, 512–1024 и 1024–1518 байтов
History	Периодическая запись статистических выборок из сети и хранение их для дальнейшего использования	Период выборки, количество выборок, выбираемые элементы
Alarm	Периодическое извлечение статистических выборок из переменных в датчике и сравнение их с заранее выбранными пороговыми значениями. Если наблюдаемые значения переменных выходят за границы пороговых, генерируется событие	Включает таблицу предупреждений и требует наличия группы событий. Тип предупреждения, интервал, нижний порог, верхний порог
Host	Содержит статистические данные, связанные с каждым узлом, обнаруженном в сети	Адрес узла, передаваемые и получаемые пакеты и байты, а также широковещательные, многоадресные пакеты и пакеты ошибок
HostTopN	Составляет таблицы, описывающие узлы, которые возглавляют список, упорядоченный по одному из их статистических параметров за период времени, определяемый управляющей станцией. Таким образом, эти статистические данные являются нормированными	Статистические данные, узлы, время начала и конца выборки, база нормирования, продолжительность

Окончание табл. 57.1

Группа RMON	Функция	Элементы
Matrix	Хранит статистические данные о диалогах между наборами двух адресов. Как только устройство выявляет новый диалог, в его таблице создается новая запись	Адреса пары источник-приемник, а также пакеты, байты и ошибки для каждой пары
Filters	Разрешает приводить пакеты в соответствие с выражениями фильтров. Такие пакеты формируют потоки данных, которые могут захватываться и генерировать события	Вид битового фильтра (маскированный или не маскированный), выражение фильтра (битовый уровень), условное аыражение (и, или, нет) для других фильтров
Packet Capture	Позволяет захватывать пакеты после их прохождения по каналу	Размер буфера для захваченных пакетов, полный статус (предупреждение), число захваченных пакетов
Events	Управление генерацией и оповещением о событиях от данного устройства	Тип события, описение, время последней отправки события

Контрольные вопросы

1. Какова функция группы Matrix RMON?
2. Что такое RMON?
3. Компонентами какой группы RMON являются многоадресатные пакеты, ошибки CRC, карликовые и гигантские пакеты, фрагменты и "мусор"?



В этой главе...

- Описана база управляющей информации протокола SNMP
- Описаны версии 1,2 и 3 протокола SNMP

Глава 58

Протокол SNMP

Введение

Простой протокол управления сетью (Simple Network Management Protocol SNMP) представляет собой протокол уровня приложений, который упрощает обмен управляющей информацией между сетевыми устройствами. Протокол SNMP входит в стек протоколов TCP/IP и определен в нескольких RFC, являющихся частью стандартов IETF (Internet Engineering Task Force — IETF) .Он позволяет сетевым администраторам осуществлять мониторинг сети, конфигурировать ее, обнаруживать и решать возникающие проблемы, а также планировать развитие сети.

В документах RFC, определяющих протокол SNMP, ясно прослеживается намерение сохранять его, насколько возможно, простым и относительно недорогим при его реализации в минимальной, но достаточной форме. По этому в протоколе SNMP отсутствуют сложные структуры баз данных и сложные операции.

Были разработаны несколько версий этого протокола. Некоторые из них стали промышленными стандартами: протокол SNMP версии 1 (SNMPv1), основанный на сообществах (community-based) протокол SNMP версии 2 (SNMPv2c) и SNMP версии 3 (SNMPv3). Эти версии имеют много общих функций, однако более новые версии содержат усовершенствования, такие как дополнительные протокольные операции, операционная гибкость и средства обеспечения безопасности.

В настоящее время чаще всего используется версия SNMPv2c, однако на многих платформах по-прежнему поддерживается SNMPv1. Самая современная версия SNMPv3 была опубликована в конце 2002 года в комплекте документов IETF (RFC 3410-3418). С тех пор она реализуется все большим количеством производителей и с течением времени заменит версию SNMPv2c. В настоящей главе описаны операции рассматриваемого протокола версий SNMPv1, SNMPv2c и SNMPv3. На рис. 58.1 показана базовая сеть, управляемая согласно протоколу SNMP.

Базовые компоненты протокола SNMP

Сеть, управляемая протоколом SNMP, состоит из трех основных компонентов: управляемых устройств, агентов и систем управления сетью (Network Management System — NMS), также называемых менеджерами.

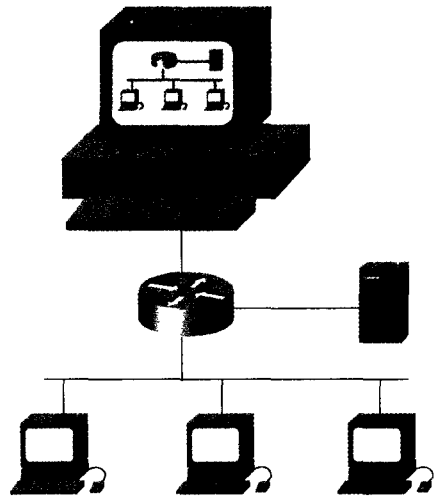


Рис. 58.1. SNMP облегчает обмен сетевой информацией между устройствами

Управляемое устройство представляет собой узел, принадлежащий управляемой сети, на котором установлен SNMP-агент. Управляемые устройства собирают, хранят и предоставляют управляющую информацию SNMP-системам управления сетью. Управляемыми устройствами, иногда называемыми сетевыми элементами, являются маршрутизаторы, коммутаторы, мосты, концентраторы, принтеры, компьютеры, серверы и брандмауэры.

Агент представляет собой программный модуль для управления сетью, установленный на управляемом устройстве. Агенту известна локальная управляющая информация, которую он преобразует в форму, совместимую с SNMP.

В *системах управления сетью* (Network-Management Systems — NMS) работают приложения, наблюдающие за устройствами и управляющие ими. В NMS сосредоточена основная часть ресурсов для обработки и хранения информации, требуемых для управления сетью. В любой управляемой сети, содержащей большое количество сетевых устройств, обязательно имеется одна или несколько систем NMS. Менеджеры NMS собирают или получают информацию от сетевых устройств по протоколу SNMP, хранят ее, генерируют статистику и предоставляют ее сетевым администраторам.

Взаимоотношения между этими тремя компонентами показаны на рис. 58.2.

Основные команды протокола SNMP

Мониторинг управляемых устройств и управление ими осуществляются с помощью четырех базовых команд протокола SNMP: **`read`**, **`write`**, **`trap`** и операций слежения.

Операция **`read`** используется системами NMS для наблюдения за управляемыми устройствами. Менеджеры NMS проверяют значения различных переменных, поддерживаемых управляемыми устройствами.

Операция **`write`** используется системами NMS для управления устройствами. Менеджер NMS изменяет значения переменных, хранящихся в управляемых устройствах.

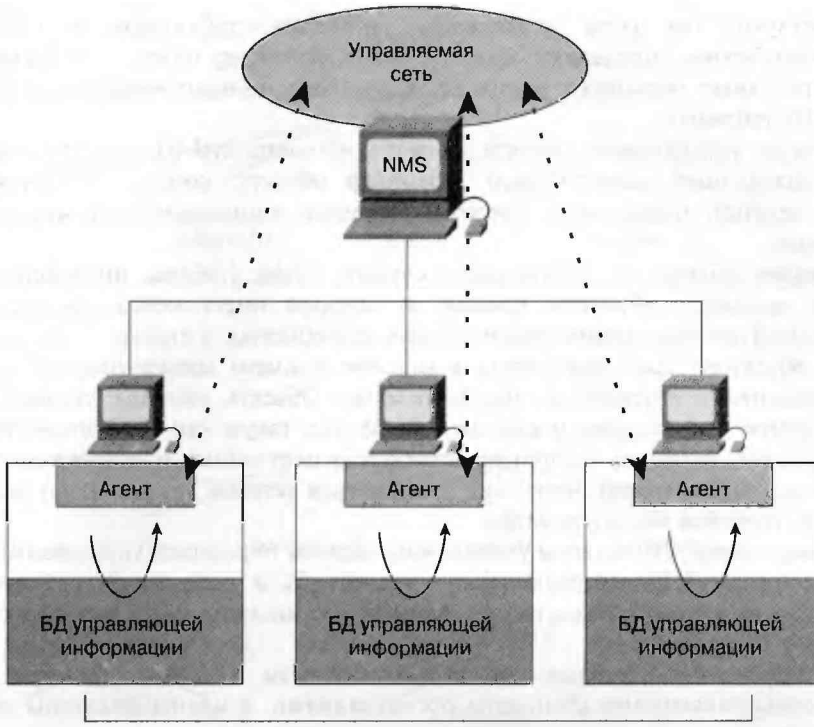


Рис. 58.2. Сеть, управляемая по протоколу SNMP, состоит из управляемых устройств, агентов и систем управления сетью

Операция **trap** используется управляемыми устройствами для асинхронного сообщения системам управления сетью NMS о событиях в сети. Когда происходят какие-либо заранее определенные события, управляемое устройство посылает прерывание менеджеру NMS.

Операции слежения (traversal operations) используются NMS-станциями для определения переменных, поддерживаемых управляемыми устройствами, и последовательного сбора информации из различных таблиц, например из таблиц маршрутизации.

База управляющей информации протокола SNMP

База управляющей информации (Management Information Base — MIB) представляет собой совокупность иерархически организованной информации. Доступ к базам MIB осуществляется посредством какого-либо протокола управления сетью, например, протокола SNMP. Базы MIB состоят из управляемых объектов; для обращения к этим базам используются идентификаторы объектов.

Управляемый объект (иногда называемый *MIB-объектом*, просто *объектом* или *MIB*) представляет собой одну из нескольких специфических характеристик управляемого устройства. Управляемые объекты состоят из одного или нескольких элементов, которые, как правило, являются переменными.

Существуют два типа управляемых объектов: табличные и скалярные. *Скалярные объекты* определяют единственный экземпляр объекта. *Табличные объекты* определяют несколько взаимосвязанных экземпляров объекта, объединенных в MIB-таблицах.

Примером управляемого объекта является величина sysUpTime. Это скалярный объект, содержащий единственный экземпляр объекта, которым является время (в сотнях секунд), прошедшее со времени последней реинициализации модуля управления сетью.

Примером табличного объекта может служить ifTable (таблица интерфейсов). Она содержит несколько объектов, каждый из которых имеет несколько экемпляров. Столбцы этой таблицы можно рассматривать как объекты, а строки — как экземпляры этих объектов. Если рассмотреть в качестве примера маршрутизатор, то объект ifTable относится к интерфейсам маршрутизатора. Объекты таблицы (столбцы) содержат различную информацию о каждом интерфейсе, такую как тип интерфейса, скорость передачи, название, состояние, количество полученных и отправленных пакетов. Каждый объект имеет несколько экземпляров (строки таблицы), по одной для каждого интерфейса маршрутизатора.

Идентификатор (ID) объекта уникальным образом определяет управляемый объект в MIB-иерархии. MIB-иерархию можно представить в виде дерева с безымянным корнем, уровни которого назначаются разными организациями. На рис. 58.3 показана структура MIB-дерева.

Идентификаторы объектов верхнего уровня базы MIB определяются различными разрабатывающими стандарты организациями, а идентификаторы объектов низшего уровня выделяются ассоциированными организациями.

Производители определяют частные ветви, куда помещают управляемые объекты для своих продуктов. В частных базах MIB можно определить специфические для данной сети объекты, позволяющие осуществлять более полное управление различными устройствами. Нестандартизованные базы MIB обычно размещаются в экспериментальной ветви базы.

Управляемый объект atInput может быть уникально идентифицирован либо по объектному имени — iso.identified-organization.dod.internet.private.enterprise.cisco.temporary variables. AppleTalk.atInput — либо по эквивалентному объектному дескриптору — 1.3.6.1.4.1.9.3.3.1.

Одной из задач сетевого администратора при установке и конфигурировании протокола SNMP для управления сетью является выбор правильных объектов, которые будут использоваться станцией NMS. Для этого требуется просмотреть несколько частных и общедоступных баз MIB и выяснить какие ветви, таблицы и объекты содержат информацию которая должна обновляться и по которой следует вести мониторинг.

Протокол SNMP и представление данных

Протокол SNMP должен выявлять несовместимости между управляемыми объектами и подстраиваться к ним. Разные компьютеры используют различные методы представления данных, которые могут помешать обмену информацией между управляемыми устройствами по протоколу SNMP. Для обмена данными между разными системами в SNMP используется подмножество синтаксической системы Abstract Syntax Notation 1 (ASN.1).

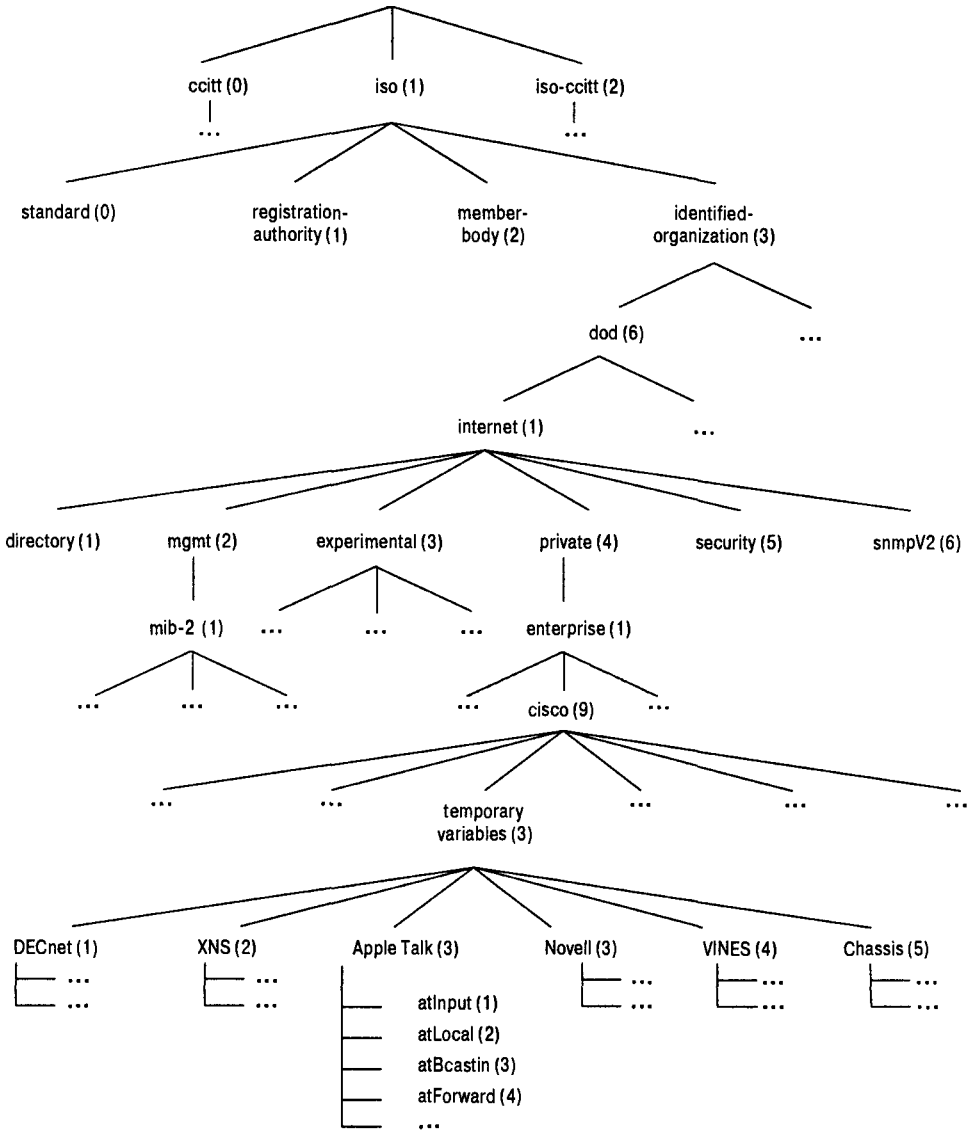


Рис. 58.3. MIB-дерево представляет собой иерархическую структуру, создаваемую различными организациями

Протокол SNMP версии 1

SNMP версии 1 (SNMPv1) представляет собой первоначальную реализацию протокола SNMP. Она описана в RFC 1157 и функционирует в рамках спецификаций структуры управляющей информации (Structure of Management Information — SMI). SNMP 1 работает с такими протоколами, как User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP) и Novell Internetwork Packet Exchange (IPX).

SNMP 1 широко распространен и фактически является стандартным протоколом управления сетью в Internet. Для протоколов стека TCP/IP протокол SNMP использует порты UDP 161 (команды `read` и `write`) и UDP 162 (команда `trap`).

Протокол SNMPv1 и структура управляющей информации

Структура управляющей информации (Structure of Management Information — SMI) определяет правила описания управляющей информации, используя абстрактную синтаксическую нотацию версии 1 (Abstract Syntax Notation One — ASN.1). Структура SMI для версии SNMPv1 описана в RFC 1155. SMI определяет три основные спецификации: типы данных ASN.1, типы данных SMI и таблицы MIB протокола SNMP.

Типы данных SNMPм1 и ASN.1

Согласно SMI SNMP 1, с каждым управляемым объектом связано некое подмножество типов данных ASN.1. Среди них обязательно присутствуют три типа данных ASN.1: имя, синтаксис и система кодирования. Имя служит идентификатором (ID) объекта. Синтаксис определяет тип данных объекта (например, целое число или строка). В SMI используется подмножество синтаксических определений ASN.1. Данные системы кодирования описывают форматирование информации, связанной с управляемым объектом, в наборы элементов данных для передачи по сети.

SNMP 1 и типы данных SMI

Структура SMI протокола SNMPv1 определяет использование некоторых типов данных SMI, которые делятся на две категории: простые типы данных и типы данных приложений.

В SMI SNMPv1 определены три простых типа данных; все они являются уникальными: целые числа, строки октетов и идентификаторы объекта. Целочисленные данные представляет собой целые числа со знаком в диапазоне от -2147483648 до 2147483647. Строки октетов представляет собой упорядоченные последовательности октетов от 0 до 65535 октетов. Идентификаторы объектов являются подмножеством всех идентификаторов объектов, созданных по правилам ASN.1.

В структуре SMI протокола SNMPv1 существует семь типов данных приложений, которые описаны ниже.

- Сетевые адреса представляет собой адреса, принадлежащие определенному семейству протоколов. SNMPv1 поддерживает только 32-разрядные IP-адреса
- Счетчики (counters) представляют собой неотрицательные целочисленные переменные, которые увеличиваются до тех пор, пока не достигнут максимального значения, после чего обнуляются. В SNMPv1 определен 32-разрядный счетчик.
- Калибр (gauge) представляет собой неотрицательное целое число, которое может увеличиваться или уменьшаться, но сохраняет максимальное достигнутое значение.
- Такт (time tick) равен количеству сотых долей секунды после какого-либо события.
- Под "непрозрачным" (opaque) объектом понимается произвольная система кодирования, используемая для передачи всех информационных строк, не принадлежащих к какому-либо из типов данных SMI.

- Целочисленный объект содержит целое число со знаком. Этот тип данных переопределяет целочисленный тип, который может иметь произвольную точность в ASN.1, а в SMI имеет ограниченную точность.
- Целочисленный объект без знака представляет целое число без знака и применяется для неотрицательных значений. Этот тип данных переопределяет целочисленный тип, который может иметь произвольную точность в ASN.1, а в SMI имеет ограниченную точность.

MIB-таблицы протокола SNMP

Структура SMI протокола SNMPv1 определяет строго структурированные таблицы, которые используются для группировки экземпляров табличных объектов (то есть объектов, содержащих несколько переменных). Таблицы могут иметь несколько строк или не иметь ни одной: эти строки проиндексированы таким образом, чтобы протокол SNMP мог извлекать или изменять целую строку одной операцией **Get**, **GetNext** или **Set**.

Операции протокола SNMPv1

SNMP является простым протоколом типа "запрос-ответ". Система управления сетью выдает запросы, а управляемые устройства отвечают на них. Это происходит при помощи одной из четырех протокольных операций: **Get**, **GetNext**, **Set** и **Trap**. Операция **Get** используется NMS для получения от агента значений одного или нескольких объектов. Если агент, отвечающий на операцию **Get**, не может предоставить значения всех объектов в списке, то он не выдает ни одного. Операция **GetNext** используется NMS для получения от агента значения следующего объекта в таблице или списке, а операция **Set** — для присвоения значения объекту агента. Операция **Trap** используется агентом для асинхронного оповещения NMS о важном событии.

Протокол SNMPv2

Протокол SNMP версии 2 (SNMPv2) является усовершенствованным вариантом версии *SNMPv1*. Первоначально, в 1993 г., SNMPv2 был опубликован как набор предлагаемых стандартов Internet; в настоящее время это проект стандарта. Как и для SNMPv1, функции SNMPv2 соответствуют спецификациям структуры управляющей информации (Structure of Management Information — SMI).

Теоретически SNMPv2 содержит ряд улучшений по сравнению с SNMPv1, включая дополнительные протокольные операции и функции защиты сети. Поскольку относительно спецификации по мерам безопасности в версии SNMPv2 не было единого мнения, в 1996 году была предложена новая версия — протокол SNMP версии 2, основанный на сообществах (SNMP version 2 community-based — SNMPv2c). В версии SNMPv2c были исключены функции обеспечения безопасности версии SNMPv2 и использовалась та же концепция сообществ, которая имеется в версии SNMPv1. Концепция сообществ рассматривается далее в настоящей главе. Соответственно, при обсуждении версии SNMPv2 имеется в виду обновленная версия (SNMPv2c).

SNMP 2 и структура управляющей информации

Структура SMI определяет правила описания управляющей информации с использованием синтаксических правил ASN.1.

Набор правил SMI SNMPv2 описан в RFC 1902. В этот документ вошли дополнения и улучшения типов данных структуры SMI для SNMPv1, такие как битовые строки, сетевые адреса и счетчики. Битовые строки определены только в SNMPv2 и состоят из нуля или более именованных битов, задающих некоторое значение. Сетевые адреса представляют собой адреса определенного семейства протоколов. В версии SNMPv1 поддерживаются только 32-разрядные IP-адреса, а в SNMPv2 — и другие типы адресов. Счетчики представляет собой неотрицательные целочисленные переменные, значения которых увеличиваются до определенного предела, после чего обнуляются. В версии SNMPv2 определен 32-разрядный счетчик, а в SNMP 2 также и 64-разрядный.

Информационные модули SMI

Набор правил SMI для версии SNMPv2 также определяет информационные модули, описывающие группы связанных между собой определений. Существуют три типа информационных модулей SMI:

- MIB-модули, которые содержат описания взаимосвязанных управляемых объектов.
- Операторы соответствия систематически описывают группы управляемых объектов, которые должны быть реализованы в соответствии со стандартом.
- Операторы возможностей точно показывают уровень поддержки, которую агент требует для MIB-группы.

Система управления сетью регулирует свое поведение относительно агентов в соответствии с операторами возможностей, связанными с каждым из них.

Операции протокола SNMPv2

Операции **Get**, **GetNext** и **Set**, используемые в протоколе SNMPv1, полностью сохранились и в версии SNMPv2. Однако в SNMPv2 появились некоторые новые операции, а другие были улучшены. Например, операция **Trap** в SNMPv2 выполняет ту же функцию, что и в SNMPv1, однако использует другой формат сообщений, и предназначена для замены операции **Trap** версии SNMPv1.

В версии SNMPv2 также определены две новые операции: **GetBulk** и **Inform**. Операция **GetBulk** используется системой сетевого управления NMS для эффективного извлечения больших блоков данных, например нескольких строк таблицы. **GetBulk** помещает в ответное сообщение максимально возможное для его размера количество требуемых данных. Операция **Inform** заключается в том, что одна система сетевого управления посылает trap-информацию другой системе сетевого управления NMS с целью получения ответа.

В версии SNMPv2 в случае, если агент, отвечающий на операцию **GetBulk**, не может присвоить значения всем переменным в списке, то он предоставляет частичные результаты. Важно отмечать направление каждой операции, как показано на рис. 58.4. Операции **Get**, **GetNext** и **Set** генерируют пакеты (UDP порт 161), которые посылаются станцией NMS (менеджером) управляемому устройству (агенту). После этого агент отправляет пакеты назад станции NMS. Операция **Trap** также генерирует пакеты (UDP порт 162), посылаемые управляемым устройством станции NMS, однако для операции **Trap** ответа или подтверждения не предполагается.

Вопросы безопасности

Поскольку протоколы SNMPv2 и SNMPv1 не выполняют аутентификацию, многие производители не реализуют в своих продуктах операцию **Set**, сводя тем самым функции SNMP к мониторингу сети.

Для уменьшения риска и повышения уровня безопасности при работе с SNMPv1/SNMPv2 рекомендуется ограничить диапазон адресов, имеющих доступ к агенту SNMP несколькими управляющими станциями. В случае использования маршрутизаторов это может быть сделано, например, путем применения списков доступа. Также рекомендуется использовать обзоры SNMP, что ограничивает количество доступных объектов и баз MIB. Это, однако, не может полностью исключить возможность несанкционированного доступа, если для этого агента используется протокол SNMPv1 или SNMPv2.

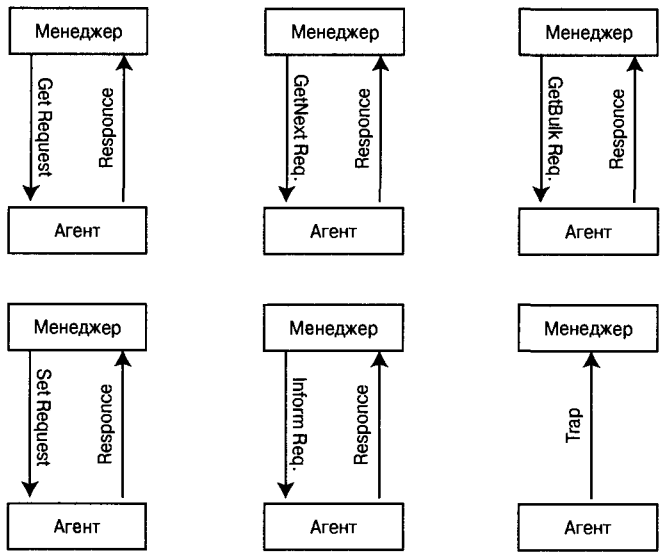


Рис. 58.4. Сообщения протокола SNMP

Протокол SNMP версии 3

Протокол SNMP версии 3 (SNMPv3) был предложен в качестве стандарта Internet в январе 1998 года для укрепления защиты сети протоколов SNMPv1 и SNMPv2. Эти первоначальные версии протокола SNMP не обеспечивали шифрования и аутентификации сообщений SNMP. Второй и третий наборы документов были предложены в качестве стандартов Internet для версии SNMPv3 в апреле 1999 года и декабре 2002 года. Последний набор в настоящее время является стандартом для SNMPv3.

Угрозы безопасности

Полное отсутствие аутентификации в протоколах SNMPv1/SNMPv2 делает сеть уязвимой в плане самых разнообразных угроз безопасности. Что касается обеспечения безопасности архитектуры протокола SNMPv3, то к наиболее известным угрозам от-

носятся нелегальное проникновение в сеть, изменение информации, перехват и модификация потока сообщений.

- Нелегальное проникновение имеет место в том случае, когда неавторизованный пользователь пытается выполнить операции по управлению сетью, предоставляя идентификационные данные авторизованного субъекта управления;
- Модификация информации включает в себя попытку неавторизованного субъекта изменить транзитные сообщения, созданные авторизованным субъектом управления, таким образом, чтобы выполнить несанкционированные операции управления сетью, в частности, фальсификацию значений объектов;
- Под перехватом понимается ситуация, в которой неавторизованный субъект извлекает значения, сохраняемые в управляемых объектах или узнает о значительных событиях в сети путем наблюдения за обменом информацией, происходящим между менеджерами и агентами;
- Модификация потока сообщений имеет место в том случае, когда неавторизованный субъект переупорядочивает, задерживает или копирует и позднее повторно воспроизводит сообщение, сгенерированное авторизованным субъектом.

Два других типа угроз: отказ в обслуживании и анализ проходящих потоков данных рассматриваются как менее важные и архитектура протокола SNMPv3 не гарантирует защиты от них. В настоящей главе эти два типа атак не обсуждаются.

Модульная архитектура

Архитектура протокола SNMPv3 по природе своего проектирования является модульной, как показано на рис. 58.5. Модульность архитектуры позволяет с течением времени изменять ее в соответствии с эволюцией стандартов SNMP. Любое устройство протокола SNMP содержит SNMP-модуль, который включает в себя диспетчер, подсистему обработки сообщений, подсистему защиты сети и подсистему управления доступом. Оно может также включать в себя различные приложения протокола SNMP, выполняющие специфическую функциональную обработку данных управления.

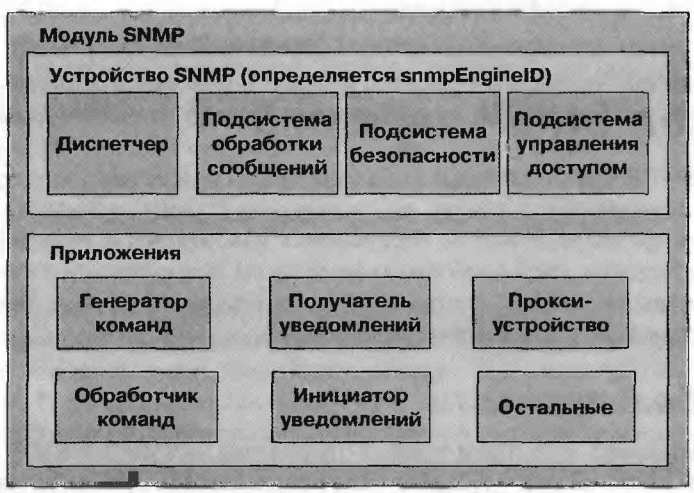


Рис. 58.5. Компоненты устройства протокола SNMP

Каждый тип устройства SNMP имеет модуль SNMP и различные модули приложений. Например, менеджер SNMP должен включать в себя устройство с приложениями генератора команд и/или получателя уведомлений. Агент SNMP должен включать в себя ответчика на команды и/или приложения инициатора уведомлений.

Устройство SNMP имеет один модуль SNMP, который обеспечивает службы отправки, получения и обработки сообщений, аутентификации и шифрования сообщений, а также службу управлении доступом к управляемым объектам. Эти службы обеспечиваются следующим образом:

- Диспетчер допускает одновременную поддержку нескольких версий сообщений SNMP в модуле SNMP. Он посылает и получает сообщения SNMP и распределяет модули данных протокола SNMP между приложениями протокола SNMP. В том случае, когда необходимо подготовить сообщение SNMP или извлечь данные из сообщения SNMP, диспетчер передает решение этих задач обрабатывающей сообщения модели, учитывающей версию сообщения; эта модель находится в подсистеме обработки сообщений.
- Подсистема обработки сообщений является частью модуля SNMP, которая взаимодействует с диспетчером в процессе обработки сообщений SNMP конкретной версии. Потенциально она содержит несколько моделей обработки сообщений для версий SNMPv3, SNMPv2, SNMPv1 и других.
- Подсистема обеспечения безопасности обеспечивает службы защиты, такие как аутентификация и сохранение конфиденциальности.
- Подсистема управления доступом обеспечивает службы авторизации, которые позволяют устройствам получать различные уровни доступа к управляемым объектам.

Ниже приведены модули приложений.

- Генератор команд осуществляет мониторинг и обрабатывает управляющие данные. Он также генерирует и обрабатывает ответы модулей PDU команд **Get**, **GetNext**, **GetBulk** и **Set**.
- Обработчик команд обеспечивает доступ к данным управления. Он получает модули PDU вышеупомянутых типов (сгенерированные ответчиком команд), генерирует ответное сообщение и отправляет его инициатору запроса.
- Инициатор уведомления инициирует асинхронные сообщения. Он осуществляет мониторинг системы, а после этого, в зависимости от заданных ему конфигурациейфункций, генерирует сообщение **Trap** или **Inform** и отсылает его заранее определенным устройствам получателей.
- Получатель уведомления обрабатывает асинхронные сообщения. Он просматривает проходящие по сети данные с целью обнаружения сообщений-уведомлений, сообщений команды **Trap** и информационных сообщений. Если полученное сообщение является информационным, то он посылает ответ его инициатору.
- Прокси-устройство пересылки пересылает сообщения SNMP между устройствами. Реализация приложения прокси-пересылки не является обязательной и осуществляется по желанию пользователя.

Архитектура безопасности

Документы RFC, определяющие протокол SNMPv3, описывают проблемы безопасности на двух разных этапах: приема/передачи сообщений и обработки содержания сообщений. В документах RFC для протокола SNMPv3 термин "безопасность" применяется по отношению к аспектам безопасности на уровне сообщений, а термин "управление доступом" — по отношению к вопросам безопасности протокольных операций.

Типичными функциями обеспечения безопасности на уровне сообщений являются аутентификация, шифрование и проверка срока давности. В процессе обработки сообщения может потребоваться управление доступом. Оно ограничивает доступ к управляемым объектам для выполнения операций над ними. Модель управления доступом (Access Control Model) определяет механизмы, которые принимают решение о том, разрешен ли доступ к управляемому объекту.

Для поддержки служб безопасности и управления доступом в протоколе SNMP применяется понятие *принципала (principal)*. Под принципалом понимается устройство, от имени которого предоставляются службы или происходит обработка. Принципал может быть отдельным субъектом, выполняющим определенную роль, набором таких субъектов, каждый из которых выполняет определенную функцию, приложением или набором приложений, а также комбинацией вышеупомянутых. Идентификационные данные принципала используются для задания функций безопасности, которые будут использоваться при осуществлении связи с агентом. Архитектура протокола SNMPv3 определяет три уровня обеспечения безопасности: отсутствие аутентификации и обеспечения конфиденциальности, аутентификацию и отсутствие обеспечения конфиденциальности, а также аутентификацию и обеспечение конфиденциальности.

Модель защиты сети для отдельного пользователя

Модель обеспечения безопасности протокола SNMP поддерживает следующие службы: обеспечение целостности данных, аутентификация источника, обеспечение конфиденциальности, проверка срока давности и ограниченную защиту от атаки воспроизведения. Для решения этих задач в версии SNMPv3 используется понятие авторитетного SNMP-устройства, которое является одной из частей процесса передачи сообщения. Для определения того, что является авторитетным устройством, используются два правила:

- Если полезная нагрузка сообщения требует подтверждения или ответа (модули PDU, требующие подтверждения: **`Get`**, **`GetNext`**, **`GetBulk`**, **`Set`** или **`Inform`**), то авторитетным устройством является получатель.
- Если полезная нагрузка сообщения на требует ответа (модули PDU, не требующие подтверждения: **`Response`**, **`Report`** или **`Trap`**), то авторитетным устройством является отправитель.

При отправке SNMP-сообщения устройство отправителя включает в него набор индикаторов ограничения времени, а получатель оценивает их для того, чтобы определить, является ли это сообщение новым. Срок давности сообщения определяется по часам, которые поддерживаются авторитетным устройством. Каждое сообщение также

включает в себя идентификатор, уникальный для авторитетного устройства SNMP, логически связанного с отправителем сообщения или предполагаемыми получателем.

Для каждого отправленного сообщения USM включает в заголовок несколько параметров безопасности, которые оцениваются USM-процессом на стороне получателя. Эти параметры содержат информацию о пользователе, протоколе авторизации, ключе авторизации, авторитетном устройстве, протоколе обеспечения конфиденциальности и времени отправки. Для этой модели обеспечения безопасности устройства SNMP должны иметь предварительную информацию обо всех пользователях, которые имеют авторизацию на проведение операций по управлению.

RFC 3414, *User-based Security Model for SNMPv3*, определяет приведенные ниже требования.

- В качестве протокола аутентификации должен поддерживаться протокол HMAC-MD5-96.
- В качестве протокола аутентификации должен также поддерживаться протокол HMAC-SHA-96, а в будущем возможна поддержка дополнительных или заменяющих вышеупомянутые протоколов аутентификации.

Следует отметить, что протокол HMAC-MD5-96 использует MD5 (см. RFC 1321, Message Digest 5) в качестве хэш-функции для основанного на хэш-функции режима кода аутентификации сообщения (Hash-based Message Authentication Code — HMAC). Протокол MD5-96 осуществляет усечение выходных данных до 96 битов. Протокол HMAC-SHA-96 делает то же самое, однако использует в качестве хэш-функции SHA (SHA-NIST). Протокол HMAC (см. RFC 2104) представляет собой механизм аутентификации сообщения, а MD5 и SHA используются в качестве криптографических хэш-функций.

В аспекте обеспечения конфиденциальности определяется использование симметричного шифрования CBC-DES вместе с моделью безопасности для конкретного пользователя. В будущем могут быть также определены в качестве дополнительных или заменяющих другие протоколы обеспечения конфиденциальности. CBC-DES представляет собой режим стандарта шифрования данных (Data Encryption Standard — DES) с объединением шифровых блоков, который, в случае поступающего запроса, USM использует для шифрования отправляемого сообщения и предотвращения чтения содержимого этого сообщения третьими сторонами.

Модель управления доступом на основе View

Как определяется в RFC 3415, *VACM for the SNMP*, подсистема управления доступом устройства SNMP проверяет, разрешен ли запрашиваемый тип доступа (read, write, notify) к данному объекту (instance). Когда устройство SNMP обрабатывает запрос на извлечение данных (Get, GetNext, GetBulk) или запрос на модификацию (Set), оно должно осуществлять контроль доступа. Например, приложение ответчика на команды применяет контроль доступа при обработке запроса, которое оно получает от приложения-генератора запроса. Перед отправкой SNMP-сообщения-уведомления (инициированного приложением создающим уведомление) устройство протокола SNMP также должно выполнить контроль доступа.

Управление доступом конфигурируется группой пользователей, при этом каждая группа может включать в себя нескольких пользователей. Политика обеспечения безопасности должна быть предварительно сконфигурирована на устройствах SNMP, осуществляющих управление доступом. Для выработки политики управления доступом

администратор сначала определяет, какой тип операции может быть использован этой группой (**read**, **write** или **notify**). После этого администратор определяет права доступа к этой операции. Например, агент может быть сконфигурирован таким образом, что он дает группе пользователей право чтения только одной базы MIB (или части базы MIB). Он может быть также сконфигурирован так, чтобы другая группа пользователей получила право записи в несколько MIB-объектов.

Управление посредством SNMP

SNMP является протоколом распределенного управления. Система может функционировать исключительно как NMS или в качестве агента, или выполнять обе эти функции. В последнем случае другая NMS может потребовать, чтобы устройства управлялись системными запросами, чтобы предоставлялись краткие сводки о полученной информации или чтобы система сообщала о сохраняемой локальной управляющей информации.

Справочные данные протокола SNMP: форматы сообщений SNMP

Сообщения SNMPv2 состоят из заголовка и модуля PDU. Базовый формат SNMP-сообщений показан на рис. 58.6.

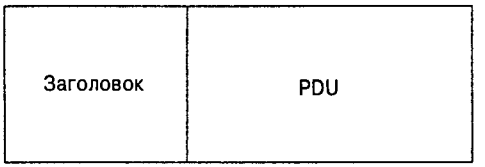


Рис. 58.6. Сообщения SNMP 2 состоят из заголовка и PDU

Заголовок сообщения SNMP

Заголовки сообщений SNMPv2 состоят из двух полей: номера версии и имени сообщества. Ниже приводится краткое описание этих полей.

- **Номер версии.** Версия SNMP.
- **Имя сообщества.** Среда доступа для группы NMS. Предполагается, что системы сетевого управления данного сообщества принадлежат тому же административному домену. Имена сообществ не очень хорошо подходят для идентификации, так как устройства, которым не известно правильное имя сообщества, не допускаются к операциям SNMP.

Модуль данных SNMP

В пользователе SNMP определено два формата модулей PDU, в зависимости от операции протокола SNMP. Поля PDU SNMP имеют переменную длину, описанную в ASN.1.

Поля PDU (протокола SNMPv2) Get, GetNext, Inform, Response, Set и Trap показаны на рис. 58.7.

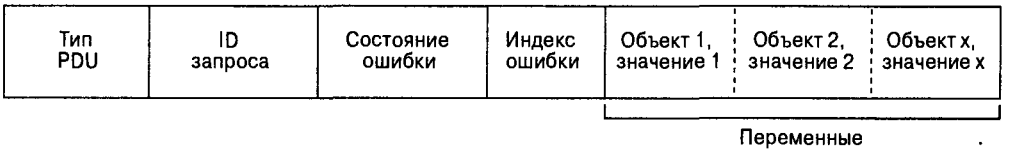


Рис. 58.7. Модули PDU протокола SNMPv2 Get, GetNext, Inform, Response, Set и Trap содержат одинаковые поля

Их описания приводятся ниже.

- **Тип PDU.** Тип переданного PDU (Get, GetNext, Inform, Response, Set или Trap).
- **ID запроса.** Ассоциирует запросы SNMP с откликами.
- **Состояние ошибки.** Номер и тип ошибки. Это поле заполняется только операциями отклика. Остальные операции заносят туда ноль.
- **Индекс ошибки.** Ассоциирует ошибку с конкретным объектом. Это поле заполняется только операциями отклика. Остальные операции заносят туда ноль.
- **Переменные.** Поле данных PDU SNMPv2. Каждая переменная соответствует конкретному объекту и его текущему значению (за исключением запросов Get и GetNext, для которых значение игнорируется).

Формат PDU GetBulk

Поля модуля PDU GetBulk SNMPv2 показаны на рис. 58.9.

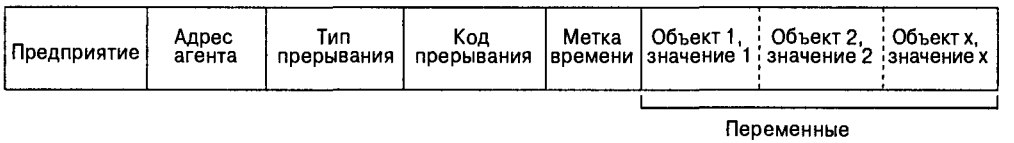


Рис. 58.8. Модуль PDU GetBulk SNMPv2

Ниже описаны поля, показанные на рис. 58.8.

- **Тип PDU.** Идентифицирует PDU как операцию GetBulk.
- **ID запроса.** Ассоциирует запросы SNMP с ответами.
- **Без повторений.** Количество объектов, указанных среди переменных, которые не должны извлекаться больше одного раза с начала запроса. Это поле используется, если некоторые из объектов являются скалярными и имеют только одну переменную.
- **Максимум повторений.** Максимальное количество извлечений переменных, не указанных в поле "без повторений".
- **Переменные.** Поле данных PDU SNMPv2. Каждая переменная соответствует конкретному объекту и его текущему значению (за исключением запросов Get и GetNext, для которых значение игнорируется).

Trap PDU Format

На рис. 58.9 показаны поля модуля PDU Trap протокола SNMP.

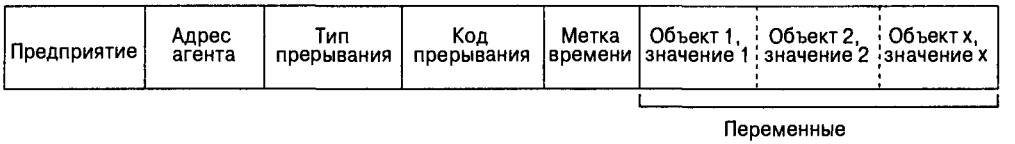


Рис. 58.9. Поля модуля PDU Trap протокола SNMP

Ниже описаны поля, показанные на рис. 58.9.

- **Предприятие.** Тип управляемого объекта, генерирующего прерывание.
- **Адрес агента.** Адрес управляемого объекта, генерирующего прерывание.
- **Общий тип прерывания.** Номер общего типа прерывания.
- **Код прерывания.** Номер специального типа прерывания.
- **Метка времеии.** Время, которое прошло между последней реинициализацией сети и генерированием прерывания.
- **Переменные.** Поле данных модуля PDU протокола SNMP. Каждая переменная соответствует конкретному объекту и его текущему значению.

Резюме

Протокол SNMP представляет собой протокол уровня приложений стека протоколов TCP/IP. Он был создан для того, чтобы стандартизовать архитектуру сетевого управления. Протокол SNMP использует схему, включающую в себя станции управления сетью (менеджеры), которые осуществляют мониторинг и управление сетевыми устройствами. Менеджер также выполняет функции интерфейса между самой сетью и сетевым администратором. На управляемом устройстве установлено агентское программное обеспечение, которое взаимодействует с менеджером с помощью набора протокольных операций, таких как `Get`, `Set`, `Get`, `Next`, `GetBulk` и `Trap`. Эти операции работают с множеством иерархически организованных переменных, называемом базой MIB, которая поддерживается агентским программным обеспечением на управляемых устройствах.

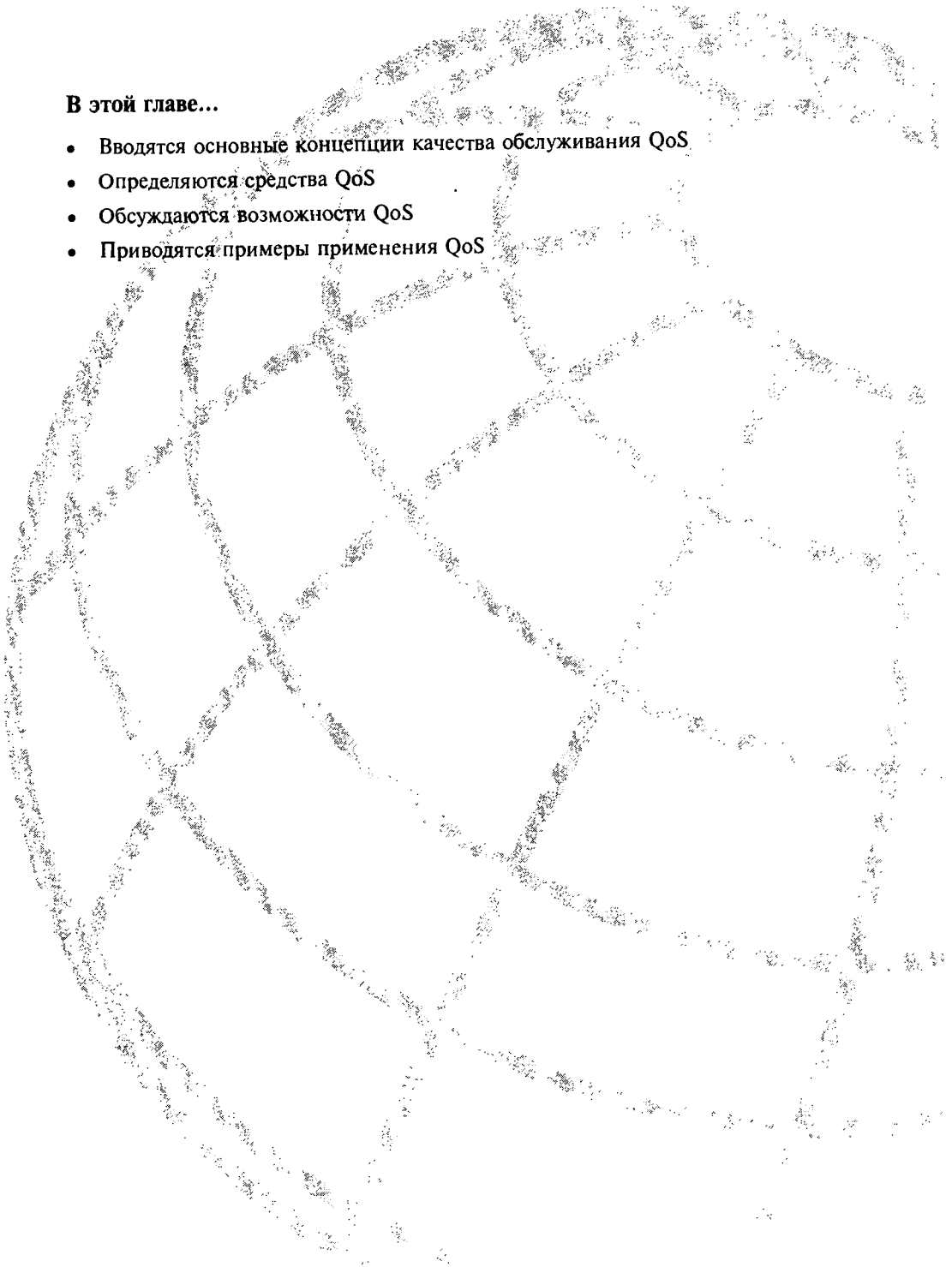
Для расширения возможностей протокола SNMP за последние несколько лет были разработаны несколько версий этого протокола. В самой последней версии этого протокола (SNMPv3) были преодолены ограничения предыдущих версий, связанные с обеспечением безопасности сети и включены новые функции, связанные с аутентификацией, шифрованием и управлением доступом.

Контрольные вопросы

1. Что такое агент SNMP?
2. Что такое база MIB и как получить к ней доступ?
3. Назовите несколько протокольных операций, доступных в протоколе SNMPv2.
4. Каков основной недостаток версий SNMPv3 и SNMPv2, устраненный в SNMPv3?

В этой главе...

- Вводятся основные концепции качества обслуживания QoS
- Определяются средства QoS
- Обсуждаются возможности QoS
- Приводятся примеры применения QoS



Глава 59

Качество обслуживания

Введение

Под качеством обслуживания (Quality of Service — QoS) понимается способность сети предоставлять улучшенное обслуживание определенным видам передаваемых по сети данных при помощи различных технологий, таких как Frame Relay, Asynchronous Transfer Mode (ATM) и др. Эти технологии могут также применяться в сетях Ethernet, 802.1, SONET и в сетях с IP-маршрутизацией. Целями QoS являются: задание приоритетов, выделение определенной полосы пропускания, управление уровнем дребезга и величиной задержки (это необходимо для некоторых видов потоков данных реального времени и данных интерактивного обмена), а также уменьшение потерь. Кроме того, важно гарантировать, что задание высокого приоритета одному или нескольким потокам данных не приведет к прекращению передачи остальных потоков. Технологии QoS представляют собой элементарные компоненты, которые будут использоваться в будущих коммерческих приложениях для сетей кампусов, распределенных сетей и для сетей провайдеров служб. В настоящей главе описываются возможности и преимущества QoS, предоставляемые операционной системой IOS Cisco.

Примечание

Существует несколько определений потока данных. Часто потоком называют комбинацию адресов источника и получателя, их номеров сокетов и идентификатора сеанса. Более широкое определение потока — любая последовательность пакетов, исходящих от определенного приложения или поступающих на входной интерфейс. Современные средства идентификации позвопяют определить поток более точно (например, по URL или по типу MIME в пакете HTTP). В настоящей главе под *потоком (flow)* может подразумеваться любое из этих определений.

Программное обеспечение операционной системы IOS Cisco позволяет управлять качеством обслуживания и гарантировать определенный уровень QoS различным сетевым приложениям и типам потоков данных в объединенных сетях. Использование QoS позволяет повысить эффективность работы практически любой сети, будь то сеть небольшой фирмы, провайдера служб Internet или крупная корпоративная сеть. Программное обеспечение IOS Cisco QoS предоставляет следующие преимущества.

- **Управление ресурсами.** Контроль использования ресурсов (полосы пропускания, оборудования, глобальных каналов и т.п.). Например, можно ограничить полосу пропускания основной магистрали, используемую для передачи данных протокола FTP или задать высокий приоритет доступу к важной базе данных.
- **Более эффективное использование сетевых ресурсов.** Средства анализа сетевого управления и учетных записей Cisco позволяют определить, для чего используется сеть, и обслуживать в первую очередь потоки данных, наиболее важные с коммерческой точки зрения.
- **Обслуживание по заказу.** Управление передачей данных и возможность наблюдения за ней, обеспечиваемые QoS, позволяют провайдерам услуг Internet предложить своим клиентам широкий диапазон служб в соответствии с пожеланиями пользователя.
- **Сосуществование важных приложений.** Технологии Cisco QoS гарантируют рациональное использование глобальной сети приложениями, критически важными с коммерческой точки зрения. Они гарантируют мультимедийным приложениям и приложениям для обработки звука нужную полосу пропускания и минимальные задержки, а также соответствующее качество обслуживания других приложений, использующих этот канал, не мешая прохождению критически важных данных.
- **Основа для создания в будущем полностью интегрированной сети.** Внедрение технологий QoS Cisco представляет собой рациональное начало реализации полностью интегрированной мультимедийной сети, которая потребуется в ближайшем будущем.

Концепции QoS

QoS обеспечивает главным образом улучшенное обслуживание некоторых потоков. Это достигается либо с помощью повышению приоритета потока, либо путем понижения приоритета другого потока. Используя средства управления перегрузкой, можно повысить приоритет потока путем организации очередей и обслуживания таких очередей разными способами. Программа управления очередями, используемая для предотвращения переполнения в сети, повышает приоритет, отбрасывая низкоприоритетные потоки раньше, чем высокоприоритетные. Использование политик и формирование потоков обеспечивает приоритетность потоку путем ограничения пропускной способности для остальных потоков. Механизмы повышения эффективности каналов связи ограничивают большие потоки, оказывая предпочтение более мелким.

Программное обеспечение качества обслуживания QoS в операционной системе IOS Cisco представляет собой набор утилит, многие из которых позволяют достичь одного и того же результата. Их использование можно сравнить с затягиванием гайки: это можно сделать и плоскогубцами, и гаечным ключом. Оба способа одинаково эффективны, но используют разные инструменты. То же самое относится к утилитам QoS: разные утилиты позволяют добиться одного и того же результата. Вопрос о том, какую из них следует применять, зависит от характера потоков данных. Было бы нерационально выбирать инструмент, не зная, для каких целей он нужен. Это было бы похоже на попытку вбить гвоздь отверткой.

Утилиты QoS позволяют решить большинство проблем переполнения. Однако часто поток данных оказывается слишком велик для имеющейся полосы пропускания. В таких случаях QoS — всего лишь бандаж, укрепляющий "узкое место". Напрашивается простая аналогия с заливанием сиропа в бутылку: для того чтобы перелить сироп из одной емкости в другую, горлышко второй должно быть не уже, чем у первой. Если струя шире горлышка, то сироп прольется. Но если взять воронку, диаметр которой гораздо шире, чем горлышко бутылки, то можно будет залить сироп из широкой емкости в узкую, не пролив его. Однако если лить не переставая, то воронка тоже в конце концов переполнится.

Базовая архитектура QoS

Базовая архитектура QoS состоит из трех основных компонентов (рис. 59.1).

- Методы идентификации и маркировки для согласования QoS между различными элементами сети.
- QoS в отдельном элементе сети (например, организация очередей, задание расписания и ограничение потоков данных).
- Функции задания политик, управления и учета QoS для управления и администрирования сквозной передачи данных в сети.

Рис. 59.1. Базовая реализация QoS содержит три основных компонента

Идентификация и маркировка QoS

Идентификация и маркировка QoS выполняются путем классификации и резервирования.

Классификация

Для первоочередного обслуживания определенного типа данных необходимо в первую очередь обеспечить его идентификацию. Кроме того, пакет может быть маркирован. Эти две задачи выполняются путем классификации. Если пакет идентифицирован, но не маркирован, то классификация выполняется последовательно на узлах следующего перехода. Это означает, что классификация относится только к данному устройству и не передается следующему маршрутизатору. Такая ситуация имеет место при использовании приоритетной очередности (Priority Queuing — PQ) или настраиваемой очередности (Custom Queuing — CQ). Если пакеты маркируются для общесетевого использования, то могут быть установлены биты IP-приоритетности (см. раздел "IP-приоритетность: передача информации о дифференцированном QoS".).

Основными методами идентификации потоков являются списки управления доступом (Access Control Lists — ACL), маршрутизация на основе политик, согласованная скорость доступа (Committed Access Rate — CAR) и распознавание приложений на основе типа сети (Network-Based Application Recognition — NBAR).

Функции QoS в пределах одного сетевого элемента

Качество обслуживания в пределах одного сетевого элемента обеспечивается путем управления перегрузкой, очередностью, эффективностью канала, а также средствами ограничения потоков и задания политик.

Управление перегрузкой

Вследствие пульсирующего характера потоков аудио-, видео- и цифровых данных их объемы иногда превышают возможности канала. Что в таком случае делает маршрутизатор? Помещает ли он все данные в буфер общей очереди, откуда пакет, поступивший первым, первым и отправляется? Или он помещает пакеты в разные очереди и обслуживает некоторые из них чаще других? Эти вопросы решаются при помощи средств управления переполнением, таких как задание приоритетной очередности (PQ), настраиваемой очередности (CQ), взвешенной справедливой очередности (WFQ) или основанной на классах взвешенной справедливой очередности (CBWFQ).

Управление очередями

Поскольку очереди не бесконечны, они могут заполняться и переполняться. Если очередь уже заполнена, то новые пакеты в нее не попадают и отбрасываются. Это явление называется концевыми потерями. Проблема концевых потерь заключается в том, что в этой ситуации маршрутизатор не может не отбрасывать данный пакет, даже если он имеет высокий приоритет. Таким образом, необходим механизм, выполняющий следующие две операции.

1. Выяснить, действительно ли очередь переполнена и нет ли в ней места для пакетов с высоким приоритетом.

2. Сформулировать некоторые критерии, по которым в первую очередь будут отбрасываться пакеты с более низким приоритетом, и только потом — с более высоким.

Оба эти механизма обеспечиваются алгоритмом взвешенного случайного раннего распознавания (Weighted Early Random Detect — WRED).

Методы повышения эффективности канала

При передаче мелких пакетов по низкоскоростным соединениям часто возникают проблемы. Например, задержка при разбиении на части 1500-байтового пакета при передаче по 56-килобитовому каналу составляет 214 мсек. Если бы за этим большим пакетом следовал бы голосовой пакет, то его лимит задержки был бы превышен еще до того, как пакет покинул маршрутизатор! Фрагментация и чередование позволяют разделять такие крупные пакеты на пакеты меньшего размера, чередующиеся с голосовыми пакетами. Чередование не менее важно, чем фрагментация. Было бы бессмысленным фрагментировать пакет и направлять голосовой пакет вслед за всеми получившимися фрагментами.

Примечание

Задержка при разбиении на части определяется временем, необходимым для помещения пакета в канал. Для приведенного выше примера получаем:

размер пакета: 1500 байт × 8 бит/байт = 12000 бит

скорость передачи: 56000 бит/с

задержка: 12000 бит / 56000 бит/с = 0,214 с = 214 мс

Другим способом повышения производительности является ликвидация лишних битов служебной нагрузки. Например, заголовок протокола RTP состоит из 40 байтов. В некоторых случаях при полезной нагрузке в 20 байтов служебная нагрузка может оказаться вдвое больше полезной. Сжатие заголовка RTR (результат называется сжатым заголовком протокола реального времени (Compressed Real-Time Protocol — CRTP) позволяет сократить его до более управляемого размера.

Формирование потока и применение политик

Формирование или ограничение потока (shaping) позволяет создать поток данных, ограничивающий потенциал полной полосы пропускания. Формирование потока часто используется для предотвращения описанных во введении проблем переполнения. Например, многие сетевые топологии используют технологию Frame Relay и звездообразную структуру. При этом центральный узел, как правило, имеет высокоскоростной канал (например, T1), а удаленные узлы — сравнительно низкоскоростные каналы (например, каналы 384 Кбит/с). В этом случае потоки данных, передаваемые из центрального узла, могут переполнить узкую полосу пропускания на другом конце. В этом случае ограничение потоков является эффективным способом настроить скорость передачи данных таким образом, чтобы она была близка к 384 Кбит/с, для предотвращения перегрузки удаленного канала. Данные, передача которых в данный момент превышает возможности канала, помещаются в буфер и передаются позже.

Использование *политик* аналогично ограничению потоков, однако отличается в одном очень важном пункте: данные, которые не удается передать, не буферизируются (они, как правило, отбрасываются).

Примечание

Cisco-реализация политик с использованием согласованной скорости доступа (Committed Access Rate — CAR) позволяет выполнять, кроме отбрасывания данных, еще ряд действий. Однако обычно использование политик позволяет только отбрасывать избыточные данные.

Управление QoS

Управление QoS дает возможность задавать политики QoS и определять их цели. Общая методика включает в себя приведенные ниже действия.

Этап 1: Установить в сети устройства типа датчиков RMON. Это позволит определить типовые параметры передачи данных по сети. Кроме того, необходимо установить приложения, требующие использования функций QoS (обычно требования приложений представляют собой время отклика).

Этап 2: После того, как будут получены параметры передачи данных по сети и выбраны приложения, требующие повышения QoS, следует настроить соответствующие механизмы QoS.

Этап 3: Оценить результаты путем тестирования откликов от выбранных приложений, чтобы определить, достигнуты ли нужные показатели QoS.

Для упрощения внедрения QoS можно использовать менеджер политик Cisco (Quality of Service Policy Manager — QPM) и менеджер устройств Cisco (Quality of Service Device Manager — QDM). Для тестирования полученного уровня обслуживания можно воспользоваться менеджером производительности сети Cisco (Internetwork Performance Monitor — IPM).

Следует исходить из того, что в постоянно меняющейся сетевой среде обеспечение QoS не является единичным действием, а является постоянной и существенной частью сетевого проекта.

Уровни сквозного QoS

Под *уровнями обслуживания* понимаются реальные возможности обеспечения сквозного качества обслуживания QoS, т. е. возможности сети по предоставлению уровня обслуживания, необходимого конкретному потоку данных на всем протяжении его пути следования от одной конечной станции до другой. Службы различаются по уровням *строгости соблюдения QoS*, т. е. по тому, насколько точно служба выполняет требования к полосе пропускания, задержке, дребезжанию и допустимому уровню потерь.

В гетерогенных сетях предоставляются описанные ниже три основных уровня сквозного QoS (рис. 59.2).

- **Обслуживание с негарантированной доставкой.** Также называется службой без QoS. Простейшее соединение без каких-либо гарантий доставки. Важнейшим признаком такого обслуживания является использование очередей типа "первым вошел — первым вышел" (first in — first out — FIFO), в которых отсутствует дифференциация потоков.

- **Дифференцированное обслуживание.** Также называется гибким QoS. При его использовании некоторые виды данных обрабатываются лучше, чем остальные (быстрее обрабатываются, больше средняя полоса пропускания, ниже средний уровень потерь). Однако это лишь статистическая оценка, без жестких и четких гарантий. Этот вид обслуживания обеспечивается путем классификации потоков данных и использования таких средств QoS, как установка очередностей PQ, CQ, WFQ, и WRED (все они описываются далее в настоящей главе).
- **Гарантированное обслуживание.** Также называется жестким QoS. Полное резервирование сетевых ресурсов для конкретных типов данных. Обеспечивается с помощью таких средств QoS, как протокол резервирования ресурсов (Resource Reservation Protocol — RSVP) и установка очередности CBWFQ (описываются далее в настоящей главе).

Выбор типа обслуживания зависит от описанных ниже факторов.

- Тип используемого приложения или проблемы, которые нужно решить пользователю. Каждый из трех типов обслуживания подходит для определенных приложений. Это не означает, что пользователь должен переходить на дифференцированное, а затем на гарантированное обслуживание (хотя, возможно, многие пользователи именно так впоследствии и сделают). Ему вполне может подойти дифференцированное обслуживание или даже негарантированная доставка — все зависит от требований, выдвигаемых приложениями пользователя.
- Реальные возможности пользователя быстро модернизировать свою инфраструктуру. Обычно модернизация осуществляется в направлении обеспечения дифференцированного, а затем и гарантированного обслуживания, которое требует расширения набора средств, необходимых для дифференцированного обслуживания.
- Стоимость реализации и распространения гарантированного обслуживания, скорее всего, будет выше стоимости внедрения дифференцированного обслуживания.

Интерфейс командной строки модульного качества обслуживания QoS

Интерфейс командной строки (Command-Line Interface — CLI) модульного QoS Cisco определяет на маршрутизаторе новую конфигурацию основанного на CLI модульного QoS. Эта новая структура для задания политик QoS группирует элементы конфигурации QoS в три отдельных модуля: определение класса потока данных, задание политики и применение политики.

В CLI-модели модульного QoS политики QoS могут быть сконфигурированы на маршрутизаторе в три этапа, по одному на каждый модуль новой модели интерфейса CLI.

1. Определение класса для потока данных: конфигурирование политики классификации потоков. Это осуществляется с помощью команды конфигурирования **`class map`**.
2. Задание политики: конфигурирование политик для различных определенных классов потоков данных. Для этого используется команда конфигурирования **`policy map`**.

3. Применение политики: включение использования политики на интерфейсе. Для этого используется команда конфигурирования **service policy**.

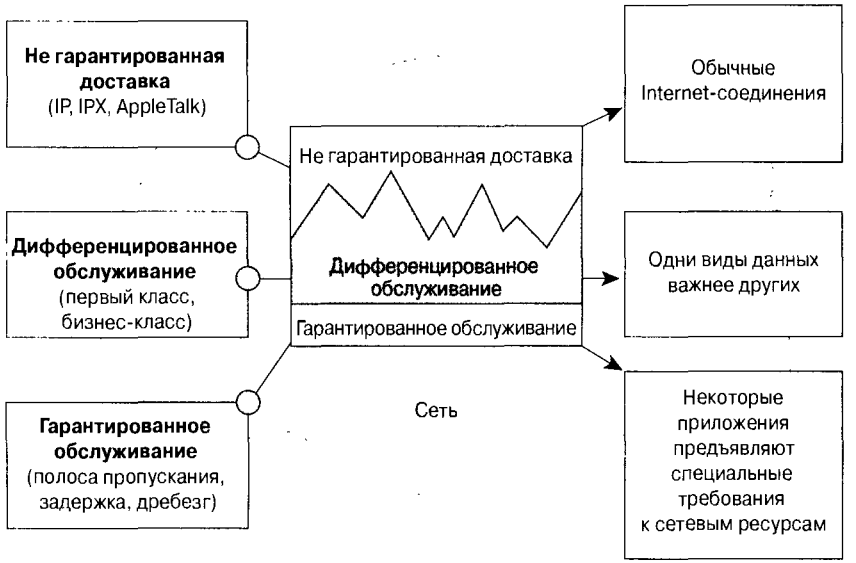


Рис. 59.2. Три уровня сквозного QoS: негарантированная доставка, дифференцированное обслуживание и гарантированное обслуживание

Различные архитектуры QoS

Для облегчения реализации QoS в IP-сети группа IETF (Internet Engineering Task Force) разработала две модели: модель интегрированных служб (Integrated Services — IntServ) и модель дифференцированных служб (Differentiated Services — DiffServ или DS). Модель IntServ следует модели сигнализируемого QoS, в котором конечный узел сообщает сети о своих потребностях в QoS. Модель DiffServ работает на основе provisioned модели QoS, в которой сетевые элементы конфигурируются для обслуживания различных классов данных с разными требованиями к QoS. Программное обеспечение IOS Cisco поддерживает обе модели: как IntServ, так и DiffServ QoS.

Модель IntServ обеспечивает всеобъемлющее сквозное решение проблемы QoS путем сквозной сигнализации, поддержки состояния (для каждого потока и резервирования протокола RSVP) и управление допуском к каждому сетевому элементу. С другой стороны, модель DiffServ удовлетворяет потребность в относительно простых, хотя и не слишком строгих методах обеспечения QoS путем причисления потоков данных к различным классам обслуживания (CoS) и применения к этим классам параметров QoS. Для этого пакеты подразделяются на классы путем задания типа обслуживания (type-of-service — ToS) в соответствующем байте IP-заголовка.

Архитектура интегрированных служб

Для сигнализации и резервирования ресурсов, которое обеспечивает требуемое качество обслуживания QoS каждого потока в сети, модель IntServ использует протокол

резервирования ресурсов RSVP. Обычно пакеты, проходящие по сети, идентифицируются на основе принадлежности к определенному потоку с использованием пяти полей в IP-заголовке: IP-адрес источника, IP-адрес получателя, поле протокола IP, а также порты источника и получателя. Отдельный поток состоит из пакетов, передаваемых от приложения станции-отправителя приложению станции получателя. Пакеты, принадлежащие к одному и тому же потоку, имеют одни и те же значения в пяти полях потока IP-заголовка. С помощью протокола RSVP могут быть запрошены два типа обслуживания ToS (предполагается, что все сетевые устройства на маршруте от отправителя к получателю поддерживают протокол RSVP). Первый тип представляет собой строгую гарантирующую службу, которая задает четкие границы сквозной задержки и гарантированную полосу пропускания для потоков данных, удовлетворяющих спецификациям резервирования ресурсов. Второй тип обслуживания представляет собой службу, управляющую нагрузкой, которая гарантирует, что поток с зарезервированными ресурсами на пути к получателю будет иметь минимальное вмешательство со стороны потоков данных негарантированной доставки.

Архитектура дифференцированных служб

Модель DiffServ обеспечивает дифференцированное качество обслуживания QoS различным типам данных приложений путем отнесения потоков данных к различным классам обслуживания.

Архитектура дифференцированных служб предлагает использование строго определенного набора элементарных блоков, на основе которых создаются различные типы служб. В этой архитектуре каждый пакет переносит в своем заголовке информацию, которая используется на каждом переходе для выбора этому пакету индивидуального способа пересылки.

Архитектура модели DiffServ задает стандартные комбинации битов в байте DiffServ и для каждой из них определяет свой способ пересылки, называемый стратегией на отдельном переходе (per-hop behavior). Обработка по принципу негарантированной доставки, которая используется в настоящее время в Internet, является одним из возможных способов пересылки данных.

Архитектура DiffServ обеспечивает структуру, в которой провайдеры служб могут предложить своим клиентам ряд сетевых служб, дифференцированных по уровню производительности. Пользователь может выбрать требуемый ему уровень производительности для отдельных пакетов; для этого достаточно установить в пакете соответствующее значение поля кодовой точки дифференцированных служб (Differentiated Services Code Point — DSCP).

Байт дифференцированных служб

IP-очередность при отбрасывании использует три бита очередности в поле ToS заголовка протокола IPv4 для задания класса обслуживания каждому пакету.

Группа дифференцированных служб при IETF стандартизовала использование 6 битов байта ToS IP-заголовка для кодовой точки DSCP. Младшие 2 бита в настоящее время не используются (currently unused — CU). Кодовая точка DSCP представляет собой расширение 3-х битов, используемых IP-очередностью.

Аналогично IP-очередности при отбрасывании использование кодовой точки DSCP обеспечивает дифференцированное обслуживание соответствующим образом

помеченным пакетам. При стандартизации поля DSCP байт ToS был переименован в байт дифференцированных служб (DS byte). 6-битовый шаблон для кодовой точки (DSCP) в DS-байте, определенный в RFC 2474, показан на рис. 59.3.

Кодовая точка дифференцированных служб (DSCP): 6 бит
Сейчас не используется (CU): 2 бит

Рис. 59.3. Кодовая точка DSCP, определенная в RFC 2474

Классификация: идентификация потоков

Для того, чтобы предоставить некоторым потокам повышенный приоритет, их необходимо идентифицировать и (при желании) пометить (снабдить меткой). Эти две задачи обычно называют *классификацией (classification)*.

Исторически сложилось так, что идентификация осуществлялась с использованием списков управления доступом (access control list — ACL). Списки ACL идентифицируют потоки данных для таких механизмов управления переполнением, как PQ-очередность и CQ-очередность. Поскольку очередности PQ и CQ устанавливаются на маршрутизаторах только в рамках одного перехода (т.е. приоритеты качества обслуживания QoS относятся лишь к данному маршрутизатору и не передаются следующим на маршруте маршрутизаторам), идентификация пакета используется только на одном маршрутизаторе. В некоторых случаях классификация CBWFQ также относится только к одному маршрутизатору. Такой подход противоположен установке битов IP-очередности.

Для установки очередности, основанной на классификации по расширенным спискам доступа, могут быть использованы такие функции, как маршрутизация, основанная на политиках и согласованная скорость передачи CAR. Это обеспечивает значительную гибкость при назначении очередности, в частности ее назначение в зависимости от приложения или пользователя, от подсети получателя или отправителя и т.д. Обычно эти функции применяются как можно ближе к границе сети (или административного домена), с тем чтобы каждый последующий сетевой элемент мог предоставить службу, основанную на определенной ранее политике.

Для более подробной идентификации потоков данных используется основанное на типе сети распознавание приложения (Network-based application recognition — NBAR). Например, могут быть идентифицированы адреса URL в пакете протокола HTTP. Как только пакет идентифицирован, он может быть помечен путем задания ему приоритета.

Задание политики QoS и основанная на политике маршрутизация

Основанная на политике маршрутизация IOS Cisco (Cisco IOS Policy-Based Routing — PBR) позволяет классифицировать потоки данных на основе критериев расширенных списков доступа, установить биты очередности протокола IP и даже направить эти потоки по маршрутам, выбранным в результате перераспределения потоков, которое может потребоваться для обеспечения требуемого QoS при передаче данных по сети. Путем установки уровней очередности для входных потоков данных и использования их вместе с механизмами очередности, описанными выше в настоящей главе, можно

создать дифференцированную службу. Эти механизмы предоставляют мощные, простые и гибкие варианты реализации политик QoS в сети пользователя.

При использовании основанной на политике маршрутизации происходит преобразование маршрутов для того, чтобы они удовлетворяли определенным критериям потоков. После того, как удовлетворены требования списков доступа, а происходит установка битов очередности.

Следует разделять возможность установки IP-очередности и первичную способность маршрутизации PBR маршрутизировать пакеты на основе сконфигурированных политик. Некоторые приложения или потоки данных могут использовать в разных ситуациях конкретные типы QoS-маршрутизации, например, передавать в течение короткого времени информацию фондовой биржи в корпоративный офис по более дорогостоящему, но имеющему большую полосу пропускания каналу и одновременно продолжая передавать обычные данные приложений, такие как сообщения электронной почты, по недорогим каналам с небольшой полосой пропускания. Маршрутизация PBR может быть использована для направления пакетов по маршрутам, отличающимся от тех, которые были выбраны протоколами маршрутизации. Она предоставляет более гибкие средства маршрутизации пакетов, дополняя существующие механизмы протоколов маршрутизации.

Использование преобразования маршрутов также дает возможность идентифицировать пакеты на основе атрибутов протокола граничного шлюза (Border Gateway Protocol — BGP), таких как списки сообществ и маршруты автономных систем AS Такая идентификация известна как *распространение политики QoS при посредстве протокола граничного шлюза (QoS policy propagation via Border Gateway Protocol)*.

Согласованная скорость передачи CAR: установка IP-очередности

Функция согласования скорости передачи CAR в некоторых аспектах аналогична маршрутизации PBR. Она позволяет классифицировать потоки данных на входном интерфейсе, а также выполнить спецификацию политик для обработки потоков данных, которым требуется полоса пропускания, превышающая выделенную. Функция CAR просматривает данные, полученные на некотором интерфейсе или подмножество таких данных, выбранное на основе критериев списка доступа, сравнивает их скорость передачи со скоростью маркеров в сконфигурированном контейнере и на основе этого сравнения принимает решение о том, какие действия следует предпринять (например, отбросить пакеты или изменить IP-очередность).

Имеет место некоторая путаница при использовании CAR для установки битов IP-очередности. Ниже сделана попытка внести ясность в этот вопрос. Как показано далее в настоящей главе, маршрутизация CAR (что видно из ее названия) используется для передачи потоков данных с *согласованной скоростью передачи (committed access rate)*. Это делается с помощью контейнера маркеров (token bucket). Контейнер маркеров содержит маркеры, каждый из которых соответствует одному байту данных (1 маркер = 1 байт). Контейнер заполняется маркерами со скоростью, сконфигурированной пользователем. Когда поступают пакеты для последующей отправки, система просматривает содержимое контейнера на предмет наличия в нем маркеров. Если количество маркеров в контейнере соответствует размеру пакетов, то маркеры удаляются и пакет передается (в этом случае говорят,

что пакет *соответствует условиям [conforms]*). Если количество маркеров в контейнере меньше размера пакета, то он отбрасывается (в этом случае говорят, что пакет является *избыточным — exceeds*).

При использовании CAR-реализации в операционной системе IOS Cisco кроме передачи пакета или отбрасывания его имеется много других возможных вариантов действий. Одним из таких вариантов является установка битов IP-очередности. Если обе операции — "conform" и " exceed" указывают на необходимость установки одних и тех же значений битов очередности, то выполняется уже не функция выбора политики, а просто используется метод установки битов IP-очередности.

На рис. 59.4. показан процесс принятия решения о согласованной скорости передачи. Любой пакет, находящийся ниже этой скорости передачи, соответствует заданным условиям. Пакеты, находящиеся выше скорости передачи, являются избыточными. В приведенном примере предписываемое действие для обоих случаев состоит в установке set prec = 5. В этом случае скорость передачи не имеет значения, а функция CAR просто используется для установки битов очередности.

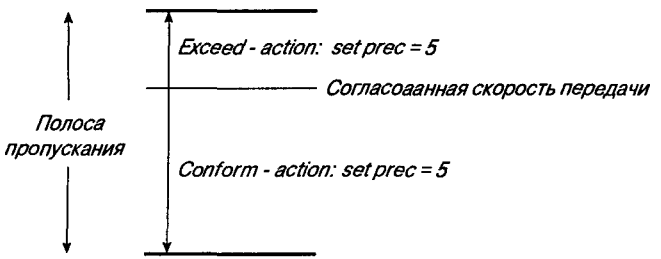


Рис. 59.4. Принятие решения о согласованной скорости передачи.

При установке IP-очередности на узле или в сети пользователя эта установка может использоваться по желанию пользователя; однако она может быть изменена политикой, определенной в сети. IP-очередность позволяет установить классы обслуживания с использованием уже существующих в сети механизмов задания очередности (например, WFQ или WRED), без внесения изменений в уже существующие приложения или сложные требования сети. Следует отметить, что этот подход может быть легко распространен на протокол IPv6 путем использования поля приоритета (Priority field).

Для решения этой задачи программное обеспечение IOS Cisco использует преимущества сквозной природы протокола IP путем наложения зависящей от технологии 2-го уровня QoS-сигнализации на методы 3-го уровня IP-сигнализации QoS протокола RSVP и IP-очередности.

Платформа Cisco 7500

Программное обеспечение IOS Cisco также обеспечиваст распределенную согласованную скорость доступа (Distributed Committed Access Rate — D-CAR) на процессорах универсального интерфейса (Versatile Interface Processor — VIP) платформы 7500. Функция D-CAR может быть использована для установки битов IP-очередности точно таким же образом, как и функция CAR. Она может также поместить пакеты в группы QoS, которые используются в основанной на классах очередности D-WFQ, а также для задания политики в D-CAR.

NBAR: динамическая идентификация потоков

Новейшим методом классификации, разработанным корпорацией Cisco, является распознавание приложений на основе типа сети (Network-Based Application Recognition — NBAR) Строго говоря, в настоящее время метод NBAR является только инструментом идентификации, однако в настоящем изложении он будет рассматриваться как метод классификации. Как и во всяком механизме классификации, наиболее сложной частью является идентификация потоков данных. Маркировка пакетов относительно проста. Функция NBAR переносит идентификацию (которая является частью классификации) на другой уровень. При более глубоком анализе содержимого пакета идентификация может быть выполнена, например, по адресу URL или по типу MIME HTTP-пакета. Эта возможность становится существенной по мере того, как все большее количество приложений начинает базироваться на Web-технологиях.

В этом случае возникает необходимость различать заказ на передачу данных и обычную Web-навигацию. Кроме того, функция NBAR может идентифицировать различные приложения используя виртуальные порты. NBAR делает это, просматривая управляющие пакеты с целью определения портов, на которые приложение решает отправить данные.

NBAR имеет две представляющие большой интерес дополнительные функции, которые делают ее исключительно ценной. Одна из них состоит в способности NBAR определить используемый протокол. Это позволяет ей упорядочивать на интерфейсе данные различных протоколов. Функция NBAR составляет список протоколов, которые она может идентифицировать, и предоставляет статистику по каждому из них. Второй функцией является использование модуля языкового описания пакета (Packet Description Language Module — PDLM), который позволяет легко добавлять дополнительные протоколы к имеющемуся у NBAR списку идентифицируемых протоколов. Эти модули создаются и загружаются во флэш-память, которая, в свою очередь, загружается в RAM. Использование модулей PDLM позволяет добавлять к этому списку идентифицируемых протоколов дополнительные протоколы без замены версии IOS на более позднюю и без перезагрузки маршрутизатора.

Внимание!

Хотя NBAR лишь идентифицирует пакеты, они могут быть также и помечены с помощью установки битов IP-очередности.

Средства управления переполнением

Одним из способов, используемых сетевыми элементами для предотвращения переполнения, является применение какого-либо алгоритма очередности для сортировки потоков данных и выбор одного из методов задания приоритетов на выходных каналах. Программное обеспечение IOS Cisco позволяет использовать несколько методов организации очереди, описанных ниже.

- Очередь "первым вошел — первым вышел" (First-In, First-Out — FIFO).
- Приоритетная очередность (Priority Queuing — PQ).
- Настраиваемая очередность (Custom Queuing — CQ).

- Основанная на потоках справедливая взвешенная очередность (Weighted Fair Queuing — WFQ).
- Основанная на классах справедливая взвешенная очередность (Class-Based Weighted Fair Queuing — CBWFQ).

Каждый алгоритм очередности предназначен для решения определенной задачи сетевого обмена и по-своему влияет на производительность сети.

Примечание

Алгоритмы очередности работают в случае переполнения. По определению, если канал не перегружен, то нет необходимости помещать пакеты в очередь. В отсутствие переполнения все пакеты поступают непосредственно на интерфейс.

Очередность FIFO: простейший способ промежуточного хранения

Простейшая очередь FIFO заключается в сохранении пакетов, если сеть перегружена, и их передаче в порядке поступления, когда сеть больше не перегружена. Иногда FIFO является стандартным алгоритмом установки очередности и, таким образом, не требует настройки, но у такого подхода есть ряд недостатков. Прежде всего очередь FIFO не решает вопросы приоритетности пакета; выделение полосы пропускания, скорость передачи и выделение места в буфере определяются порядком поступления пакетов. FIFO также не обеспечивает защиту от некорректно работающих приложений (источников). Источники, генерирующие всплески при передаче данных, могут вызывать большие задержки при доставке чувствительных ко времени данных и, возможно, управляющих и сигнальных сообщений. Очередь FIFO была необходимым первым шагом в управлении сетевым потоком, но современные интеллектуальные сети нуждаются в более сложных алгоритмах. Кроме того, заполнение очереди приводит к отбрасыванию концевых пакетов, а это нежелательно, потому что отброшенный пакет может иметь высокий приоритет. Маршрутизатор не может предотвратить отбрасывание этого пакета, так как для него в очереди нет места (не говоря о том, что FIFO не отличает пакеты с высоким приоритетом от пакетов с низким приоритетом). В программном обеспечении Cisco IOS реализованы алгоритмы очередности, лишенные недостатков FIFO.

PQ: задание данным приоритетов

Алгоритм *приоритетной очередности (Priority Queuing — PQ)* обеспечивает первоочередную обработку важных данных в каждой точке, где он используется. Приоритетная очередность может гибко изменяться в соответствии с сетевым протоколом (IP, IPX или AppleTalk), входящим интерфейсом, размером пакета, адресом источника или приемника и т.п. При использовании очередности PQ каждый пакет помещается в одну из четырех очередей, в зависимости от присвоенного ему приоритета — высокого, среднего, нормального или низкого. Пакеты, не классифицированные по этой системе, попадают в нормальную очередь (рис. 59.5). При передаче алгоритм оказывает абсолютное предпочтение очередям высшего приоритета по сравнению с очередями низкого приоритета.

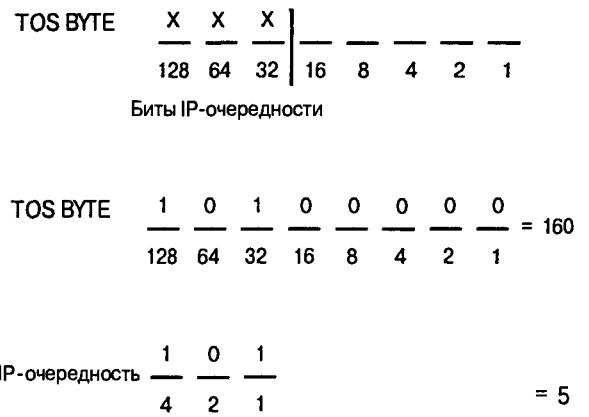


Рис. 59.5. Алгоритм приоритетной очередности помещает данные в одну из четырех очередей: высокого, среднего, нормального или низкого приоритета

Применение очередности PQ полезно в тех случаях, когда требуется гарантировать приоритетную передачу критически важных данных по различным каналам распределенных сетей WAN. Например, в продуктах Cisco PQ обеспечивается доставка важных отчетов по продажам на базе Oracle ранее других, менее важных данных. В настоящее время в PQ применяется статическая конфигурация, поэтому этот метод не может автоматически адаптироваться к изменяющимся требованиям сети.

CQ: гарантированная полоса пропускания

Назначение алгоритма *настраиваемая очередность (Custom Queuing — CQ)* состоит в совместном использовании сети приложениями, требующими гарантированной минимальной полосы пропускания или задержки, не превышающей некоего заданного максимума. В таких средах полоса пропускания должна быть пропорционально распределена между приложениями и пользователями. Эта функция Cisco CQ обеспечивает гарантированную полосу пропускания в потенциальной точке перегрузки, предоставляя каждому виду данных фиксированную часть доступной полосы пропускания. Остаток распределяется между другими типами данных. Каждому классу пакетов в настраиваемой очереди отводится определенная часть очереди, после чего очередь обслуживается циклически (рис. 59.6).

Например, передача инкапсулированных данных архитектуры системной сетевой архитектуры (Systems Network Architecture — SNA) требует гарантированного минимального уровня обслуживания. В этом случае можно зарезервировать половину доступной полосы пропускания для данных протокола SNA, а оставшуюся половину отдать другим протоколам, таким, например, как IP и IPX (Internet Packet Exchange).

Алгоритм очередности размещает сообщения в одной из 17 очередей (очередь 0 предназначена для системных сообщений, таких как сообщения об активности и сигнализация) и освобождает эти очереди согласно взвешенному приоритету. Маршрутизатор циклически обслуживает очереди с 1 по 16, извлекая в течение каждого цикла определенное количество байтов из каждой очереди. Такая особенность гарантирует, что никакое приложение (или группа приложений) не получит больше заранее определенной части полосы пропускания в случае большой нагрузки

на канал. Подобно PQ, очередность CQ конфигурируется статически и не адаптируется автоматически к изменениям условий в сети.

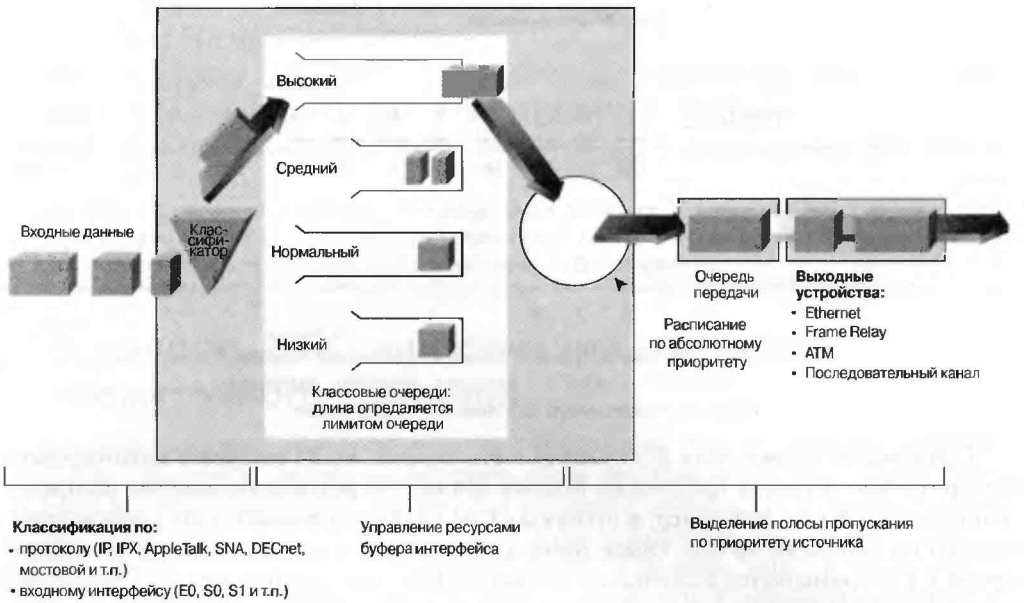


Рис. 59.6. Настраиваемая очередь обрабатывает потоки данных, предоставляя определенное место каждому классу пакетов и затем обслуживая до 17 очередей по кругу

Основанная на потоках очередность WFQ: создание равноправных потоков

В тех случаях, когда желательно обеспечить быстрый отклик как для крупных, так и для мелких сетевых пользователей, не увеличивая полосу пропускания, можно применить основанную на потоках взвешенную справедливую очередность (Weighted Fair Queueing — WFQ), обычно называемую просто очередностью WFQ. WFQ — одна из первых технологий очередности, разработанных корпорацией Cisco. Это потоковый алгоритм очередности, который устанавливает "битовое равенство", поскольку в одном цикле обслуживает равное количество байтов из каждой очереди. Например, если в 1-й очереди номер находятся 100-байтовые пакеты, а во 2-й очереди номер — 50-байтовые, то согласно алгоритму WFQ в каждом цикле будут выбираться два пакета из очереди 2 и один из очереди 1. Таким образом, все очереди обслуживаются равноправно — каждый раз из них выбирается по 100 байтов.

Алгоритм WFQ исключает нехватку полосы пропускания для очередей и обеспечивает предсказуемое обслуживание данных. Потоки с низкой плотностью передачи данных — а таких большинство — обслуживаются чаще и из них передается столько же байтов, сколько из потоков с высокой плотностью передачи. Это выглядит как режим благоприятствования для потоков малой плотности, однако в действительности является просто установлением равноправия (рис. 59.7).

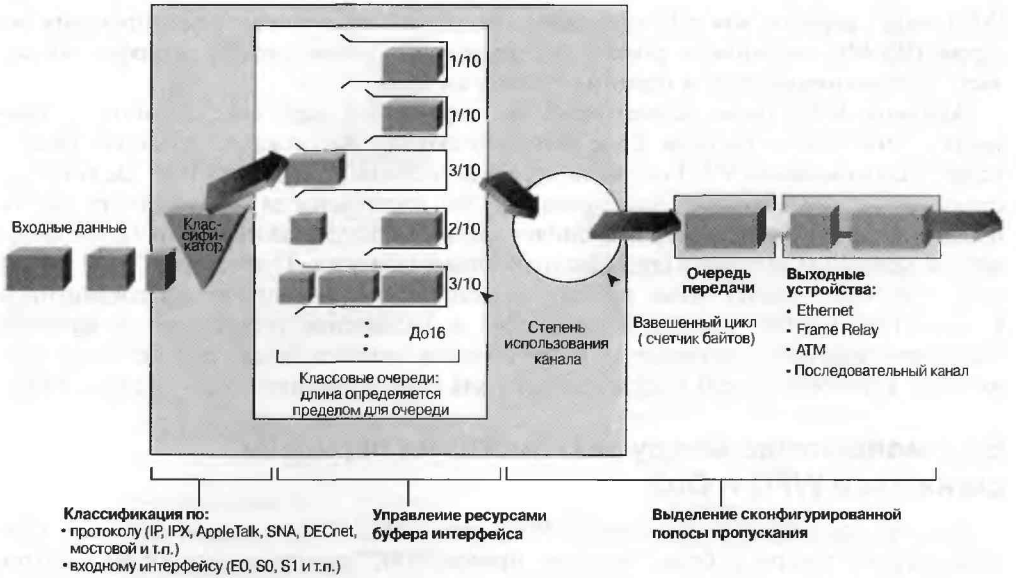


Рис. 59.7. При интенсивном обмене данными применение WFQ обеспечивает гораздо более предсказуемые скорость передачи и интервал между двумя приемами данных

Одной из целей создания очередности WFQ было сведение к минимуму усилий по конфигурированию за счет автоматической адаптации к изменяющимся условиям прохождения данных по сети. В действительности очередность WFQ столь хорошо подходит для многих приложений, что в большинстве последовательных интерфейсов, работающих на скоростях E1 (2048 Мбит/с) и ниже она используется по умолчанию.

Потоковая очередность WFQ создает *потоки* на основе ряда характеристик пакета. Каждому потоку (называемому также *диалогом*) предоставляется отдельная очередь для буферизации в случае перегрузки. В последующем изложении понятия потока, диалога и очереди используются как синонимы.

Примечание

Общими характеристиками, определяющими поток, являются адреса источника и приемника, номера сокетов и идентификаторы сеанса. Точные критерии, определяющие поток, описываются в технической документации Cisco Systems (http://www.cisco.com). Следует отметить, что для разных протоколов используются разные критерии.

Связанная с заданием весов часть алгоритма WFQ для улучшенного обслуживания определенных очередей опирается на использование битов IP-очередности. Используя значения от 0 до 5 (значения 6 и 7 зарезервированы), WFQ с помощью своего алгоритма определяет, какой уровень обслуживания предоставить очереди. Подробнее такой процесс описывается в следующем ниже разделе "Взаимодействие между технологиями передачи сигналов WFQ и QoS".

Эффективность использования WFQ достигается за счет возможности передавать данные из потоков с низким приоритетом, если потоки с высоким приоритетом отсутствуют. В этом очередность WFQ отличается от обычной мультиплексной передачи с разделением времени (Time-Division Multiplexing — TDM), в которой полоса пропускания просто делится и, если данные определенного типа отсутствуют, не используется.

WFQ может работать как с IP-приоритетами, так и с протоколом резервирования ресурсов (RSVP), описанными далее в этой главе, обеспечивая дифференцированное качество обслуживания QoS и гарантированные службы.

Алгоритм WFQ также решает проблему переменной задержки, связанной с подтверждением приема сигнала. Если ведется несколько интенсивных диалогов, то благодаря использованию WFQ скорость передачи и время между поступлением сигналов становятся гораздо более предсказуемыми. Это достигается за счет битового равноправия. Если в последовательных циклах диалоги обслуживаются устойчивым образом, то колебание задержки (дребезжание) стабилизируется. Применение WFQ значительно улучшает работу таких алгоритмов, как управление логическим соединением (Logical Link Control — LLC) в сетях SNA и управление перегрузкой и функции "затяжного старта" в протоколе TCP. Результатом является более предсказуемые пропускная способность сети и время отклика для каждого активного потока (рис. 59.8).

Взаимодействие между технологиями передачи сигналов в WFQ и QoS

Как уже упоминалось, очередность WFQ распознает IP-приоритеты, благодаря чему обнаруживает пакеты с более высоким приоритетом, маркированные IP-источником, и обрабатывает их быстрее, обеспечивая таким данным уменьшенное время отклика. Эта часть алгоритма WFQ относится к заданию весов. Поле IP-приоритета принимает значения от 0 (по умолчанию) до 7 (значения 6 и 7 зарезервированы и обычно не устанавливаются сетевым администратором). Чем выше приоритет, тем большую полосу пропускания выделяет алгоритм для данного диалога, чтобы обеспечить ему ускоренное обслуживание в случае перегрузки. WFQ присваивает вес каждому потоку, что определяет порядок передачи пакетов из очереди. По такой схеме чем ниже вес, тем скорее обслуживается поток. IP-приоритет стоит в знаменателе этого весового коэффициента. Например, данные с IP-приоритетом, равным 7, получают более низкий вес, чем данные с IP-приоритетом, равным 3, и, таким образом, имеют перед ним преимущество при передаче.

Примечание

Вес представляет собой значение, вычисляемое на основании IP-очередности пакета в потоке. По весу алгоритм WFQ определяет последовательность обслуживания пакетов.

Вес = (4096 / (IP-приоритет + 1)

Вес = (32384 / (IP-приоритет + 1)

В версии v12.0 числитель изменился с 4096 на 32384.

Для просмотра весов используется команда **show queue** *<интерфейс>*.

Результат назначения IP-очередности

Если на каждом уровне IP-приоритета в интерфейсе есть только один поток, то каждому потоку будет выделена часть канала, равная его приоритету + 1:

1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 = 36

Потоки получат 8/36, 7/36, 6/36, 5/36 и т.д.полосы пропускания канала. Однако если на всех уровнях по одному потоку, а на одном — 18, то формула будет выглядеть следующим образом:

1 + 18×2 + 3 + 4 + 5 + 6 + 7 + 8 = 36 - 2 + 18×2 = 70

Потоки получат 8/70, 7/70, 6/70, 5/70, 4/70, 3/70, 2/70 и 1/70 канала, а каждый из 18 потоков получит приблизительно по 2/70 канала.

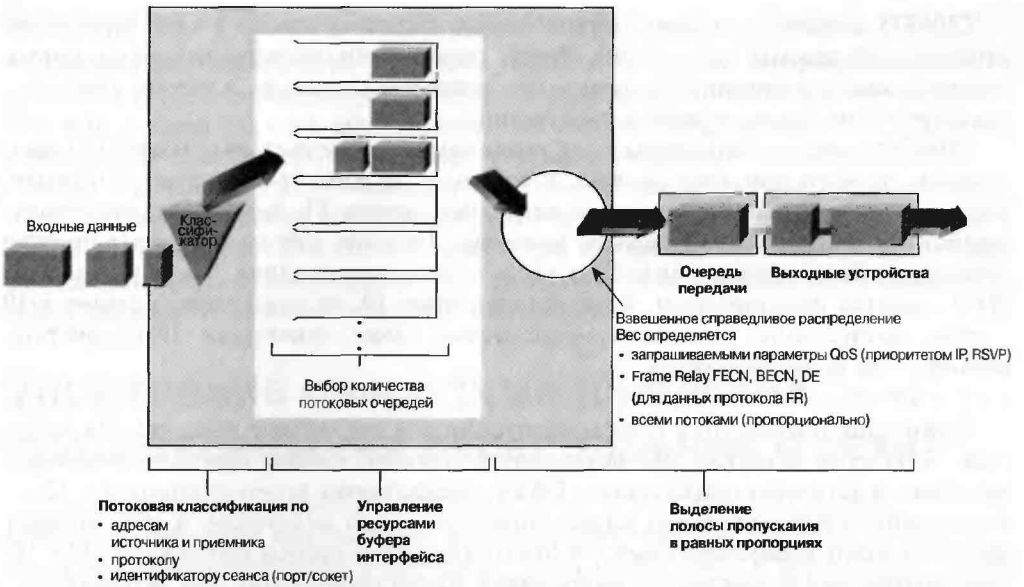


Рис. 59.8. Пример интерактивной задержки потоков данных (канал WAN-сети, Frame Relay, 128 Кбит/с)

Алгоритм WFQ также поддерживает использование протокола RSVP. Протокол RSVP использует очередность WFQ для выделения буферов и планирования передачи пакетов, что гарантирует полосу пропускания для зарезервированных потоков. Кроме того, в сетях Frame Relay для уведомления о перегрузке используется установка в сообщениях битов FECN и BECN. При прохождении данных через коммутирующий модуль Frame Relay, бит очередности при отбрасывании (DE), биты FECN и BECN фрейма влияют на установленные значения весов WFQ. В случае установки битов переполнения веса, используемые алгоритмом, изменяются так, чтобы данные диалога, испытывающего перегрузку, передавался реже.

Платформа 7500

Программное обеспечение Cisco IOS также обеспечивает распределенную взвешенную равноправную очередность (Distributed Weighted Fair Queuing — D-WFQ), которая представляет собой скоростную версию WFQ, работающую на распределенных процессорах VIP. Алгоритм D-WFQ обеспечивает два типа WFQ: потоковую (основанную на потоках) равноправную очередность и классовую (основанную на классах) равноправную очередность. Потоковый вариант D-WFQ отличается от WFQ тем, что не распознает установленные IP-приоритеты и, таким образом, не присваивает веса потокам.

Основанная на классах очередность WFQ: гарантированная полоса пропускания

Алгоритм основанной на классах очередности WFQ (Class-Based WFQ — CBWFQ) представляет собой одну из последних разработок Cisco для более гибкого управления перегрузкой. Очередность CBWFQ обеспечивает минимальную полосу пропускания, в отличие от CAR и механизмов формирования потоков, обеспечивающих максимальную полосу пропускания.

CBWFQ позволяет сетевому администратору создавать классы с гарантированной минимальной полосой пропускания. Вместо организации очереди для каждого потока создается класс, состоящий из одного или нескольких потоков. Каждому классу гарантируется минимальная полоса пропускания.

CBWFQ может использоваться для предотвращения подавления одного потока с высоким приоритетом несколькими потоками с низким приоритетом. Например, поток видео, требующий половину полосы пропускания T1, получит ее при использовании WFQ, только если потоков всего два. По мере добавления новых потоков видеопоток будет получать меньшую часть полосы пропускания, так как механизм WFQ является равноправным. Если потоков будет 10, то видеопоток получит 1/10 полосы пропускания, чего явно недостаточно. Даже присвоение IP-приоритета, равного 5, не решит проблемы.

$1 \times 9 + 6 = 15$

Видеопоток получит 6/15 полосы пропускания, а это меньше того, что ему требуется. Необходим механизм, обеспечивающий половину полосы пропускания для видеопотока и установка очередности CBWFQ предоставляет такую возможность. Сетевой администратор определяет класс, помещает в него видеопоток и дает команду маршрутизатору предоставить ему 768 Кбит/с (половина полосы пропускания T1). Теперь видеопотоку предоставлена необходимая полоса пропускания. Для остальных потоков используется основной класс. Этот класс обслуживается по потоковым схемам очередности WFQ, распределяющим остаток полосы пропускания (в данном случае, вторую половину T1) между потоками.

Примечание

Сказанное выше *не означает*, что использование алгоритма WFQ нецелесообразно. Очередность WFQ является прекрасным средством управления перегрузкой (из-за чего и используется по умолчанию в интерфейсах E1 и ниже). Рассмотренный пример был приведен с целью показать ситуацию, в которой эффективно работает CBWFQ.

Кроме того, может быть назначена очередь с малой задержкой (Low-Latency Queue — LLQ), которая является очередью, основанной на приоритетах. Эта функция также называется приоритетной очередью в системе взвешенной классовой равноправной очередности (Priority Queue Class-Based Weighted Fair Queuing — PQCBWFQ).

Использование очереди с малой задержкой позволяет обслуживать класс как очередь со строго определенным приоритетом. Данные этого класса обслуживаются раньше всех остальных классов. При этом резервируется определенная часть полосы пропускания. Любые данные, выходящие за пределы этой полосы пропускания отбрасываются. Без CBWFQ аналогичное обслуживание возможно только для данных протокола RTP с использованием IP-приоритета RTP (также называемого PQWFQ) или резервирование IP RTP.

Примечание

CBWFQ позволяет зарезервировать для определенного класса минимальную полосу пропускания. Если доступна большая полоса пропускания, то класс может ее использовать. Однако в любом случае ему гарантирована минимальная полоса пропускания. Если же класс не использует гарантированную ему полосу пропускания, то ее могут занять другие приложения.

Платформа 7500

Программное обеспечение IOS Cisco также обеспечивает распределенную основанную на классах справедливую взвешенную очередность (которая так же называется D-WFQ), которая является высокоскоростной версией WFQ, работающей на распределенных VIP-процессорах. Основанная на классах очередность D-WFQ отличается от CBWFQ тем, что использует иной синтаксис команд, однако по существу реализует ту же самую службу. Кроме обеспечения гарантированной полосы пропускания основанная на классах WFQ в D-WFQ может при соответствующем конфигурировании распознавать биты IP-очередности, что отсутствует в основанной на потоках WFQ (такая очередность называется основанной на ToS).

Управление очередями (средства предотвращения переполнения в сети)

Предотвращение переполнения является формой управления очередями. *Методы устранения перегрузок* контролируют интенсивность передачи данных в сети и стремятся предвидеть перегрузки в типичных "узких местах" сети и избегать их, в отличие от методов управления перегрузкой, которые берут на себя контроль перегрузки *после* того, как она произойдет. Основным средством IOS по предотвращению перегрузок в Cisco IOS является взвешенное случайное раннее выявление (Weighted Random Early Detection — WRED).

WRED: устранение перегрузок

Целью алгоритмов *случайного раннего обнаружения (Random Early Detection RED)* является предотвращение перегрузок в объединенных сетях прежде, чем они реально возникнут. Алгоритмы RED следят за интенсивностью передачи данных в контрольных точках сети и случайным образом отбрасывают пакеты в случае возникновения признаков переполнения. Результатом отбрасывания является то, что источник обнаруживает отброшенные данные и замедляет их передачу. Первоначально алгоритмы RED предназначались для протокола TCP в IP-средах.

Взаимодействие алгоритма WRED и технологий сигнализации QoS

Алгоритм WRED сочетает в себе возможности алгоритма RED и IP-приоритеты. Это сочетание обеспечивает возможность привилегированной обработки пакетов с высоким приоритетом. При этом могут избирательно отбрасываться данные с низким приоритетом, когда на интерфейсе появляются признаки перегрузки и обеспечивает дифференцированные параметры производительности для разных классов обслуживания (рис. 59.9). Алгоритм WRED также поддерживает использование протокола RSVP и может предоставлять интегрированные службы управляемой нагрузки QoS.

В каждой очереди есть возможность разместить лишь ограниченное количество пакетов. Переполнение очереди может привести к отбрасыванию последних пакетов. Это весьма нежелательно, поскольку отброшенные пакеты могут иметь высокий приоритет, а маршрутизатор не сможет поместить их в очередь. Если очередь не заполнена,

маршрутизатор может определить приоритет поступающих пакетов и отбрасывать пакеты с низким приоритетом, пропуская пакеты с высоким приоритетом.

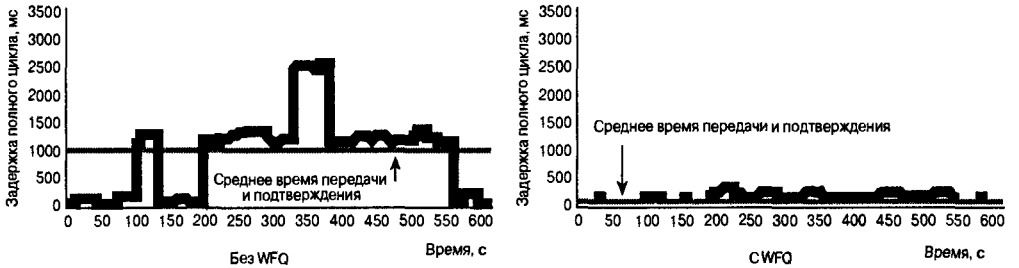


Рис. 59.9. WRED предусматривает случайное отбрасывание пакетов при повышении нагрузки

Контролируя глубину очереди (количество пакетов в ней) путем отбрасывания тех или иных пакетов, маршрутизатор делает все возможное, чтобы избежать переполнения очереди и отбрасывания последних пакетов. Это позволяет маршрутизатору отобрать пакеты, которые можно отбросить в случае заполнения очереди. Алгоритм WRED также дает возможность избежать общей перегрузки в объединенной сети. WRED использует минимальные пороговые величины для каждого уровня IP-приоритета, чтобы определить, когда пакет может быть отброшен (при превышении порога пакет становится кандидатом на отбрасывание.)
Рассмотрим следующий пример.
Глубина очереди: 21 пакет
Минимальный порог отбрасывания для IP-приоритета, равного 0: 20
Минимальный порог отбрасывания для IP-приоритета равного 1: 22

Поскольку минимальный порог отбрасывания для IP-приоритета, равного 0, превышен, такие пакеты в случае возникновении переполнения могут быть отброшены. Однако минимальный порог отбрасывания для IP-приоритета, равного 1, превышен не был, следовательно, эти пакеты отброшены не будут. Если глубина очереди превысит 22, то пакеты с IP-приоритетом, равным 1, также могут быть отброшены. WRED использует алгоритм, который повышает вероятность отбрасывания пакета при увеличении глубины очереди от минимального порога отбрасывания до максимального. При превышении максимального порога все пакеты отбрасываются.

Потоковый RED: RED для потоков, не совместимых с TCP

Алгоритм WRED предназначается в первую очередь для TCP-потоков с обратной передачей в случае отбрасывания пакета. Но существуют пакеты, не совместимые с TCP, где нет такой обратной передачи. Для обработки таких потоков используется потоковый алгоритм RED. Этот подход заключается в повышении вероятности отбрасывания, если поток превышает пороговое значение.

Для предотвращения последовательного отбрасывания (linear dumping) пакетов потоковый алгоритм WRED использует следующие два метода:

- Классификация входящих данных и разделение их на потоки в зависимости от таких параметров, как адреса и порты источника и получателя.

- Поддержка состояния активных потоков, т.е. тех, пакеты которых находятся в выходных очередях.

Эта классификация и информация о состоянии используется в потоковом WRED для того, чтобы ни один поток не занимал больше ресурсов выходного буфера, чем ему выделено. Потоковый алгоритм WRED определяет, какие потоки монополизируют ресурсы, и применяет к ним более жесткие ограничения.

Алгоритм WRED гарантирует равноправие потоков путем подсчета количества активных потоков, существующих на выходном интерфейсе. Зная число активных потоков и размер выходной очереди, алгоритм WRED определяет количество буферов, доступных для каждого потока.

На случай всплесков при передаче данных алгоритм WRED умножает количество буферов, доступных для каждого потока, на заранее определенный коэффициент и позволяет каждому активному потоку иметь определенное количество пакетов в выходной очереди. Этот коэффициент масштабирования один для всех потоков. Результатом такого увеличенного количества буферов становится установка лимита буферов на один поток. Если поток превышает свой лимит, то вероятность отбрасывания пакетов данного потока возрастает.

Платформа 7500

Программное обеспечение Cisco IOS также обеспечивает распределенное взвешенное случайное раннее распознавание (D-WRED) — скоростную версию WRED, работающую на распределенных VIP-процессорах. Алгоритм D-WRED обеспечивает те же функции, что и WRED, такие как максимальное и минимальное пороговое значения для длины очереди и возможность отбрасывания для каждого класса обслуживания.

Примечание

Хотя IOS позволяет изменять максимальную и минимальную длину очереди и условия отбрасывания, однако изменять стандартные значения этих параметров не рекомендуется. При необходимости изменить их рекомендуется проконсультироваться у специалистов по технической поддержке корпорации Cisco.

Средства формирования потоков и конфигурирования политик

В состав программного обеспечения Cisco QoS входят два средства формирования потоков для управления передачей данных и перегрузкой в сети: общее формирование потоков (Generic Traffic Shaping — GTS) и формирование потоков Frame Relay (Frame Relay Traffic Shaping — FRTS). Средством конфигурирования политик в IOS Cisco является функция согласованной скорости доступа (Committed Access Rate — CAR). Возможности CAR по классификации были описаны выше, в разделе "Согласованная скорость передачи CAR: установка IP-очередности". Ниже будут рассмотрены возможности CAR по конфигурированию политик.

CAR: политики доступа к полосе пропускания

Как отмечалось выше, базовая функция качества обслуживания QoS состоит в назначении потокам приоритетного обслуживания за счет повышения приоритета одного потока или понижения приоритета другого. Функция CAR используется для ограничения полосы пропускания одного потока в пользу другого.

Ранее в данной главе, в разделе "Классификация", была описана основная маркерная ячейка. Согласно этому описанию, пакеты, соответствующие условиям передачи, передаются, а избыточные — отбрасываются.

Версия CAR, реализованная в IOS Cisco, предусматривает несколько возможных действий: передачу, отбрасывание, установку битов IP-приоритета и продолжение передачи (последнее относится к каскадным операторам CAR). Такая гибкость допускает несколько способов воздействия на передачу данных. Ниже приводятся некоторые возможные варианты.

- Согласованному потоку данных может быть присвоен IP-приоритет, равный 5, а избыточные потоки данных могут быть отброшены.
- Согласованный поток данных может быть передан с IP-приоритетом, равным 5, а избыточный поток данных также может быть передан, но с IP-приоритетом, равным 1.
- Согласованный поток данных может быть передан, а избыточный поток данных переклассифицирован с уменьшением IP-приоритета, а затем передан следующему оператору CAR для учета дополнительных условий.

Реализация CAR в Cisco IOS также обеспечивает дополнительную маркерную ячейку. В нее помещаются дополнительные маркеры сверх исходной (нормальной) маркерной ячейки. При использовании этих маркеров возникает вероятность отбрасывания пакета (даже если поступила команда передачи). При этом используется алгоритм, аналогичный алгоритму RED, согласно которому, чем больше используется маркеров из этой ячейки, тем выше вероятность отбрасывания следующего пакета. Это позволяет медленно снизить интенсивность потока, как в алгоритме WRED, не отказываясь от возможности передать пакетов больше, чем позволяет нормальная маркерная ячейка.

Общее формирование потоков GTS: управление исходящим потоком данных

Общее формирование потоков (Generic Traffic Shaping — GTS) предоставляет способ управления потоком данных, проходящим через данный интерфейс. Он сокращает исходящий поток данных для предотвращения переполнения за счет ограничения потоков данных выбранного типа до указанной скорости передачи в битах (используется также метод маркерной ячейки) и помещения избыточных пакетов выбранного типа в очередь. Таким образом, любой поток данных, превышающий установленный порог, попадает в очередь, в отличие от использования CAR, где пакеты в очередь не устанавливаются. Следовательно, поток данных определенного профиля может быть сформирован в соответствии с требованиями исходящего потока для предотвращения образования "узких мест" в сетевой топологии, в которых скорость передачи не соответствует возможностям канала. Схема работы GTS показана на рис. 59.10.

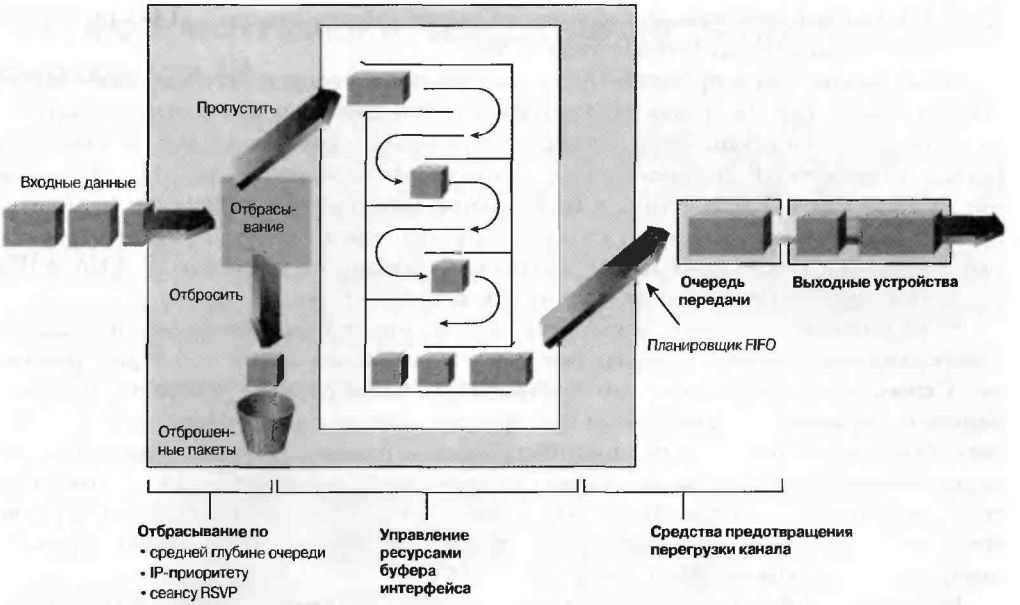


Рис. 59.10. Общее формирование потоков применяется отдельно на каждом интерфейсе

Формирование потоков GTS применяется к каждому отдельному интерфейсу, может использовать списки доступа для выбора формируемого поток данных и поддерживает ряд технологий 2-го уровня, в том числе Frame Relay, ATM, SMDS (Switched Multimegabit Data Service) и Ethernet.

В подинтерфейсе Frame Relay можно настроить GTS на динамическую адаптацию к полосе пропускания с помощью сигналов BECN или же просто установить заранее заданный уровень. Механизм GTS можно также сконфигурировать с помощью платы интерфейсного процессора ATM (ATM/AIP) таким образом, чтобы он реагировал на сигналы протокола RSVP, передаваемые по статически сконфигурированным постоянным виртуальным ATM-каналам (PVC).

FRTS: управление потоками данных Frame Relay

Механизм *формирования потоков данных Frame Relay (Frame Relay Traffic Shaping — FRTS)* предоставляет параметры, позволяющие управлять перегрузкой в сети. Эти параметры включают в себя согласованную скорость передачи информации (committed information rate — CIR), уведомления FECN и BECN, а также бит DE очередности при отбрасывании. В течение определенного времени компания Cisco обеспечивала поддержку уведомлений FECN для сетей DECnet и BECN для SNA, используя непосредственную инкапсуляцию LLC2, описанную в RFC 1490, а также поддержку бита DE. Функция FRTS базируется на этой поддержке Frame Relay с дополнительными возможностями, увеличивающими масштабируемость и производительность сетей Frame Relay, повышающими плотность передачи по виртуальным каналам и сокращающими время отклика.

В частности, имеется возможность принудительной установки пиковых уровней для ограничения исходящих потоков данных при помощи CIR и других параметров,

таких как уровень избыточной информации (excess information rate — EIR) на отдельных виртуальных каналах (virtual circuit — VC).

Также можно задать приоритетную и настраиваемую очередность на уровне виртуального канала или на уровне подынтерфейса. Это позволяет более точно разграничить приоритеты и организовать очереди для различных потоков данных, а также дает больше возможностей управления ими на отдельных виртуальных каналах. Применение очередности CQ в сочетании с поканальной организацией очередей и возможностью принудительной установки уровней позволяет организовать передачу виртуальными каналами Frame Relay данных различных протоколов, таких как IP, SNA и IPX с гарантированной полосой пропускания для каждого из них.

FRTS позволяет избежать "узких мест" в сетях Frame Relay использующих высокоскоростные соединения с центральным узлом и низкоскоростные — с периферийными. Скорость передачи можно сконфигурировать таким образом, чтобы она была ограничена значением, используемым при передаче данных по VC-каналу центральному узлу. Производительность сети может быть дополнительно повышена путем использования имеющейся функции назначения приоритета по существующему идентификатору канального соединения (Data-Link Connection Identifier — DLCI). В сетях Frame Relay механизм FRTS применяется только для PVC-каналов и для коммутируемых виртуальных каналов (switched virtual circuit — SVC).

Используя информацию поступающих из сети пакетов, маркированных тегом BECN, FRTS также позволяет динамически замедлять передачу данных. При таком замедлении скорости передачи пакеты хранятся в буферах маршрутизатора с целью уменьшения потоков данных из маршрутизатора в сеть Frame Relay. Замедление передачи выполняется для каждого VC-канала в отдельности, и скорость передачи настраивается в зависимости от количества полученных пакетов, маркированных тегом BECN.

FRTS также предоставляет механизм совместного использования среды передачи несколькими VC-каналами. Повышение скорости передачи позволяет контролировать выбранную маршрутизатором скорость передачи по критериям, отличным от скорости канала, таким как CIR и EIR. Функция повышения скорости передачи может быть использована для предварительного выделения полосы пропускания каждому каналу VC, в результате чего создается виртуальную сеть TDM. Кроме вышесказанного, механизм FRTS Cisco позволяет интегрировать средство управления нагрузкой в замкнутой цепи (StrataCom ATM Foresight) для активной адаптации к условиям перегрузки для исходящих потоков.

Механизмы повышения эффективности канала

В настоящее время программное обеспечение Cisco IOS предусматривает два механизма повышения эффективности канала: фрагментацию и чередование в канале (Link Fragmentation and Interleaving — LFI) и сжатие заголовков протокола реального времени (Real-Time Protocol Header Compression — RTP-HC), которые в сочетании с организацией очередей и формированием потоков повышают эффективность и предсказуемость служб уровня приложений.

LFI: фрагментация и чередование данных протокола IP

Интерактивные потоки данных (Telnet, Voice over IP и т.п.) чувствительны к повышению латентности и дребезжанию, которые возникают, когда сеть обрабатывает большие пакеты (например, при передаче данных по глобальному каналу между локальными сетями по протоколу FTP), особенно если они поставлены в очередь на медленном канале. Функция LFI операционной системы IOS Cisco сокращает задержку и уменьшает уровень дребезжания на медленных каналах путем разбиения (фрагментации) крупных дейтаграмм и чередования получившихся пакетов меньшего размера с пакетами с малой задержкой (рис. 59.11).

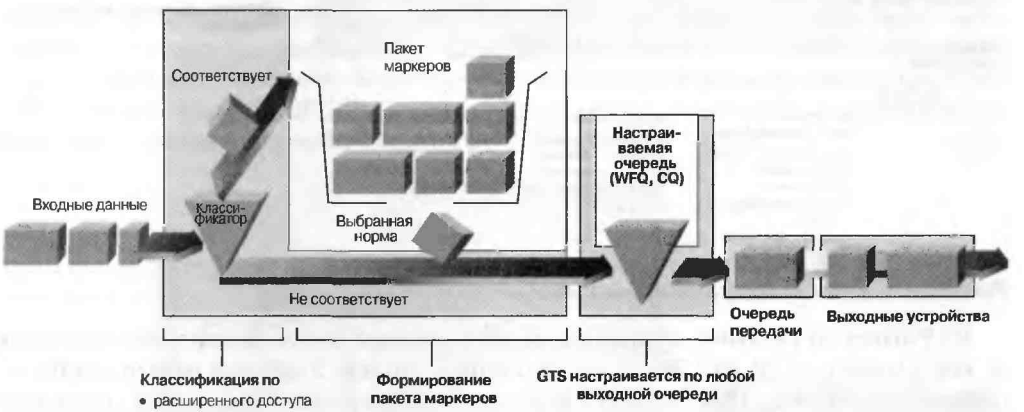


Рис. 59.11. Сокращение задержки на медленном канале путем разбиения крупных дейтаграмм посредством LFI

LFI был разработан специально для низкоскоростных каналов, где задержки фрагментации достаточно велики. На интерфейсе, в котором используется режим чередования, функционирование LFI требует установки многоканального протокола PPP. Проект IETF, называемый многоклассовым расширением многоканального PPP, (MultiClass extensions to MultiLink PPP — MCML) реализует практически те же самые функции как и LFI.

Следует обратить внимание на то, что для фрагментации в сети Frame Relay необходимо использовать функцию FRF.12, которая обеспечивает тот же результат.

Сжатие заголовков RTP: повышение эффективности при передаче данных реального времени

Транспортный протокол реального времени представляет собой протокол для передачи между узлами по IP-сетям данных современных мультимедийных приложений, в том числе пакетированных аудио- и видеоданных. Транспортный протокол реального времени обеспечивает сквозную передачу информации для приложений, требующих обмена данными в реальном времени, такой как аудио, видео и данные моделирования по одиночному адресу или по группе адресов. Благодаря сжатию заголовка

протокола RTP повышается эффективность работы многих современных мультимедийных приложений и приложений VoIP, в особенности на медленных каналах. Схема сжатия заголовка протокола RTP показана на рис. 59.12.

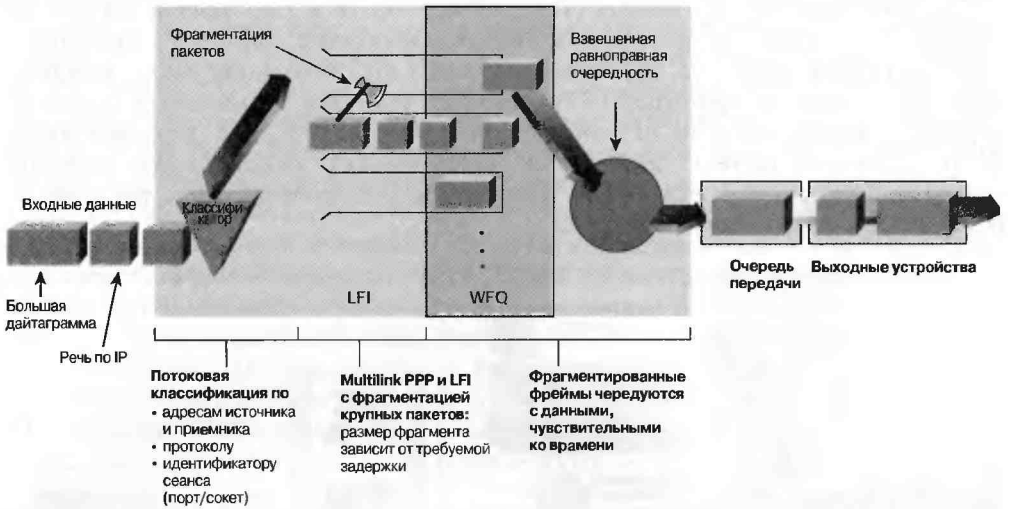


Рис. 59.12. Сжатие заголовка транспортного протокола реального времени

RTP-пакет со сжатыми данными аудиоприложений имеет 40-байтовый заголовок и, как правило, от 20 до 150 байтов полезной нагрузки. Учитывая размер комбинированного заголовка IP/UDP/RTP, неэффективно передавать несжатый заголовок. Сжатие заголовка RTP/UDP/IP с 40 до 2–5 байт обеспечивает более эффективную работу этого протокола, особенно на низкоскоростных каналах. Это особенно выгодно для небольших пакетов (таких, как данные VoIP) на медленных каналах (385 Кбит/с и ниже), в которых сжатие RTP-заголовка может значительно снизить объем управляющих сигналов и задержку при передаче. Сжатие заголовка протокола RTP также позволяет снизить удельный вес управляющих сигналов для мультимедийных данных протокола RTP и, соответственно, уменьшить задержку, особенно для пакетов небольшой (относительно заголовка) длины.

Сжатие RTP-заголовка поддерживается на последовательных каналах с помощью Frame Relay, протокола HDLC или инкапсуляции PPP. Его поддерживают также интерфейсы ISDN. Те же функции выполняет разработка IETF, называемая сжатым RTP (Compressed RTP — CRTP).

Протокол RSVP: гарантии QoS

RSVP представляет собой протокол Internet-стандарта IETF (RFC 2205), позволяющий приложению динамически резервировать полосу пропускания сети. Этот протокол дает приложениям возможность запросить качество обслуживания QoS для потока данных (рис. 59.13). В реализации Cisco протокол RSVP также может быть использован в сети с настроенным прокси-сервером RSVP. Таким образом, сетевые менеджеры имеют возможность использовать преимущества RSVP даже для тех приложений и узлов, которые не поддерживают протокол RSVP.

На узлах и маршрутизаторах RSVP применяется для доставки запросов QoS маршрутизаторам по маршруту передачи потока данных и для поддержания маршрутизатора и узла в состоянии, позволяющем обеспечивать требуемый уровень обслуживания — обычно полосу пропускания и задержку. Для определения резервируемой полосы пропускания RSVP использует информацию о средней скорости передачи данных, наибольшем количестве данных, которые маршрутизатор может держать в очереди, и минимальный уровень QoS.

Очередности WFQ или WRED выступают в качестве рабочего инструмента для RSVP, осуществляя классификацию и устанавливая расписание передачи пакетов для зарезервированных потоков. Используя очередность WFQ, протокол RSVP может предоставлять гарантированный набор интегрированных служб, в том числе службу управляемой нагрузки. Очередность WFQ по-прежнему управляет потоками данных, для которых резервирование не производится, ускоряя прохождение интерактивных данных и равномерно распределяя оставшуюся полосу пропускания между интенсивными потоками. Очередность WRED, соответственно, обслуживает потоки, не относящихся к RSVP. Протокол RSVP можно реализовать в существующих сетях путем обновления программного обеспечения.

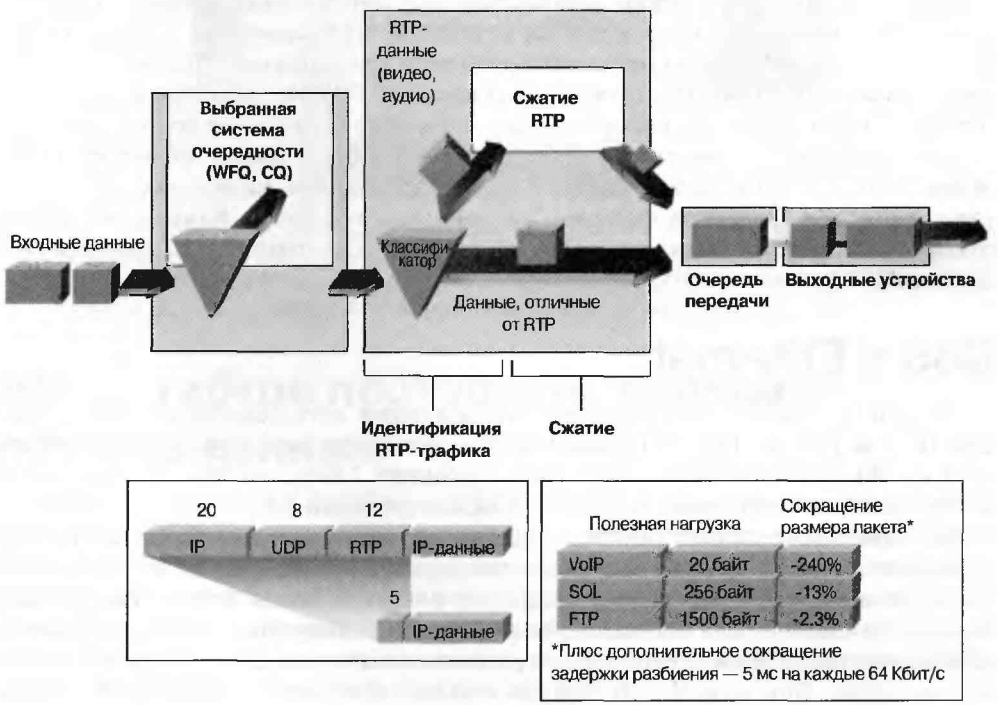


Рис. 59.13. Работа протокола RSVP в сети с маршрутизаторами Cisco

Управление QoS

Во введении был описан общий (но отнюдь не единственный) метод управления QoS.

Измерение состояния сети производится с помощью датчиков RMON и программного обеспечения (например, Traffic Director) для качественного анализа

параметров передачи данных по сети. Функция обнаружения в NBAR (описанная выше в этой главе) обеспечивает краткий обзор загрузки на уровне интерфейса, но датчики RMON дают более полную информацию. Кроме того, необходимо организовать измерения параметров основных приложений (обычно измеряется время отклика). Эта информация помогает обосновать любую систему QoS. На основании таких данных определяются и реализуются требуемые политики QoS.

После реализации необходимо оценить политики QoS и решить, нужны ли дополнительные службы. Для определения эффективности политики QoS можно измерить времена отклика в объединенной сети при помощи монитора производительности объединенной сети (Internetwork Performance Monitor — IPM). Сравнение новых результатов измерений для отдельных приложений с первоначальными данными позволит определить, насколько оправдано применение политик QoS. В дополнение к этому датчики RMON должны и далее проводить мониторинг сети постоянно, потому что характеристики передачи данных по сети, скорее всего, будут изменяться. Постоянное наблюдение за работой сети поможет проводить изменения в сети и позволит сетевому администратору быстрее выполнять новые требования.

Для настройки QoS во всей сети Cisco используется менеджер политик QoS (QoS Policy Manager — QPM) с графическим пользовательским интерфейсом. Правила, или политики, создаются и загружаются в сетевые устройства. QPM совместим с Common Open Policy Server (COPS), стандартным протоколом для загрузки политик на COP-совместимые устройства. Предложенный стандарт (RFC 2748) является простой клиент-серверной моделью для управления политиками по сигнальным протоколам QoS.

Для управления устройствами QoS применяется Cisco Quality of Service Device Manager (QDM). QDM представляет собой Web-приложение, написанное на Java, которое хранится в групповой файловой системе маршрутизатора. Клиентский броузер создает соединение со встроенным Web-сервером маршрутизатора, где хранится приложение QDM, и может настраивать устройство при помощи Web-интерфейса Java.

QoS в Ethernet

На линии Catalyst многоуровневых коммутаторов есть возможность обеспечить QoS на 2-м уровне. На этом уровне фрейм использует класс обслуживания (CoS) 802.1p и ISL (Interlink Switch Link). CoS использует 3 бита, подобно IP-приоритету, и устанавливает однозначное соответствие между уровнями 2 и 3.

Коммутаторы позволяют различать фреймы по характеристикам CoS. При наличии нескольких очередей фреймы могут быть помещены в разные очереди и обслуживаться по взвешенному циклическому алгоритму (Weighted Round Robin, WRR). Таким образом, каждой очереди соответствует свой уровень обслуживания. Внутри очереди устанавливаются пороги WRED. Эти пороги подобны минимальным порогам WRED на 3-м уровне. Они играют роль исходных точек, по которым определяется, с какой вероятностью может быть отброшен пакет.

На рис. 59.14 показана схема применения WRR и WRED для двух очередей с двумя порогами в каждой. Такая схема называется *2Q2T* (2 Queues, 2 Thresholds — 2 очереди, 2 порога). В очередь 1 помещены пакеты с CoS от 4 до 7, а в очередь 2 — от 0 до 3. Очередь 1 настроена на обслуживание в течение 70% времени, а очередь 2 — в течение 30% времени. Когда очередь 1 заполнена на 30%, пакеты с CoS 4 и 5 могут быть отброшены. Пакеты с CoS 6 и 7 отбрасываются только в случае, если

очередь заполнена более чем на 85%. Если очередь 2 заполнена на 20%, могут быть отброшены пакеты с CoS 0 и 1. Пакеты с CoS 2 и 3 отбрасываются только тогда, когда очередь заполнена на 60%.

Во многих реализациях имеется преобразование ToS (или IP-приоритета) в CoS. В данном случае CoS фрейма Ethernet можно преобразовать в байт ToS IP-пакета, и наоборот. Это обеспечивает сквозную передачу приоритета потока данных.

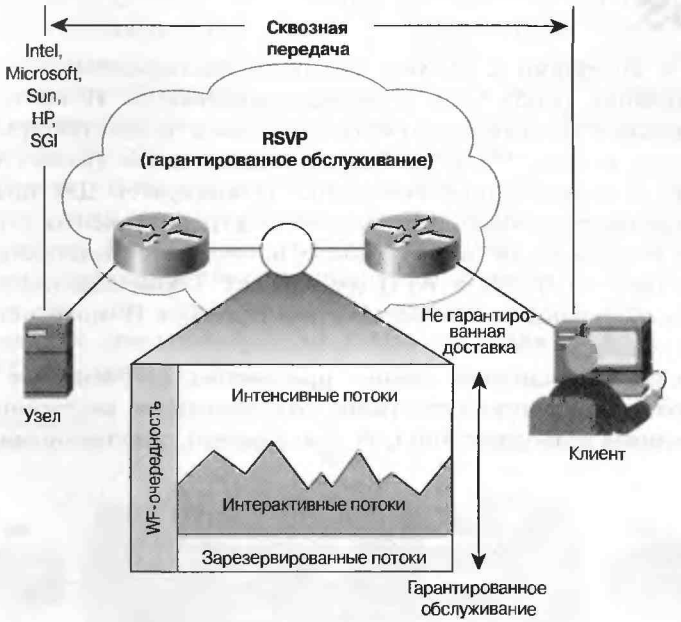


Рис. 59.14. WRR и WRED с двумя очередями, по два порога в каждой

MPLS: гибкое построение передачи потоков данных

Функция Cisco MPLS (Multiprotocol Label Switching, многопротокольная коммутация по меткам, (также называемая *коммутацией тегов*) содержит механизмы, обеспечивающие взаимодействие и использующие преимущества систем управления RSVP и IP-приоритета. Заголовок MPLS содержит 3-разрядное поле, которое может использоваться как признак приоритета потока данных. Его также можно применять для направления отдельных потоков и классов данных по спроектированным MPLS-маршрутам, чтобы получить требуемое QoS для MPLS-сети.

Управление политиками QoS

Архитектура управления политиками QoS должна стать базой новой сетевой политики CiscoAssure. В CiscoAssure большое значение уделяется стандартным протоколам управления QoS и механизмам распространения политик QoS с единого консольного интерфейса.

На уровне инфраструктуры классификация пакетов является основной функцией каждого механизма политик, которая позволяет передавать через данный элемент

сети или интерфейс определенные пакеты, соответствующие данному QoS. Затем этим пакетам может быть назначен соответствующий IP-приоритет или они идентифицируются как RSVP. Управление политиками также требует интеграции с основополагающими сетевыми технологиями канального уровня и протоколами, отличными от IP.

SNA ToS

SNA ToS в сочетании с DLSw+ позволяет преобразовывать традиционный класс обслуживания (CoS) SNA в дифференцированное IP-обслуживание. Эта функция использует управляющие сигналы и элементы архитектуры QoS. DLSw+ открывает четыре сеанса TCP и преобразует каждый поток данных SNA ToS в отдельный сеанс. Каждому сеансу назначается IP-приоритет. Для того чтобы обеспечить гарантированную полосу пропускания и другие элементы улучшенного обслуживания в интранет-сети, в этих сеансах применяются технологии управления перегрузкой Cisco — CQ, PQ и WFQ (рис. 59.16). Таким образом традиционным клиентам SNA обеспечивается возможность миграции в IP-интранет с сохранением производительности SNA.

Следовательно, традиционные важные приложения, рассчитанные на мэйнфреймы, могут пользоваться преимуществами развивающихся внутренних и внешних IP-сетей, не жертвуя возможностями QoS, традиционно свойственными сетям SNA.

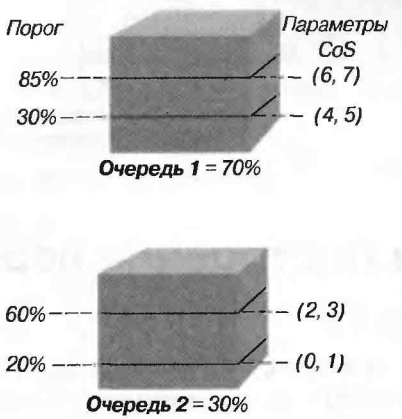


Рис. 59.15. SNA ToS в сочетании с DLSw позволяет преобразовывать SNA CoS в дифференцированное IP-обслуживание

QoS для речевых пакетов

Одним из самых перспективных направлений использования IP-сетей является совместная передача речи и обычных межсетевых данных. Как правило, расходы на передачу при этом сокращаются за счет уменьшения количества подключений к существующим каналам, инфраструктуре и т.п.

У Cisco есть широкий ассортимент сетевых продуктов и технологий для передачи речи, в том числе ряд продуктов для передачи речи по IP-сетям (Voice over IP, VoIP).

Однако, чтобы улучшить качество речи, к традиционным информационным сетям следует добавить функцию QoS. QoS в Cisco IOS позволяет обслуживать на должном уровне и потоки данных VoIP, и традиционные типы данных.

На рис. 59.17 показана схема компании, где решили несколько сократить расходы на телефонные переговоры, объединив передачу голосовых данных с существующей IP-сетью. Голосовые данные каждого офиса оцифровываются речевыми модулями на процессорах 3600. Дальнейший маршрут этих данных определяется драйвером шлюза (Gatekeeper) H.323, которому также нужно знать QoS для голосовых данных. Последнему в данном случае присваивается высший IP-приоритет. На всех интерфейсах маршрутизаторов этой сети используется очередь WFQ, которая автоматически ускоряет передачу с каждого интерфейса голосовых данных с высоким приоритетом, уменьшая задержки и искажения.

Поскольку IP-сеть изначально рассчитана на передачу обычных межсетевых данных, многие проходящие через нее дейтаграммы представляют собой крупные пакеты размером 1500-байтов. При низкой скорости связи (ниже T1/E1) речевые пакеты иногда задерживаются, ожидая прохождения одного из таких больших пакетов и запаздывая на десятки или даже сотни миллисекунд. Чтобы прервать подобные "супердейтаграммы" и пропустить речевой пакет, уменьшив задержку и искажения, совместно с WFQ используется LFI.

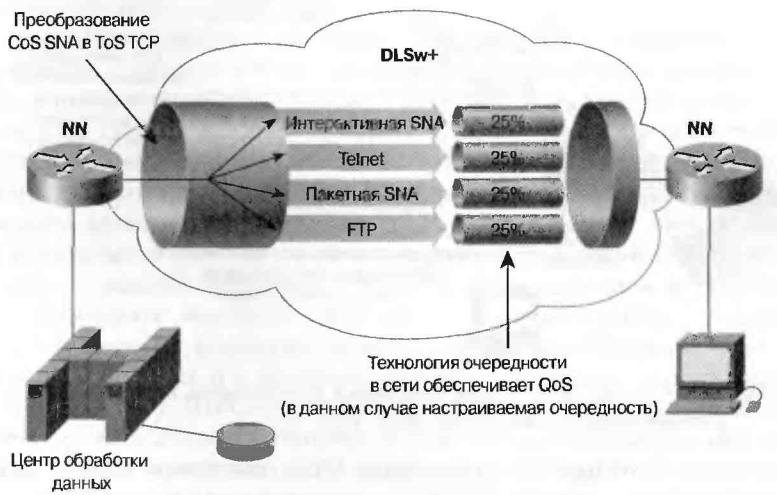


Рис. 59.16. Схема работы QoS VoIP

QoS при передаче видеопотоков

Одной из самых серьезных проблем IP-сетей, традиционно рассчитанных только на доставку пакетов, стало предоставление некоторых гарантий при передаче различных типов информационных потоков. Особенно большие сложности возникли при передаче видеопотоков, так как это обычно требует резервирования значительной полосы пропускания.

В сети, показанной на рис. 59.18, для обеспечения гарантированной полосы пропускания между ячейками использован протокол RSVP и асинхронные каналы PVC. RSVP настроен Cisco IOS так, чтобы обеспечивать обмен данными между маршрути-

зируемыми сетями через асинхронное ядро. Затем моделируемый информационный поток использует эти гарантированные пути в соответствии с ограничениями, свойственными географически распределенной модели в реальном масштабе времени. Расположенные в узлах компьютеры с поддержкой видео также используют данную сеть для проведения видеоконференций в прямом эфире.

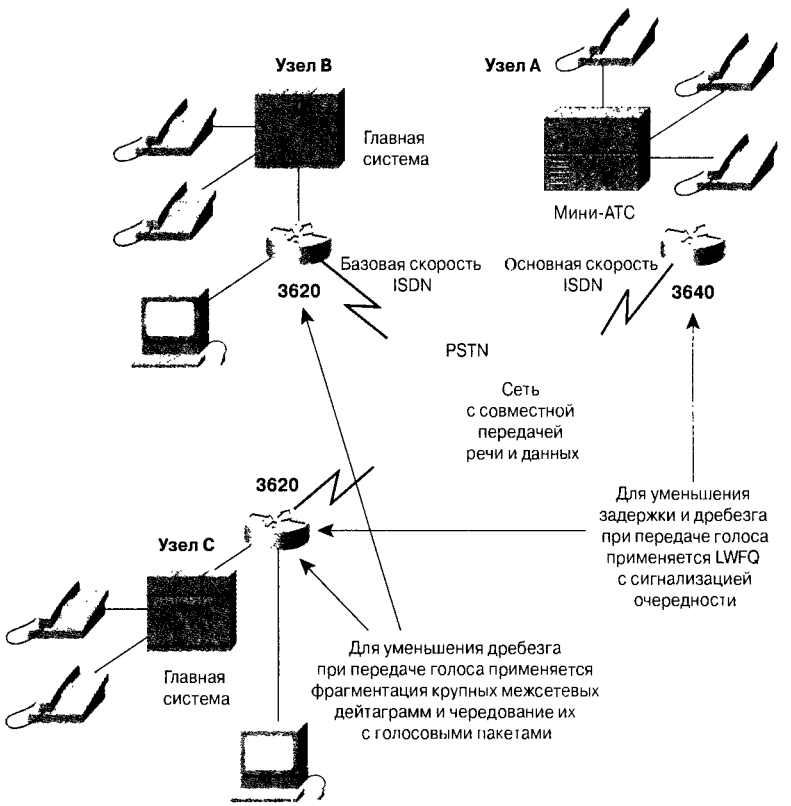


Рис. 59.17. Схема сети, демонстрирующая использование протокола RSVP в полносеточной асинхронной среде ATM

В таком случае асинхронные соединения OC-3 настроены как множество PVC-каналов со скоростью передачи 3 Мбит/с, подключенных к различным удаленным узлам. Протокол RSVP гарантирует, что QoS данного PVC-канала распространяется на соответствующее приложение по локальной маршрутизируемой сети. В будущем Cisco IOS дополнит это свойство RSVP возможностью динамической настройки асинхронных SVC-каналов, что позволит упростить и в значительной степени автоматизировать настройку.

Автоматизация QoS

Автоматизация QoS (Automated QoS — AutoQoS) упрощает конфигурирование и реализацию QoS. Критически важные приложения делают QoS все более весомым фактором успеха как для предприятий, так и для провайдеров служб. Однако реализация

QoS может оказаться весьма непростой задачей. Разные приложения предъявляют различные требования к QoS. Нахождение соответствующей конфигурации для каждого приложения оказывается серьезной задачей при реализации и управлении сетью. Вследствие этого предприятия и провайдеры служб не всегда оказываются в состоянии воспользоваться всеми преимуществами новых IP-приложений. Применение AutoQoS Cisco позволяет значительно уменьшить затраты средств и времени на реализацию в сети качества обслуживания QoS.

Применение AutoQoS Cisco является новым подходом, который интегрирует функции QoS в программное обеспечение IOS Cisco и автоматизирует их для конкретной сети и параметров потоков данных в ней. В настоящее время AutoQoS Cisco обеспечивает автоматизацию конфигурирования QoS при реализации VoIP. Будущие разработки будут включать в себя поддержку промышленных приложений для работы с данными, видео и других мультимедийных приложений, а также более современные функции управления, такие как подробная регистрация характера потоков данных.

Резюме

Механизмы качества обслуживания QoS операционной системы IOS Cisco предоставляют набор средств, которые позволяют обеспечить необходимые сетевые службы для успешной передачи потоков данных.

QoS предоставляет дифференцированные службы для назначения потокам более высокого приоритета или гарантии определенного уровня обслуживания — в отличие от принципа негарантированной доставки, при использовании которого качество обслуживания QoS обычно не обеспечивается. Очередность FIFO обеспечивает только негарантированную доставку. В этом случае потоки не различаются и обрабатываются по принципу "первым пришел, первым обслужили".

С помощью средств классификации (PBR, CAR и NBAR) потоки идентифицируются и маркируются для использования другими средствами QoS во всей объединенной сети. Средства управления перегрузкой (очередности PQ, CQ, WFQ и CBWFQ) управляют доставкой пакетов в тех случаях, когда требуемая полоса пропускания превышает возможности канала. Для предотвращения перегрузок, как в отдельных очередях, так и в объединенной сети, используется система управления очередностью (WRED). Используя свойства протокола TCP, технология WRED позволяет регулировать скорость потоков, отбрасывая некоторые из них. Она может также обеспечивать приоритетность, отбрасывая потоки с низким приоритетом раньше, чем потоки с высоким приоритетом. Средства повышения эффективности канала (LFI и сжатие RTP-заголовков) облегчают передачу чувствительных к задержкам потоков в каналах с узкой полосой пропускания. В LFI для этого фрагментируются большие пакеты, а сжатие заголовков RTP уменьшает объем передачи служебных данных для RTP-пакетов.

Гарантированное обслуживание обычно обеспечивается протоколом RSVP, хотя CBWFQ также может рассматриваться как форма гарантированного обслуживания. RSVP представляет собой протокол сигнализации, который сигнализирует всем устройствам сети на маршруте следования пакета о необходимости обеспечения гарантированного обслуживания поддерживается. Механизм очередности CBWFQ отличается тем, что гарантирует обслуживание только в пределах данного интерфейса.

Будущее QoS

В процессе эволюции по направлению к сквозному обеспечению QoS корпорация Cisco расширяет сферу его применения в объединенных сетях для того, чтобы обеспечить более плавный переход между разнородными канальными технологиями, и тесно сотрудничает с разработчиками основных платформ для обеспечения взаимодействия между сетями и конечными системами.

QoS находится на переднем крае развития сетевых технологий. Возможно, в будущем появятся средства обеспечения QoS для каждого конкретного пользователя, в которых политики QoS будут в равной степени основаны на требованиях пользователя и приложений. Такие средства, как NBAR, с их возможностью глубокого анализа пакетов, обеспечивают надежную идентификацию потоков. Сквозные системы QoS (от настольного ПК до настольного ПК) разработки Cisco позволяют сделать сети Cisco ведущим провайдером, обеспечивающим сквозное качество обслуживания.

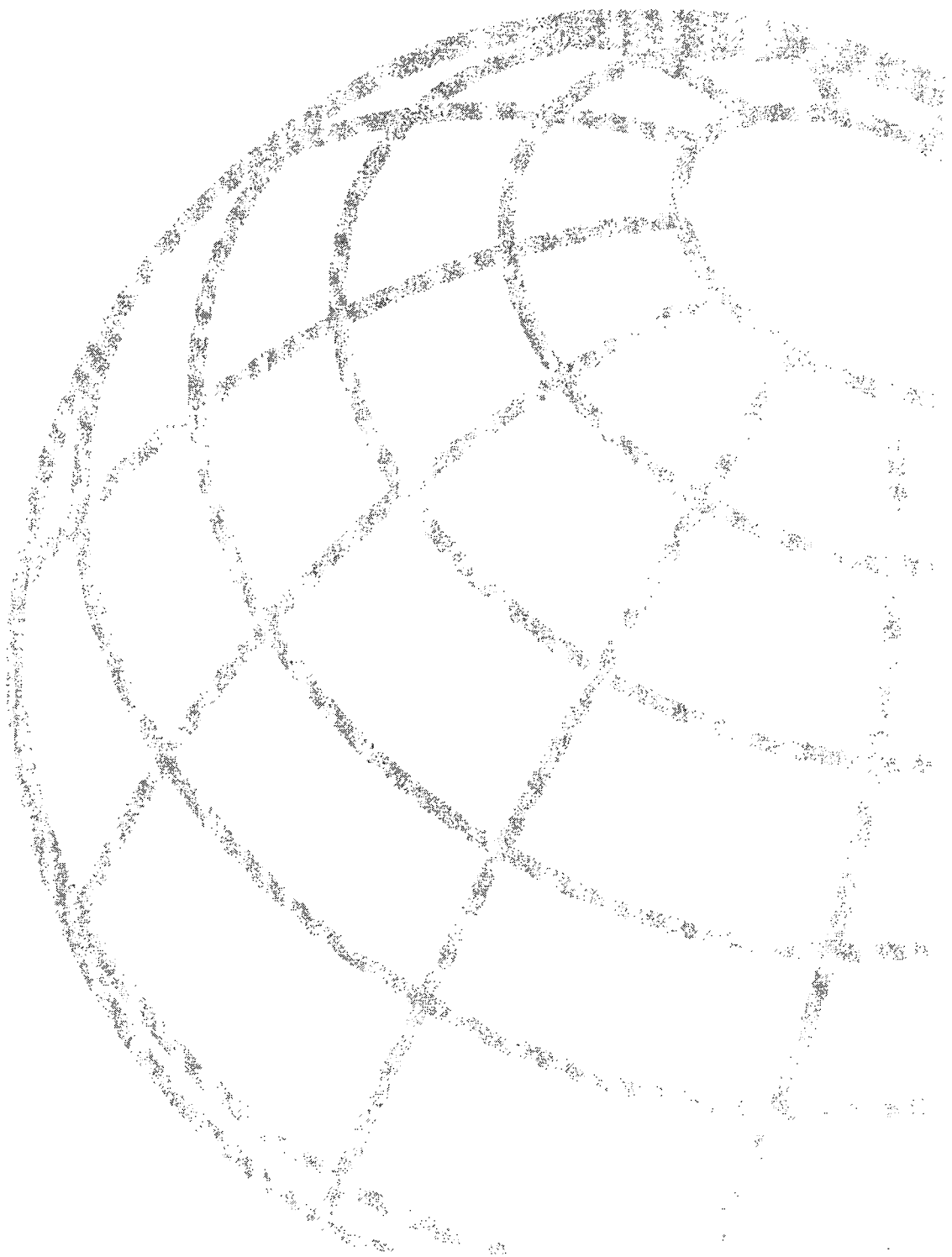
Контрольные вопросы

1. В чем заключается основное назначение QoS?
2. Каковы основные типы средств QoS?
3. Что называется управляющей сигнализацией?
4. Что представляет собой IP-приоритетность?
5. Что называется кодовой точкой дифференцированных служб (DSCP)
6. Что называется интерфейсом командной строки модульного QoS (MQC)?
7. Чем отличается потоковая очередность WFQ от классовой очередности WFQ (CBWFQ)?
8. Какое средство используется для управления очередями в целях предотвращения перегрузок? Каким образом оно предотвращает перегрузки?
9. Каковы два основных назначения механизма CAR?
10. Какое средство QoS следует использовать для обеспечения минимально необходимой полосы пропускания?
11. Каким средством QoS необходимо пользоваться для ограничения максимальной полосы пропускания, используемой потоком?
12. Что делает NBAR и в чем заключаются его две уникальные особенности?
13. В каких случаях обычно применяется формирование потоков?
14. Какое средство используется для интегрированного QoS?

Дополнительные источники

- Cisco Systems. *Cisco IOS 12.0 Quality of Service.* Indianapolis: Cisco Press, 1999.
- Ferguson, Paul, and Huston, Geoff. *Quality of Service: Delivering QoS on the Internet and in Corporate Networks.* New York: John Wiley & Sons, 1998.
- Lee D. *Enhanced IP Services.* Indianapolis: Cisco Press, 1999.

- Vegesna S. *IP Quality of Service for the Internet and the Intranets.* Indianapolis: Cisco Press, 2000.
- Cisco IOS QoS (http://www.cisco.com/warp/public/732/Tech/quality.shtml)
- RFC 2386, "A Framework for QoS-Based Routing in the Internet".



Часть IX

Приложения

Приложение А. Ответы на контрольные вопросы
Приложение Б. Традиционные технологии

Приложение A

Ответы на контрольные вопросы

Глава 1

1. *Из каких уровней состоит модель OSI?*

   Ответ: Из уровней приложений, представления, сеансового, транспортного, сетевого, канального и физического.

2. *Какой уровень определяет выбор маршрута в объединенной сети?*

   Ответ: 3-й, сетевой уровень.

3. *Что именно определяется на физическом уровне?*

   Ответ: Уровни напряжения, синхронизация изменений напряжения, физические скорости передачи данных, максимальные расстояния передачи данных, физические соединения и тип передающей среды.

4. *Какие существуют методы преобразования сетевых адресов в адреса MAC?*

   Ответ: Протокол ARP, приветствия, алгоритм с предсказанием.

5. *Какие службы сильнее нагружают сеть: ориентированные на соединение или не требующие подтверждения соединения?*

   Ответ: Службы, ориентированные на установку соединения.

Глава 2

1. *Опишите способы доступа к среде передачи, используемые в сетях Ethernet.*

   Ответ: В сетях Ethernet используется множественный доступ с контролем несущей и обнаружением коллизий (CSMA/CD). Каждая сетевая станция прослушивает сеть до и после передачи данных. Если обнаруживается коллизия, то обе станции ждут в течение некоторого случайно выбираемого временного интервала, а затем пытаются снова отправить данные.

2. *Опишите способы доступа к среде передачи, используемые в сетях Token Ring.*

   Ответ: В сетях Token Ring по сети передается особый тип пакета, называемый маркером. Если сетевому устройству требуется отправить данные, то оно должно

ждать, пока не будет получен маркер, и только затем посылать данные. После того как данные отправлены, маркер передается дальше в сеть.

3. *Опишите одноадресатную, многоадресатную и широковещательную рассылку данных.*

   Ответ: Одноадресатной называется передача данных от одного источника одному получателю. Многоадресатной называется передача данных от одного источника нескольким станциям, которые зарегистрированы для получения таких данных. Широковещательной называется передача данных от одного источника всем станциям в сегменте локальной сети.

Глава 3

1. *Какие типы каналов используются в распределенных сетях WAN?*

   Ответ: Каналы типа "точка-точка", каналы с коммутацией пакетов и каналы с коммутацией каналов.

2. *Что представляет собой маршрутизация по требованию (DDR) и чем она отличается от создания резервного канала?*

   Ответ: DDR представляет собой маршрутизацию по требованию с удаленным доступом. DDR обеспечивает доступ к удаленному узлу, если туда требуется направить какие-либо данные. Резервный телефонный канал используется для предоставления службы того же типа в случае выхода из строя основной линии связи. В случая ее неработоспособности включается резервная телефонная линия и работает до тех пор, пока не будет восстановлена основная.

3. *Для чего используется модуль CSU/DSU?*

   Ответ: Устройства CSU/DSU служат интерфейсом между маршрутизатором и цифровой линией, такой, например, как линия T1.

4. *В чем состоит различие между модемом и терминальным адаптером ISDN?*

   Ответ: Модем преобразует цифровые сигналы в аналоговые для передачи по телефонной линии. Поскольку линии связи ISDN являются цифровыми, для них такое преобразование не требуется.

Глава 4

1. *Каковы четыре основных типа памяти, используемые маршрутизатором?*

   Ответ: Постоянная память ROM, оперативная память RAM, флэш-память и NVRAM.

2. *Каковы три основных командных режима IOS Cisco?*

   Ответ: Пользовательский режим, привилегированный режим и режим конфигурирования.

3. *Как называется процесс повторного запуска операционной системы IOS Cisco?*

   Ответ: Перезагрузка системы.

Глава 5

1. *На каком уровне модели OSI работают мосты и коммутаторы?*

   Ответ: Мосты и коммутаторы представляет собой устройства передачи данных, работающие главным образом на 2-м уровне эталонной модели OSI. Поэтому их часто называют устройствами канального уровня.

2. *Чем управляет канальный уровень?*

   Ответ: На канальном уровне происходят операции моста по анализу и коммутации фреймов; этот уровень также контролирует потоки данных, обрабатывает ошибки передачи, обеспечивает физическую (в противоположность логической) адресацию и управляет доступом к физической среде передачи.

3. *Какие существуют типы мостов?*

   Ответ: Локальные и удаленные. Локальные мосты обеспечивают непосредственную связь между несколькими смежными сегментами локальной сети. Удаленные мосты соединяют несколько сегментов локальной сети, расположенных далеко друг от друга, обычно по линиям телекоммуникаций.

4. *Что такое коммутатор?*

   Ответ: *Коммутатором* называется устройство канального уровня, которое, как и мост, позволяет соединять между собой несколько физических сегментов локальной сети в одну более крупную сеть.

Глава 6

1. *Что такое маршрутизация пакетов?*

   Ответ: Маршрутизацией называется передача информации через объединенную сеть от источника к получателю.

2. *Назовите несколько типов алгоритмов маршрутизации.*

   Ответ: Статические и динамические, линейные и иерархические, выполняющиеся на рабочей станции и на маршрутизаторе, внутридоменные и междоменные, алгоритмы по состоянию канала и дистанционно-векторные.

3. *Чем отличается статическая маршрутизация от динамической?*

   Ответ: Статическая маршрутизация конфигурируется сетевым администратором и не адаптируется к изменениям в сети без его вмешательства. Динамическая маршрутизация автоматически адаптируется к изменениям сетевой топологии путем анализа поступающих сообщений об обновлении маршрутов без вмешательства администратора.

4. *Назовите несколько метрик, используемых протоколами маршрутизации.*

   Ответ: Длина маршрута, надежность, задержка, полоса пропускания, нагрузка и затраты на передачу (оценка маршрута).

Глава 7

1. *Назовите различные области управления сетью.*

   Ответ: Конфигурирование, учетные записи, регистрация сбоев, безопасность и производительность.

2. *Каковы цели управления производительностью?*

   Ответ: Измерять и делать доступными для администратора различные параметры производительности сети, с тем чтобы можно было поддерживать ее производительность на приемлемом уровне.

3. *Каковы цели управления конфигурацией?*

   Ответ: Целью управления конфигурацией является анализ данных сети и конфигурации системы, с тем чтобы оценить влияние различных элементов версий аппаратных средств и программного обеспечения на работу сети и добиться таким путем максимальной производительности.

4. *Каковы цели управления учетными записями?*

   Ответ: Измерять параметры использования сети, чтобы можно было соответствующим образом регулировать работу отдельных пользователей или их групп.

5. *Каковы цели управления отказоустойчивостью?*

   Ответ: Обнаруживать в сети ошибки, заносить их в журнал событий, уведомлять о них пользователей и автоматически их исправлять для поддержки эффективной работы сети.

6. *Каковы цели управления безопасностью?*

   Ответ: Контролировать доступ к сетевым ресурсам в соответствии с корпоративной политикой безопасности во избежание нанесения сети ущерба, а также доступа к секретной информации лиц, не имеющих соответствующих прав.

Глава 8

1. *Следует ли модернизировать все сети 10BaseT до 100 Мбит/с? Почему?*

   Ответ: Нет, это не является обязательным. Если сеть 10BaseT построена на повторителях, то достаточно заменить их на ненасыщенные коммутаторы 10/100, что приведет к автоматическому расширению средней полосы пропускания для каждой конечной станции в *n* раз.

2. *Какая версия (версии) 100Base предпочтительнее? Почему?*

   Ответ: Если горизонтальные каналы построены на неэкранированной витой паре категории 5 или выше, то рекомендуется использовать 100BaseTX; для категории 3 можно применять версию 100BaseT4, если удастся ее приобрести (по некоторым данным, поскольку спецификация 100BaseTX появилась более чем на год раньше T4, она захватила 95% рынка). Версия 100BaseT2 в настоящий момент не используется.

3. *Какая версия (версии) 1000Base предпочтительнее? Где их следует применять?*

   Ответ: Версию 1000BaseT рекомендуется использовать в том случае, когда горизонтальные каналы построены на неэкранированной витой паре категории 5 или выше. 1000BaseSX можно использовать если они построены на многомодовом оптоволоконном кабеле, а также для некоторых многомодовых магистралей. 1000BaseLX применяется как для одно-, так и для многомодового оптоволоконного кабеля (см. табл. 8.5). 1000BaseCX используется для комнатных коротких соединительных кабелей длиной до 25 м.

4. *Какой тип кабеля следует использовать для создания новой сети и для модернизации уже существующей? Почему?*

   Ответ: Для прокладки новых или замены старых линий на базе неэкранированной витой пары может использоваться категория 5E или выше, что увеличит скорость передачи до 1000 Мбит/с. Как показано в табл. 8.5, многомодовый оптоволоконный кабель применяется для 1000BaseSX или, как отмечено в следующем за табл. 8.5 параграфе, для 1000BaseLX. (Впоследствии эти кабели обеспечат также скорость 10000 Мбит/с на коротких расстояниях 100-300 м [в зависимости от длины волны].) Для обеспечения будущих потребностей и возможности работы длинных магистралей рекомендуется выбрать одномодовый оптоволоконный кабель.

5. *Как определить, нуждается ли сеть в модернизации? С чего начать?*

   Ответ: Существует несколько способов узнать о необходимости модернизации сети:

   - Узнать от пользователей (желательно делать это после того, как пройдут их отрицательные эмоции);
   - Система управления сетью должна определять нагрузку каждого порта DCE, что позволит определить наличие перегрузок.
   - Модернизация становится необходимой, если руководство компании решит установить новые приложения (например, мультимедийные), которые потребуют большей пропускной способности.
   - Модернизация требуется в том случае, если организация расширяется и нужны дополнительные DCE-порты для подключения новых пользователей.

   Определив потребности, можно рассмотреть варианты возможных действий. Следует помнить о том, что чем продолжительнее срок службы сетевых компонентов (таких, как каналы, к которым подключены сетевые серверы и коммутаторы), тем дороже их замена. Поэтому необходимо учитывать развитие сети в будущем и, по возможности, стараться повторно использовать эти компоненты.

Глава 9

1. *Каковы преимущества интерфейса FDDI по сравнению с интерфейсом CDDI?*

   Ответ: Большее расстояние передачи, отсутствие влияния радио- и электромагнитных помех.

2. *Какова роль DAC-устройств в сети FDDI?*

   Ответ: Концентратор DAC представляет собой устройство с двухпортовым подключением, которое обеспечивает целостность сетевого кольца даже в случае отключения однопортовых устройств, такие как персональные компьютеры.

Глава 10

1. *К какому типу технологий относится протокол Frame Relay?*

   Ответ: Frame Relay представляет собой технологию, использующую коммутацию пакетов.

2. *Назовите два вида технологий с коммутацией пакетов, описанных в настоящей главе, и кратко опишите каждый из них.*

   Ответ: В главе обсуждались описанные ниже технологии коммутации пакетов.

   1. При коммутации пакетов переменной длины пакеты коммутируются между различными сетевыми сегментами, чтобы наилучшим способом использовать сетевые ресурсы, пока не будет достигнут получатель.
   2. При статистическом мультиплексировании ресурсы сети используются значительно эффективнее.

3. *Опишите различия между каналами SVC и PVC.*

   Ответ: Коммутируемый виртуальный канал (SVC) создается при каждой передаче данных и прерывается по ее завершении. Постоянный виртуальный канал (PVC) является постоянным сетевым соединением, которое не разрывается после окончания передачи данных. Ранее не очень широко поддерживаемые оборудованием Frame Relay, в настоящее время каналы SVC используются в большинстве сетей.

4. *Что представляет собой идентификатор канального соединения?*

   Ответ: Идентификатор канального соединения (Data-Link Connection Identifier — DLCI) представляет собой значение, присваиваемое каждому виртуальному каналу и точкам подключения устройства DTE к глобальной сети Frame Relay. Двум различным соединениям в одной распределенной сети Frame Relay могут быть присвоены одинаковые значения — по одному на каждом конце виртуального соединения.

5. *Опишите отличия протокола LMI Frame Relay от базового протокола Frame Relay.*

   Ответ: В интерфейсе локального управления Frame Relay (Local Management Interface — LMI) есть ряд дополнений к стандартному протоколу Frame Relay, называемых расширениями. Основные расширения LMI обеспечивают выполнение следующих функций: глобальную адресацию, рассылку сообщений о состоянии виртуального канала и многоадресатную рассылку.

Глава 11

1. *Назовите не меньше трех преимуществ реализации в сети технологии HSSI.*

   Ответ: Преимущества HSSI заключаются в следующем:

   - Технология HSSI обеспечивает высокоскоростной обмен данными по распределенным и локальным сетям.
   - В HSSI используется дифференцированная эмиттерно-связанная логика, которая обеспечивает высокоскоростную передачу данных при низком уровне шумов.
   - В HSSI применяются одобренные FCC микроминиатюрные 50-контактные разъемы, меньшие, чем их аналоги для V.35.
   - В кабеле HSSI такое же количество контактов и проводов, как и в кабеле Small Computer System Interface 2 (SCSI-2), но электрическая спецификация HSSI гораздо четче.

- HSSI упрощает распределение полосы пропускания, тем самым делая более доступными T3 и другие широкополосные службы.
- HSSI требует наличия только двух управляющих сигналов ("DTE available" и "DCE available"), что обеспечивает его высокую надежность, так как уменьшает количество каналов, в которых может произойти сбой.
- В HSSI выполняется четырехкратный петлевой контроль надежности.

2. *Перечислите четыре вида контроля маршрутных петель, которые осуществляются в HSSI.*

   Ответ: Тест кабеля, тест DCE, тест телефонной линии и тест DTE.

Глава 12

1. *Какая контрольная точка для логических устройств ISDN используется только в Северной Америке?*

   Ответ: U — контрольная точка между устройствами NT1 и канальными терминаторами в сети провайдера.

2. *Какие две скорости передачи предусмотрены для служб PRI-интерфейса сетей ISDN?*

   Ответ: В Северной Америке и Японии 23 B-канала (1,472 Мбит/с) плюс один D-канал (64 Кбит/с); в Европе и Австралии — 30 B-каналов (1,984 Мбит/с) плюс один D-канал (64 Кбит/с).

3. *Сколько из 48 битов в формате физического фрейма ISDN занимают данные?*

   Ответ: 36 битов.

Глава 13

1. *Каковы главные компоненты протокола PPP?*

   Ответ: Инкапсуляция дейтаграмм, LCP и NCP.

2. *Каково единственное абсолютное требование физического уровня, определяемое протоколом PPP?*

   Ответ: Обеспечение дуплексного канала, выделенного или коммутируемого, который может работать в асинхронном или в синхронном побитовом режиме, прозрачном для канальных фреймов PPP.

3. *Из каких полей состоит фрейм PPP?*

   Ответ: Фрейм PPP состоит из шести полей: флага, адреса, управления, протокола, данных и поля контрольной последовательности фрейма.

4. *Из каких этапов состоит работа протокола LCP, входящего в стек протоколов PPP?*

   Ответ: Работа протокола LCP PPP состоит из четырех этапов: открытие канала, определение качества связи, согласование конфигурации протоколов сетевого уровня и закрытие канала.

Глава 14

1. *Где расположен интерфейс SNI?*

   Ответ: Между CPE и оборудованием передающего тракта — там, где заканчивается сеть клиента и начинается сеть передающего тракта.

2. *Что представляет собой интерфейс SIP?*

   Ответ: SMDS Interface Protocol — протокол интерфейса SMDS.

3. *На каких уровнях эталонной модели OSI действует каждый из трех уровней интерфейса SIP?*

   Ответ: 2-й и 3-й уровни протокола SIP действуют на MAC-подуровне канального уровня, а 1-й уровень SIP — на физическом уровне.

4. *Каким образом обеспечивается использование шины DQDB несколькими устройствами?*

   Ответ: Совместное использование шины становится возможным благодаря распределенному алгоритму установки очередности, что, однако, делает реализацию конфигурации с несколькими CPE значительно более сложной, чем конфигурации с одним CPE.

5. *В каких интерфейсах SMDS для реализации классов доступа SMDS иногда применяется схема кредитного управления?*

   Ответ: На интерфейсах SMDS со скоростью передачи DS-3.

Глава 15

1. *Сколько лет потребовалось для того, чтобы количество телефонов в американских домах достигло 90%?*

   Ответ: Телефон был изобретен в 1875 году, а в 1970 году им пользовались 90% американских семей. Это потребовало 95 лет.

2. *Какие рекомендации V-серии относятся к скорости передачи?*

   Ответ: V.21, V.23, V.27ter, V.29, V.32bis, V.34 и V.90.

3. *Сколько каналов DS0 в линиях BRI-интерфейса, T1 и E1?*

   Ответ: Два — в BRI (хотя D-канал может считаться третьим), 24 — в T1 и 32 — в E1.

4. *Что представляет собой поток данных, поступающий через модем от разъема RJ 11 к терминальному устройству?*

   Ответ: Это данные поступающие через разъем RJ 11 на аналого-цифровой преобразователь. После этого они поступают на DSP, который передает их пакетировщику, а тот, в свою очередь, — устройству или программе сжатия данных. Распакованные данные отправляются на UART, который доставляет их терминальному устройству DTE .

5. *Из каких трех этапов состоит согласование PPP? Почему так важно соблюсти их последовательность?*

   Ответ: Этими этапами являются LCP, аутентификация и NCP. LCP выполняется первым, потому что он определяет, надежно ли подключение, и согласует параметры между двумя одноранговыми узлами. Он также выясняет, требуется ли

аутентификация. Аутентификация производится перед согласованием сетевых протоколов, с тем, чтобы при согласовании протоколов можно было идентифицировать входящего пользователя или станцию и присвоить ему соответствующие сетевые атрибуты.

6. *Как связаны между собой представляющие интерес данные и таймер задержки?*

   Ответ: Если поток данных представляет интерес, то соединение продолжится, в противном случае оно будет прервано. Такой поток данных сбрасывает таймер задержки.

7. *Является ли интерфейс BRI номеронабирателем? Как асинхронный интерфейс может стать номеронабирателем?*

   Ответ: Интерфейс BRI является номеронабирателем. Асинхронный интерфейс может стать номеронабирателем, если ввести команду конфигурации **dialer in-band**.

8. *В каких случаях целесообразно использовать коммутируемые соединения, а когда нет?*

   Ответ: Коммутируемые соединения легко адаптируются к условиям среды, но имеют высокую стоимость. Для непостоянных соединений или соединений с мобильными пользователями удобным и практичным решением являются коммутируемые соединения. Для постоянных или практически постоянных соединений использование коммутируемых соединений нецелесообразно.

Глава 16

1. *Назовите два типа соединений, поддерживаемых протоколом SDLC.*

   Ответ: Каналы типа "точка-точка" и многоточечные каналы, ограниченные и неограниченные среды передачи, устройства передачи данных в полудуплексном и дуплексном режимах, сети с коммутацией каналов и сети с коммутацией пакетов.

2. *Назовите четыре основные конфигурации соединений протокола SDLC.*

   Ответ: Конфигурация типа "точка-точка", в которой используются только два узла, первичный и вторичный; многоточечная, с одним первичным и несколькими вторичными узлами; замкнутая, с замкнутой топологией, в которой первичный узел соединен с первым и последним вторичными, а промежуточные вторичные узлы — друг с другом и концентраторная, со входящим и исходящим каналами, в которой первичный узел использует исходящий канал для связи с вторичными, а вторичные используют для связи с первичным входящий канал.

3. *Из каких полей состоит фрейм протокола SDLC?*

   Ответ: Фрейм SDLC состоит из полей флага, адреса, управления, данных и поля FCS.

4. *Назовите протоколы, производные от SDLC, и укажите их основные отличия от протокола SDLC.*

   Ответ: HDLC, поддерживающий три режима передачи, в то время как SDLC поддерживает только один; LAPB, использование которого ограничено режимом передачи ABM и только комбинированными станциями; IEEE 802.2, часто на-

зываемый LLC, трех типов; QLLC, который обеспечивает контроль канала данных, что требуется для передачи данных SNA по сетям X.25.

Глава 17

1. *С каким видом сетей обычно работает протокол X.25?*

   Ответ: Обычно он применяется в обычных сетях с коммутацией пакетов, таких как телефонные сети.

2. *Назовите три основные категории, к которым относятся устройства протокола X.25.*

   Ответ: Устройства DTE, DCE и PSE.

3. *Назовите три основные функции устройства PAD.*

   Ответ: Буферизация, сборка и разборка пакетов.

Глава 18

1. *Что представляет собой виртуальная частная сеть VPN?*

   Ответ: Виртуальная частная сеть VPN (Virtual Private Network,) является общим понятием, описывающим любое сочетание технологий для безопасного соединения по незащищенным или ненадежным сетям.

2. *Какие ключевые службы безопасности обеспечивает протокол IPSec?*

   Ответ: Конфиденциальность, целостность данных и аутентификацию источника данных.

3. *Каковы функции протокола IKE?*

   Ответ: эта функция заключается в получении аутентифицированного ключа и обсуждении ассоциаций безопасности IPSec безопасным способом.

4. *Протокол IKE включает в себя две фазы. Какие функции характерны для каждой из них?*

   Ответ: На первом этапе, при обмене данными в главном режиме или в агрессивном режиме, устанавливается безопасный, аутентифицированный канал связи между двумя одноранговыми устройствами протокола IPSec. На втором этапе обмена данными в быстром режиме обсуждаются ассоциации безопасности IPSec под защитой ассоциации безопасности, созданной на первом этапе обмена.

5. *Каковы операционные режимы протокола L2TP?*

   Ответ: Принудительное туннелирование и добровольное туннелирование.

6. *Каким образом коммутация MPLS поддерживает иерархическую маршрутизацию в VPN-сетях протоколов BGP/MPLS?*

   Ответ: В VPN-сетях протоколов BGP/MPLS пакеты данных переносят две метки, находящиеся в стеке меток. Маршрутизаторы провайдера используют внешние метки для пересылки пакетов от одного PE-маршрутизатора к другому PE-маршрутизатору по базовой сети MPLS. PE-маршрутизатор использует внутреннюю метку для упрощения пересылки пакета соответствующему пользователю VPN-сети.

Глава 19

1. *Назовите три основные технологии пакетной передачи речи.*

   Ответ: Этими основными пакетными голосовыми технологиями являются передача голосовых данных по сетям Frame Relay, ATM и IP.

2. *Каким образом обеспечивается экономия на междугородных звонках при помощи технологии голосовых пакетов?*

   Ответ: Голосовые данные могут передаваться между разными городами по распределенным компьютерным сетям вместо телефонных. В зависимости от расстояния и тарифа это может дать значительную экономию.

3. *Назовите основные сигнальные протоколы передачи речи.*

   Ответ: H.323, SIP (Session Initiation Protocol) и MGCP (Media Gateway Control Protocol).

4. *Чем одноранговые сигнальные протоколы передачи голоса отличаются от клиент-серверных протоколов?*

   Ответ: Клиент-серверные сигнальные протоколы зависят от центрального устройства управления запросами, определяющего состояние конечных точек. Эта модель упрощает поддержку дополнительных функций вызова. Одноранговые протоколы используют интеллектуальные конечные точки и не требуют центрального устройства управления запросами, поэтому они лучше масштабируются.

Глава 20

1. *Каковы главные компоненты беспроводной системы?*

   Ответ:

   - источник информации;
   - приемопередатчик(трансивер)-приемник/передатчик;
   - модулятор/демодулятор;
   - локальный генератор;
   - преобразователь частоты (гетеродин)/внешний модуль;
   - кабель управления и коаксиальный кабель;
   - дуплексор.

2. *Чему равна длина волны для сигнала с частотой 850 МГц?*

   Ответ: 0.35 м

3. *Какие факторы следует учесть при выборе канала передачи?*

   Ответ:

   - ослабление RF;
   - импеданс;
   - потери по постоянному току DC;
   - физические характеристики, такие как вес, радиус изгиба и диаметр;
   - стоимость.

4. *Каковы два базовых типа антенны?*

   Ответ: направленная и всенаправленная

5. *Что означает аббревиатура EIRP?*

   Ответ: эффективная изотропная излучаемая мощность (Effective Isotropic Radiated Power)

6. *Что называется зоной Френеля?*

   Ответ: Зоной Френеля называется зона излучаемой энергии. Теоретически количество таких зон бесконечно. Однако на практике учитывается только первая зона Френеля. Эти зоны имеют эллипсоидальную форму и существуют в окрестности прямого маршрута LOS.

7. *Что представляют собой сигналы с несколькими маршрутами?*

   Ответ: сигналы с несколькими маршрутами являются продуктом тех же самых сигналов передачи которые поступают на приемник разделенными во временном домене, поскольку они проходят по разным маршрутам передачи.

8. *Каковы пять основных модулей архитектуры сети 802.11?*

   Ответ:

   - Базовый набор службы (Basic Service Set — BSS)
   - Независимый BSS;
   - BSS инфраструктуры;
   - Система распределения;
   - Расширенный набор службы.

9. *Какие пять служб предлагает служба распределения?*

   Ответ:

   - Служба установки связи;
   - Служба разъединения ;
   - Служба переустановки связи ;
   - Служба распределения;
   - Служба интеграции.

10. *Каковы четыре основных преимущества использования беспроводных технологий?*

    Ответ:

    - Эти технологии дополняют до полного комплекта технологии доступа, наряду с цифровыми абонентскими каналами (Digital Subscriber Line), кабельным доступом, выделенными линиями и другими технологиями сетевого доступа.
    - Эти технологии используются в тех случаях, когда использование других технологий невозможно, например, в гористой местности, где использование других технологий невозможно или слишком дорого.
    - Эти технологии могут быть быстро реализованы, особенно при наличии оборудования и использовании нелицензируемых частот.
    - Они могут быть использованы в качестве обходных (резервных) вместо более дорогостоящих технологий стационарной передачи, таких как оптоволоконные и медные кабели.

Глава 21

1. *Назовите существующие виды технологии DSL.*

   Ответ: ADSL, SDSL, HDSL, HDSL-2, G.SHDL, IDSL и VDSL.

2. *Какие два метода линейного кодирования применяются в ADSL?*

   Ответ: DMT и CAP.

3. *Какие версии DSL предоставляют симметричные службы?*

   Ответ: SDSL, HDSL и HDSL-2.

4. *Какая симметричная версия DSL предоставляет многоскоростную службу по одной витой паре?*

   Ответ: G.SHDSL.

5. *На какое расстояние от центрального офиса можно передавать данные с при использовании технологии IDSL?*

   Ответ: На 26000 футов.

6. *Какие скорости для нисходящего и восходящего потоков данных предлагаются для VDSL?*

   Ответ: Максимально возможная скорость нисходящего потока данных по линиям длиной до 300 метров (1000 футов). находится в диапазоне между 51 и 55 Мбит/с. Также часто встречаются скорости до 13 Мбит/с для нисходящего потока данных по линиям длиной свыше 1500 метров (4000 футов). В первых моделях скорости для входящего потока данных асимметричны, подобно ADSL, и колеблются в пределах от 1,6 до 2,3 Мбит/с.

Глава 22

1. *Опишите преимущества сетей HFC.*

   Ответ: Сети HFC обеспечивают расширенную полосу пропускания, повышенную надежность, двустороннюю передачу данных, повышенную устойчивость к шумам и сокращают затраты на обслуживание оборудования.

2. *Как происходит двусторонняя передача данных в сетях HFC?*

   Ответ: Двусторонняя передача данных в сетях HFC может обеспечиваться путем установки узкополосных восходящих усилителей, узкополосных обратных лазеров в оптическом узле, обеспечением оптического обратного пути и размещением оптического приемника на центральной станции или в концентраторе. Также необходима соответствующая процедура настройки обратного пути.

3. *Каким условиям должны соответствовать полосы пропускания для восходящего и нисходящего потоков по стандарту DOCSIS?*

   Ответ: По стандарту DOCSIS ограничения на полосу пропускания для восходящего потока составляют 5-42 МГц, а для нисходящего — 54-860 МГц.

4. *Опишите критерии доступности DOCSIS.*

   Ответ: Система DOCSIS должна обеспечивать доступность более чем на 99% при отправке 1500-байтовых пакетов со скоростью 100 пакетов в секунду, если кабельное оборудование соответствует спецификациям DOCSIS.

5. *Перечислите сетевые уровни DOCSIS.*

   Ответ: DOCSIS определяет следующие уровни: сетевой IP-уровень, канальный и физический уровни.

6. *Перечислите серверы DOCSIS 1.0. Каково их назначение?*

   Ответ: Серверы DOCSIS представляет собой сервер DHCP (RFC 2181), предоставляющий IP-адреса для CM и PC; сервер TFTP (RFC 1350) для регистрации и загрузки конфигурационных файлов CM; сервер TOD (RFC 868), который проставляет отметки времени событий операционной системы.

7. *Где MSO может установить универсальный широкополосный маршрутизатор?*

   Ответ: Универсальный широкополосный маршрутизатор устанавливается, в зависимости от потребностей, на центральной станции или концентраторе.

8. *Что такое обратная связь по телефону и когда она нужна?*

   Ответ: Обратная связь по телефону представляет собой услугу по передаче данных, которая обеспечивает высокоскоростную связь по коаксиальным кабелям и низкоскоростную — по обычной телефонной линии. Это приложение обычно используется в сельской местности, где стоимость усовершенствования сети слишком высока, или как временная мера, позволяющая MSO предоставлять услуги, пока кабельное оборудование проходит модернизацию для двусторонней передачи данных.

9. *Перечислите несколько будущих функций и приложений DOCSIS 1.1.*

   Ответ: DOCSIS 1.1 будет поддерживать VoIP, улучшенную систему защиты, сцепление и фрагментацию пакетов, а также QoS. Сервисные приложения включают телефонию и видео.

Глава 23

1. *Что представляет собой LSR-интерфейс?*

   Ответ: Вкачестве LSR-интерфейса могут выступать интерфейсы Packet Switch-Capable (PSC), Layer 2 Switch-Capable (L2SC), Time- Division Multiplexing-(TDM) Capable, Lambda Switch-Capable (LSC) и Fiber Switch-Capable (FSC).

2. *Какие три плоскости используются в G.8080 для обеспечения служб сигнализации и установки соединений?*

   Ответ: Контрольная плоскость, управляющая плоскость и транспортная плоскость.

3. *В чем состоит цель использования доменов в G.ASON?*

   Ответ: Домены позволяют подразделить контрольные плоскости. Такое подразделение позволяет провайдерам администрировать эти домены.

4. *Какие потоки данных — восходящие или нисходящие — требуют большей ширины полосы пропускания при использовании PON-сетей и почему?*

   Ответ: Нисходящие потоки данных требуют большей полосы пропускания чем восходящие. Основной причиной потребности в полосе пропускания является совместное использование нисходящих потоков для нескольких получателей. По этой причине пользователям требуется гораздо большая полоса пропускания для восходящих потоков, чем для нисходящих (для сигнализации и т.д.).

Провайдеры кабельных служб используют сети PON для обеспечения видеослужб и других.

5. *Какие два домена используются для администрирования в OTN для модели наложения?*

   Ответ: Один домен используется для уровня IP, а другой для оптического уровня.

6. *Какой тип оптической сети позволяет пользователю непосредственно принимать оптические сигналы независимо от скорости передачи оптической линии и типа фреймов?*

   Ответ: Прозрачная оптическая сеть.

7. *Что используется в G.ASON в качестве референтной точки между доменами?*

   Ответ: Интерфейс E-NNI

8. *Какой протокол используется для обеспечения работы канала и обмена информацией с соседним узлом? Почему?*

   Ответ: Для этого используется протокол управления каналом (Link Management Protocol — LMP). GMPLS имеет отдельные контрольную и управляющую плоскости, которым требуется протокол LMP для получения информации о соседних устройствах.

Глава 24

1. *Что называется драйвером шлюза в сети H.323?*

   Ответ: Драйвер шлюза протокола H.323 является необязательным компонентом, который позволяет осуществлять масштабирование сетей H.323 и централизованно управлять вызовами и конечными точками протокола H.323. В нем сохраняется динамически заполняемая таблица протокола H.323 или соответствия "псевдоним-номер" протокола E.164, которые позволяют идентифицировать получателей при получении запросов на вызов.

2. *Какова цель использования протокола SDP?*

   Ответ: С помощью протокола SDP обсуждаются возможности конечных точек протокола SIP, вовлеченных в установку сеанса SIP. При этом происходит обмен соответствиями (преобразованиями), такими как CODEC и RTP.

3. *В чем состоит главный мотив того, что компании реализуют сети H.323 и/или сети протокола SIP?*

   Ответ: С этим можно не соглашаться, однако главными являются финансовые мотивы.

   Протоколы H.323 и SIP позволяют компаниям экономить средства на различных статьях расходов, связанных с сетью и позволяют реализовать сетевые службы с меньшими расходами. Технология VoIP особенно полезна для небольших провайдеров служб, которым приходится конкурировать с крупными провайдерами.

4. *На каком протоколе основаны сообщения протокола H.225: Q.921, Q.931, Q932 или Q.703?*

   Ответ: сообщения протокола H.225 основаны на протоколе Q.931 ISDN.

5. *Какое устройство отвечает за обработку голосовых потоков и выполнение сложных алгоритмов CODEC?*

   Ответ: Цифровой сигнальный процессор (Digital Signal Processor — DSP)

6. *Какое сообщение должно следовать за сообщением 200 OK*

   Ответ: Сообщение подтверждения ACK.

Глава 25

1. *Чем отличается протокол DPT/SRP от других кольцевых технологий, таких как Token Ring и FDDI?*

   Ответ: В кольце SRP для передачи данных узлу не требуется маркер, а распаковка пакета в основном происходит у получателя, а не у источника. В протоколе DPT второе кольцо используется, а не является холостым, как в протоколе FDDI.

2. *Каким образом устанавливаются приоритеты пакетов в протоколе DPT/SRP?*

   Ответ: MAC-протокол SRP поддерживает восемь уровней очередности в формате пакета, скопированном из поля очередности при отбрасывании протокола IP (IP Precedence field). Они преобразуются в одну из двух физических очередей протокола SRP: очередь с низким приоритетом и очередь с высоким приоритетом. Имеется две очереди для передачи данных и две очереди для транзитных данных.

3. *Какой механизм используется для определения того, какое кольцо должен использовать узел для отправки пакета другому узлу?*

   Ответ: Узел, отправляющий пакет отправляет ARP-запрос по любому из двух колец. Целевой узел отвечает по этому кольцу, сообщая о наименьшем количестве переходов, определяемом в процессе автоматического анализа топологии.

4. *Как происходит самовосстановление кольца DPT/SRP в случае обрыва кабеля?*

   Ответ: Узлы, обнаружившие обрыв кабеля, осуществляют сворачивание кольца. Один из узлов направляет пакеты из внутреннего кольца во внешнее. На другом узле происходит обратная операция.

Глава 26

1. *Какое поле EAP-пакета указывает, является ли сообщение запросом, ответом на запрос, положительным или отрицательным ответом?*

   Ответ: Поле кода (Code field).

2. *В чем состоит основное преимущество использования протокола EAP в качестве механизма аутентификации?*

   Ответ: Для поддержки используемого метода аутентификации клиента не требуется сервер NAS.

3. *Какие два атрибута RADIUS используются при EAP –аутентификации?*

   Ответ: сообщение протокола EAP (EAP-Message) и аутентификатор сообщения (Message-Authenticator).

4. *Поддерживает ли EAP сертификаты со стороны сервера, со стороны клиента или оба типа сертификатов?*

   Ответ: EAP поддерживает сертификацию как со стороны сервера, так и со стороны клиента. В EAP-TLS используются и сертификат сервера, и сертификат клиента. В PEAP используются только сертификаты со стороны сервера, а клиенту по-прежнему требуется вводить свои данные для аутентификации.

Глава 27

1. *Какие три типа фреймов распространяет прозрачный мост методом лавинной маршрутизации?*

   Ответ: Неизвестные одноадресные фреймы (когда в таблице моста нет записи, соответствующей MAC-адресу приемника), широковещательные фреймы и многоадресные фреймы.

2. *Как мост узнает относительное расположение рабочей станции?*

   Ответ: Мост узнает о направлении, в котором нужно посылать фреймы, чтобы достичь станции, путем построения таблицы мостов. Мост строит таблицу, исследуя MAC-адреса источников каждого получаемого фрейма и связывая этот адрес с портом-приемником.

3. *Какие два модуля PDU генерирует прозрачный мост и для чего они используются?*

   Ответ: Прозрачные мосты создают конфигурационный PDU или PDU изменения топологии. Конфигурационные PDU помогают мостам исследовать топологию сети и избегать петель. PDU изменения топологии позволяют мостам повторно исследовать топологию сети в случае значительных изменений, например, когда один из сегментов не может больше поддерживать связность или в случае образования новой петли.

4. *В чем состоит разница между пересылкой и лавинной маршрутизацией?*

   Ответ: Мост пересылает фрейм через один интерфейс, если приемник подключен к порту, отличному от того, к которому подключен источник. Если неизвестно, где находится приемник, выполняется лавинная маршрутизация.

5. *После того как топология связующего дерева определена, мосты делятся на две категории: корневые и назначенные мосты, а их порты настраиваются на различные режимы — корневых и назначенных портов. Если в сети есть 10 мостов и 11 сегментов, сколько из них будет принадлежать широковещательному домену?*

   Ответ: В широковещательном домене существует только один корневой мост, а все остальные мосты являются назначенными. В итоге получаем один корневой мост и девять назначенных. Каждому сегменту нужен один назначенный порт: всего — десять назначенных портов. Каждый мост, кроме корневого, должен иметь единственный корневой порт: всего — девять корневых портов.

Глава 28

1. *При соединении между собой различных передающих сред, таких как Ethernet и Token Ring, возникают различные проблемы, для решения которых используются*

мостовые соединения с трансляцией. Перечислите и опишите четыре метода решения вышеупомянутых проблем.

Ответ: Для того чтобы преобразовать адрес из канонического формата в неканонический, нужно инвертировать каждый байт адреса. Например, третий октет (0x0C) в двоичной системе выглядит так: 00001100. Изменение на обратный порядок даст 00110000. В шестнадцатеричной записи это 0x30. Проделав такую процедуру с каждым байтом адреса, получим неканонический адрес 00-00-30-88-44-CC.

2. *Одна из проблем мостового соединения с трансляцией состоит в необходимости переупорядочивать биты каждого фрейма, передаваемого между сегментами Ethernet и Token Ring. Если станция Ethernet передает данные станции Token Ring с MAC-адресом 00-00-0C-11-22-33 (канонический формат), то как будет выглядеть MAC-адрес Token Ring (неканонический формат)?*

   Ответ: Нет. Для того чтобы трансляционный мост корректно преобразовывал все нужные поля в фрейме, он должен понимать формат протокола. Следовательно, если мост не понимает протокола, он не сделает всех нужных преобразований и нарушит формат этого протокола.

3. *Может ли трансляционный мост работать с любыми сетями и протоколами Ethernet и Token Ring?*

   Ответ: Мост прозрачной маршрутизации от источника понимает как фреймы маршрута от источника, так и фреймы прозрачных мостовых соединений. Поэтому он передает и фреймы с RIF-полем, и фреймы без него. Мост обычной маршрутизации от источника может передавать только фреймы с RIF-полем.

Глава 29

1. *В чем заключается основное различие в процессе передачи между прозрачными мостами и мостами с маршрутизацией от источника?*

   Ответ: Прозрачные мосты определяют, нужно ли передавать фрейм и по какому маршруту согласно локальной таблице моста. В SRB-сети источник предписывает маршрут до приемника и указывает желательный маршрут в RIF.

2. *В стандартах SRB не определен способ, с помощью которого источник выбирает маршрут к получателю из нескольких вариантов. В настоящей главе перечислены четыре метода принятия такого решения и сказано, что чаще всего выбирается маршрут первого полученного фрейма. Какие предположения о сети может сделать источник при использовании этого метода?*

   Ответ: Источник может предполагать, что фрейм прибыл первым благодаря большей пропускной способности каналов, меньшей загруженности системы и меньшим задержкам в мостовом оборудовании. Поэтому данный маршрут может быть более предпочтительным.

3. *Каким образом станции и мосты узнают, существует ли определенный во фрейме маршрут от источника?*

   Ответ: По значению бита RII. Если в фрейме есть RIF, бит RII установлен.

4. *Какие проблемы возможны в большой SRB-сети с несколькими альтернативными маршрутами?*

   Ответ: По сети с такой топологией может распространиться много фреймов-анализаторов. Поскольку анализаторы являются широковещательными фреймами, на них затрачивается полоса пропускания всего широковещательного домена и циклы CPU конечных станций.

5. *Для номера моста отводится всего 4 бита. Означает ли это, что мостов может быть не более 16 (24=16)? Обоснуйте свой ответ.*

   Ответ: Нет, не означает. Это лишь говорит о том, что может быть не более 16 мостов, соединяющих одни и те же два соседних кольца.

6. *Можно ли подключить к центральному кольцу несколько мостов с одинаковым номером?*

   Ответ: Да, можно, если только ни один из этих мостов не соединяет одни и те же два кольца.

7. *Для номера кольца отводится 12 битов. Может ли сеть состоять из более чем 4096 колец (212=4096)? Обоснуйте свой ответ.*

   Ответ: Нет, не может, потому что это число определяет общее количество колец. Номер кольца должен быть уникален.

Глава 30

1. *Многоуровневый коммутатор повторяет действия маршрутизатора после того, как маршрутизатор обработает первый фрейм. Что делает многоуровневый коммутатор с заголовками 2-го и 3-го уровней для того, чтобы точно выполнить имитацию работы маршрутизатора?*

   Ответ: Коммутатор должен модифицировать MAC-адреса источника и приемника в заголовке 2-го уровня так, чтобы казалось, что фрейм пришел через маршрутизатор или рабочую станцию. Кроме того, в заголовке 3-го уровня коммутатор должен изменить IP-значение времени существования.

2. *На какой тип межсетевых устройств больше всего похож коммутатор локальной сети?*

   Ответ: Коммутатор локальной сети ведет себя как многопортовый мост.

3. *В настоящей главе были описаны два магистральных протокола. В каких случаях применяется протокол IEEE 802.1Q?*

   Ответ: Если нужно соединить магистралью коммутаторы разных производителей. Остальные магистральные протоколы предназначены для оборудования определенного производителя.

4. *Какой метод коммутации защищает полосу пропускания сетевых сегментов от фреймов с ошибками?*

   Ответ: При коммутации с промежуточным хранением передача фрейма происходит только после проверки фрейма на целостность. Если коммутатор получает фрейм с ошибкой, то он его отбрасывает.

5. *Каким образом коммутатор с промежуточным хранением определяет, что фрейм содержит ошибку?*

   Ответ: Этот коммутатор использует CRC, чтобы определить, произошли ли какие-либо изменения в фрейме. Коммутатор вычисляет CRC полученного фрейма и сравнивает его со значением CRC, переданным вместе с фреймом. Если они отличаются, значит, фрейм изменился при передаче и будет удален.

6. *Пересекают ли маршрутизаторы границы VLAN?*

   Ответ: Нет. VLAN являются широковещательными доменами и описывают область распространения по сети широковещательных фреймов. Маршрутизаторы не обрабатывают широковещательные пакеты. Поэтому один и тот же VLAN не может существовать на двух портах маршрутизатора.

7. *Чем отличается магистральный канал от канала доступа?*

   Ответ: Канал доступа передает трафик одного VLAN. Трафик канала доступа выглядит как обычный фрейм Ethernet. Магистральный канал передает трафик нескольких VLAN по одной физической линии связи. Магистрали инкапсулируют фреймы Ethernet с другой информацией, чтобы обеспечить мультиплексирование.

8. *До появления коммутаторов и VLAN-сетей администраторы назначали пользователям сетевые ресурсы, исходя не из потребностей пользователей, а из других соображений. Из каких именно?*

   Ответ: Раньше администраторы назначали пользователям сетевые ресурсы на основании их физического соседства с устройствами и кабелями.

Глава 31

1. *Назовите четыре компонента LANE.*

   Ответ: Клиент эмуляции LAN (LEC), сервер конфигурации эмуляции LAN (LECS), сервер эмуляции LAN (LES), сервер широковещательных сообщений и сообщений для неизвестных адресатов (BUS).

2. *Какой компонент LANE содержит таблицу ARP сети ATM?*

   Ответ: Базу данных MAC- и ATM-адресов клиентов (LEC) содержит сервер эмуляции LAN (LES).

3. *Какой компонент LANE управляет компонентами ELAN?*

   Ответ: В роли устройства управления компонентами сети выступает сервер конфигурации LANE (LECS).

4. *Назовите две функции интерфейса частных сетей (PNNI).*

   Ответ: Определение топологии сети ATM и создание коммутируемой сети.

5. *По какому полю заголовка ATM проверяется целостность заголовка?*

   Ответ: Поле HEC проверяет заголовок на наличие ошибок и может исправить один ошибочный бит.

6. *В чем заключается основное отличие между заголовками UNI и NNI?*

   Ответ: Заголовок UNI содержит 8-разрядное поле VPI и 4-разрядное поле GFC. В заголовке NNI поле GFC входит в 12-разрядное поле VPI.

7. *Какой режим адаптации наиболее подходит для обмена сигналами T1 между мини-АТС в сети ATM?*

   Ответ: Для трафика с постоянной скоростью передачи, такого как T1, лучше всего подходит AAL1.

8. *Какой режим адаптации наиболее часто применяется для передачи данных по сети ATM?*

   Ответ: Подходящим способом адаптации для трафика данных, производимого, например, маршрутизаторами или подключенными к сети ATM рабочими станциями, является AAL5.

9. *Какое значение VCI резервируется для запросов установки соединения от конечных ATM-устройств?*

   Ответ: Для конечных устройств, посылающих сигнальные запросы входному ATM-коммутатору на соединение с другим устройством, резервируется VCI = 5.

10. *Какой протокол ATM облегчает работу администратора, автоматически обеспечивая совместимость определенных параметров двух устройств, подключенных к одному и тому же каналу?*

    Ответ: Протокол ILMI позволяет двум устройствам обмениваться данными и использовать общие параметры ATM, обеспечивающие функционирование канала.

11. *Какой протокол ATM используется исключительно при соединении ATM-коммутаторов?*

    Ответ: PNNI, протокол маршрутизации ATM.

12. *Чем отличается PVC от SVC?*

    Ответ: PVC (постоянное виртуальное соединение) управляется вручную. Каждый элемент такого соединения между источником и приемником необходимо настраивать отдельно. PVC неустойчиво к сбоям оборудования и среды передачи. SVC (коммутируемое виртуальное соединение) автоматически устанавливает соединение между источником и приемником. Источник сообщает, что ему необходимо соединение, и сеть создает его.

13. *Какова цель адаптационного уровня?*

14. Ответ: На адаптационном уровне происходит преобразование пользовательских данных в ячейки полезной нагрузки. В некоторых режимах адаптации данные занимают все 48 байт этого поля, в других несколько бит этого поля используются в служебных целях.

15. *Каковы преимущества MPOA?*

    Ответ: У MPOA есть два преимущества. Во-первых, он снижает нагрузку на маршрутизаторы, так как они не должны поддерживать постоянный поток данных. Во-вторых, MPOA может уменьшить количество пересечений данными сети ATM. Без MPOA данные должны пересекать все ELAN по пути к приемнику. С применением MPOA создается одно соединение, что позволяет данным пересекать сеть один раз.

Глава 32

1. *Каким образом при распределении исходящего потока по требованию находящееся в восходящем направлении LSR-устройство узнает, что ему нужна метка?*

   Ответ: Протоколы одноадресной маршрутизации распределяют информацию о сети. Когда входному LSR нужно передать фрейм в новую сеть, он может запросить метку у выходного LSR.

2. *FIB представляет собой информационную базу пересылки (Forwarding Information Base). Чем она отличается от LFIB — информационной базы пересылки по метке (Label Forwarding Information Base)?*

   Ответ: Таблицы FIB создаются по данным протоколов маршрутизации OSPF, BGP, IS-IS и т.п. LSR обращаются к этим таблицам, когда им нужна связка метка/маршрут. Сами связки содержатся в LFIB, где в одной таблице указываются приемник сети, метки и интерфейсы.

3. *Каковы два режима работы протокола LDP?*

   Ответ: Один режим представляет собой незапрашиваемое распределение исходящего потока, когда LSR выпускает связку без запроса от соседнего LSR. Второй режим представляет собой запрашиваемый поток, когда LSR запрашивает такую связку.

4. *Рекомендуется, чтобы соседние LSR-устройства работали в одном режиме протокола LDP. Что произойдет, если находящееся в восходящем направлении LSR-устройство работает в режиме распределения исходящего потока без запроса, а выходное LSR-устройство — в режиме запрашиваемого исходящего потока?*

   Ответ: В этом случае метки не будут распределены. Входной LSR предполагает, что ему не нужно запрашивать связку, в то время как выходное устройство предполагает, что ему не нужно создавать связку, если на нее не поступал запрос. Ни один из LSR не начнет распределения меток.

5. *Если маршрутизатор производителя уже использует высокоскоростную коммутацию и кэширование для передачи фреймов, то производительность не является достаточным мотивом для использования коммутации MPLS. Существуют ли иные причины, которые могут сделать целесообразным внедрение MPLS в такой сети?*

   Ответ: Перераспределение потоков может оптимизировать сеть, так как администратор будет иметь возможность выбирать путь между пунктами в зависимости от политик. В политиках могут учитываться такие параметры, как загрузка сети, безопасность и некоторые другие элементы. В противном случае администратор предоставляет выбор пути протоколам маршрутизации по адресу приемника.

Глава 33

1. *DLSw обеспечивает подтверждение на канальном уровне. Что означает подтверждение на канальном уровне? В чем его преимущества?*

   Ответ: Подтверждения на канальном уровне (acks) относятся к процессу в пределах конечного устройства. Подтверждения передаются между конечным устройством и локальным DLSw-коммутатором (маршрутизатором). Если бы не

было подтверждений на канальном уровне, подтверждение должно было бы пройти весь путь до другого конечного устройства, причем, возможно, пересечь несколько сегментов локальной сети и глобальную сеть. Последнее часто связано со значительными задержками прохождения данных, что приведет к превышению лимита времени и сбою.

2. *Какой транспортный протокол используется для передачи данных протокола SSP DLSw? Каковы его преимущества и недостатки?*

   Ответ: В SSP используется протокол TCP. Ему присущи обычные преимущества надежного транспортного протокола с мониторингом потока данных и повторной передачей данных в случае их потери (номера последовательностей и подтверждения). Однако TCP не очень хорошо адаптируется для случая равноправных отношений между большим количеством DLSw-коммутаторов.

3. *Назовите и опишите три этапа работы DLSw.*

   Ответ: На первом этапе равноправные DLSw-коммутаторы устанавливают два TCP-соединения. На втором же — они обмениваются сведениями о возможностях, что позволяет гарантировать настройку обоих коммутаторах на одинаковые режимы. Это особенно необходимо в среде, где используются DLSw-узлы разных производителей. На третьем этапе, этапе открытия каналов, конечные устройства устанавливают соединение с объектом-приемником. Для этого устанавливается локальное соединение между конечным устройством и DLSw-коммутатором, а также между DLSw-коммутаторами, чтобы выяснить, какому из равноправных DLSw-коммутаторов нужно отправить данные.

4. *Какие протоколы поддерживает DLSw?*

   Ответ: SNA и NetBIOS. Оба они зависят от подтверждений на канальном уровне.

5. *Что такое стандартный процесс 2-уровня, используемый без DLSw?*

   Ответ: До появления DLSw системы использовали алгоритм SRB. Однако из-за ограниченного количества транзитных передач (7) и неэффективной обработки широковещательного трафика SRB не очень хорошо адаптируется к глобальным сетям.

6. *В DLSw используются два типа сообщений. Каковы эти сообщения и у какого из них заголовок больше? Есть ли между ними что-либо общее?*

   Ответ: Существует два типа сообщений — для управления потоком и для получения информации о нем. Длина заголовка управляющего фрейма составляет 72 байтов, а информационного — 16 байтов. Формат первых 16 байтов этих заголовков одинаков.

Глава 34

1. *Какие два протокола маршрутизации определены в пакете OSI?*

   Ответ: Протокол "конечная система-промежуточная система " (End System-to-Intermediate System — ES-IS) и протокол "промежуточная система-промежуточная система" (Intermediate System-to-Intermediate System — IS-IS).

2. *Опишите протокол сетевой службы OSI, не требующий подтверждения соединения.*

   Ответ: Сетевая служба OSI, не требующая подтверждения соединения, реализуется при помощи сетевого протокола, не требующего подтверждения соедине-

ния (Connectionless Network Protocol — CLNP) и сетевой службы, не требующей подтверждения соединения (Connectionless Network Service — CLNS). CLNP и CLNS описаны стандартом ISO 8473.

3. *Опишите протокол сетевой службы OSI, ориентированный на соединение.*

   Ответ: Сетевая служба OSI, ориентированная на соединение, реализуется при помощи сетевого протокола, ориентированного на соединение (Connection-Oriented Network Protocol — CONP) и сетевой службы в режиме соединения (Connection-Mode Network Service — CMNS).

4. *Как реализуются запросы служб на сеансовом уровне в протоколах OSI?*

   Ответ: Запросы делаются в точках доступа к сеансовой службе (session-service access points, SSAP). SS-пользователи однозначно идентифицируются по SSAP-адресу.

5. *Что такое CASE-элементы?*

   Ответ: Сервисные элементы общих приложений - (Common-Application Service Elements — CASE) представляют собой ASE-элементы, предоставляющие службы, которые используются многими процессами приложения. Часто один элемент приложения использует несколько CASE-элементов.

6. *Назовите среды, поддерживаемые пакетом протоколов OSI.*

   Ответ: IEEE 802.2 LLC, IEEE 802.3, Token Ring/IEEE 802.5, Fiber Distributed Data Interface (FDDI) и X.25.

7. *Как был создан пакет протоколов OSI?*

   Ответ: Спецификации OSI были задуманы и реализованы двумя организациями международных стандартов: Международной организацией по стандартизации (International Organization for Standardization — ISO) и Сектором телекоммуникационных стандартов Международного телекоммуникационного союза (International Telecommunication Union—Telecommunications Standards Sector — ITU-T).

8. *Опишите протоколы сеансового уровня в пакете протоколов OSI.*

   Ответ: Реализация сеансового уровня пакета протоколов OSI состоит из сеансового протокола и сеансовой службы. Сеансовый протокол обеспечивает обмен данными между пользователями сеансовой службы (SS-пользователи) и сеансовой службой. Такие запросы делаются в точках доступа к сеансовой службе (session-service access points — SSAP). SS-пользователи однозначно идентифицируются по SSAP-адресу.

9. *Опишите протоколы уровня представлений пакета протоколов OSI.*

   Ответ: Реализация уровня представлений пакета протоколов OSI состоит из протокола представлений и службы представлений. Протокол представлений обеспечивает обмен данными между пользователями службы представлений (PS-пользователям) и службой представлений.

10. *Назовите две категории ASE-элементов.*

    Ответ: ASE-элементы делятся на две категории: сервисные элементы общих приложений -элементы (common-application service entities — CASE) и сервисные элементы конкретных приложений - (specific-application service entities — SASE). В одном элементе приложения могут присутствовать и те, и другие одновременно.

Глава 35

1. *Где содержатся описания протоколов Internet*

   Ответ: В документации RFC.

2. *Каковы две основные задачи IP*

   Ответ: Доставка дейтаграмм через объединенную сеть без подтверждения соединения методом наименьших затрат; фрагментация и повторная сборка дейтаграмм для поддержки каналов передачи данных с различными максимальными размерами передаваемого модуля данных (MTU).

3. *Какое поле IP-пакета предотвращает зацикливание пакетов в неверно сконфигурированной сети?*

   Ответ: По мере прохождения маршрутизаторов счетчик TTL (Time-to-Live — время существования) постепенно уменьшается до нуля. Когда TTL достигает нуля, пакет отбрасывается.

4. *В каком виде обычно представляется IP-адрес?*

   Ответ: 32-разрядный IP-адрес группируется по 8 бит, разделенных точками и представляемых в десятеричном формате,известном как десятичная запись с разделителями (dotted decimal notation). Каждый бит октета имеет двоичный вес (128, 64, 32, 16, 8, 4, 2, 1). Минимальное значение октета равно 0, максимальное — 255.

5. *Как определяется класс IP-адреса?*

   Ответ: По первому октету адреса.

6. *Каково назначение маски подсети в IP-адресе?*

   Ответ: Маска подсети определяет, какая часть адреса определяет сеть и какая — узел.

7. *Каково назначение протокола ARP?*

   Ответ: Протокол преобразования адресов) (Address Resolution Protocol — ARP используется для преобразования IP-адресов 3-го уровня в MAC-адреса 2-го уровня.

8. *Каково назначение протокола ICMP?*

   Ответ: Протокол управления сообщениями в сети (Internet Control Message Protocol — ICMP Internet) выдает сообщения об ошибках и другую информацию об обработке IP-пакетов.

9. *Какой тип доставки данных предоставляет TCP?*

   Ответ: TCP обеспечивает надежную передачу данных в среде IP, используя сеанс, ориентированный на соединение.

10. *Чем протокол UDP отличается от протокола TCP?*

    Ответ: Протокол передачи дейтаграмм пользователя) (User Datagram Protocol — UDPпредставляет собой транспортный протокол без подтверждения соединения, не гарантирующий доставку данных. Протокол управления передачей (Transmission Control Protocol — TCP) — протокол, ориентированный на соединение, который гарантирует доставку данных.

Глава 36

1. *Какой стандарт принят в настоящее время?*

   Ответ: IPv4.

2. *Что является основной причиной разработки IPv6?*

   Ответ: Адресация, точнее ее недостаток. Многие полагают, что 4 миллиарда адресов, доступных в IPv4, вот-вот будут заполнены. IPv6 сможет решить многие проблемы, но он пока еще не до конца разработан и не является стандартом.

3. *Сколько битов использует новая расширенная адресация?*

   Ответ: При расширенной адресации происходит переход от 32-разрядного адреса к 128-разрядному.

4. *В чем состоят другие преимущества расширенной адресации?*

   Ответ: Новые методы одноадресатной и многоадресатной передачи, а также вводит шестнадцатеричную систему записи IP-адреса и использует в качестве разделителей не точки, а двоеточия.

5. *Какие новые способы передачи появились в IPv6?*

   Ответ: Одноадресатная, многоадресатная и широковещательная.

6. *Что такое одноадресатная передача?*

7. Ответ: Одноадресатная передача представляет собой обмен данными между одним узлом и одним получателем.

8. *Что такое многоадресатная передача?*

9. Ответ: Многоадресатная передача представляет собой обмен данными между одним узлом и несколькими получателями.

10. *Что такое широковещательная передача?*

    Ответ: Широковещательная передача представляет собой обмен данными между одним отправителем и всеми доступными станциями.

Глава 37

1. *Какие два типа протоколов маршрутизации используются протоколом IPX.*

   Ответ: Это протокол маршрутной информации (Routing Information Protocol — RIP) и протокол коммуникационных услуг в среде NetWare (NetWare Link-State Protocol).

2. *Какая информация используется протоколом RIP IPX для определения маршрута передачи данных по сети?*

   Ответ: Для определения сетевого маршрута IPX RIP использует интервалы таймера (tics). В случае равенства этих показателей используется количество проходов через маршрутизаторы (hops).

3. *На какие две части делится адрес IPX*

   Ответ: На адреса сети и узла.

4. *Как станции Novell обнаруживают доступные в сети службы?*

Ответ: С помощью протокола анонсирования служб (Service Advertisement Protocol —SAP).

5. *Какой протокол используется на транспортном уровне?*

   Ответ: Наиболее распространенным транспортным протоколом NetWare является протокол последовательного обмена пакетами (Sequenced Packet Exchange — SPX).

6. *Как станции IPX преобразуют MAC-адреса в адреса протокола IPX?*

   Ответ: Поскольку MAC-адрес используется в сети IPX как адрес узла, никакого преобразования не требуется.

7. *Какое нововведение в NetWare 4.0 уменьшает необходимость в протоколе SAP?*

   Ответ: Служба каталогов NetWare (NetWare Directory Services — NDS).

8. *Какие службы обеспечиваются базовым протоколом NetWare (NetWare Core Protocol)?*

   Ответ: Основной протокол NetWare представляет собой набор серверных процедур, разработанных для обслуживания запросов приложений, которые поступают, например, от оболочки NetWare. Службами NCP являются доступ к файлам и принтерам, управление именами, система учета ресурсов и система защиты, а также файловая синхронизация.

9. *Опишите поддержку NetBIOS в сетях NetWare.*

   Ответ: NetWare поддерживает интерфейс сеансового уровня NetBIOS спецификаций IBM и Microsoft. Программы эмуляции NetWare NetBIOS позволяют запускать в среде NetWare программы, написанные для промышленного стандарта интерфейса NetBIOS.

10. *Необходимо ли фильтровать данные протокола SAP?*

    Ответ: Протокол SAP не нуждается в передаче по медленным глобальным каналам, поэтому применение фильтров может снизить объем трафика, генерируемого IPX для этих типов соединений.

Глава 38

1. *Что такое зона AppleTalk?*

   Ответ: Зона AppleTalk представляет собой логическая группа узлов или сетей, определенная при конфигурации сети сетевым администратором. Эти узлы и сети не обязательно должны быть физически смежными.

2. *Назовите четыре основных средства реализации доступа к среде передачи для протоколов AppleTalk.*

   Ответ: EtherTalk, LocalTalk, TokenTalk и FDDITalk.

3. *Как рабочим станциям назначаются адреса узлов?*

   Ответ: При создании узла LLAP присваивает узлу случайный идентификатор (ID узла). Уникальность этого ID проверяется путем передачи специального пакета, адресованного выбранному ID. На этот запрос приходит ответ, значит, такой ID уже есть. Тогда узлу присваивается другой случайный идентификатор и передача пакета повторяется. Это происходит до тех пор, пока не обнаружится ID, от которого не будет получен ответ.

4. *Какой протокол маршрутизации сетевого уровня, используемый в сетях AppleTalk, является основным?*

   Ответ: Основным протоколом маршрутизации сетевого уровня в наборе AppleTalk является протокол доставки дейтаграмм (Datagram Delivery Protocol — DDP). Он обеспечивает передачу дейтаграмм между сокетами в сетях AppleTalk методом наименьших затрат без подтверждения соединения.

5. *Назовите пять важнейших протоколов транспортного уровня в сетях AppleTalk.*

   Ответ: RTMP, NBP, AURP, ATP и AEP.

Глава 39

1. *Что разработала IBM для того, чтобы приспособить свой протокол к одноранговой сети?*

   Ответ: Протоколы Advanced Peer-to-Peer Networking (APPN) и Advanced Program-to-Program Computing (APPC).

2. *Какие типы физических устройств поддерживает SNA?*

   Ответ: Рабочие станции, коммуникационные контроллеры, контроллеры установки и терминалы.

3. *Какие три типа сетевых адресуемых модулей поддерживает SNA?*

   Ответ: Логические модули, физические модули и контрольные точки.

4. *Каковы функции логического модуля?*

   Ответ: Порт доступа пользователя к сети SNA.

5. *Каковы функции физического модуля?*

   Ответ: Наблюдение и управление подключенными сетевыми каналами и другими сетевыми ресурсами данного узла.

6. *Каковы функции контрольной точки?*

   Ответ: Управление узлами SNA и их ресурсами.

7. *Назовите три типа хорошо известных узлов в APPN.*

   Ответ: Низкоуровневые, конечные и сетевые узлы.

8. *Назовите четыре основные категории служб в APPN.*

   Ответ: Настройка, каталоги, топология и службы маршрутизации и сеансов.

9. *Для чего предназначена база данных сетевой топологии?*

   Ответ: Службы каталогов.

Глава 40

1. *Как узлы DECnet используют назначаемые производителем MAC-адреса?*

   Ответ: Они не используют MAC-адреса. Адреса сетевого уровня встраиваются в адреса MAC-уровня в соответствии с алгоритмом, который умножает номер зоны на 1024 и прибавляет к результату номер узла. Полученный 16-разрядный десятичный адрес преобразуется в шестнадцатеричное число и присоединяется к

адресу AA00.0400 с перестановкой байтов, чтобы наименее значимые байты передавались первыми.

2. *Какой протокол в DECnet Phase IV отвечает за маршрутизацию?*

   Ответ: В DECnet Phase IV маршрутизация реализована при помощи протокола маршрутизации DECnet (DECnet Routing Protocol — DRP). Этот протокол относительно прост и эффективен, его основная функция — определение оптимального маршрута в сети DECnet Phase IV.

3. *Какие функции выполняет протокол NSP?*

   Ответ: Протокол сетевых служб (Network-Services Protocol — NSP) представляет собой фирменный, ориентированный на соединение, протокол конечных коммуникаций, разработанный Digital и отвечающий за установку и разрыв соединений между узлами, фрагментацию и компоновку сообщений и управление ошибками.

4. *Какие функции выполняет протокол SCP?*

   Ответ: Протокол управления сеансом (Session Control Protocol — SCP) представляет собой протокол уровня управления сеансом DECnet Phase IV, выполняющий несколько функций. В частности, SCP запрашивает у конечных устройств логическое соединение, получает от конечных устройств запросы логических соединений, принимает или отвергает запросы логических соединений, переводит имена в адреса и обрывает логические соединения.

5. *Какие функции в DECnet выполняются на уровне пользователя?*

   Ответ: Уровень пользователя DNA поддерживает пользовательские службы и программы, которые взаимодействуют с пользовательскими приложениями. Пользователь взаимодействует непосредственно с этими приложениями, а приложения используют службы и программы на уровне пользователя.

Глава 41

1. *Может ли протокол IBGP использоваться вместо протокола IGP (RIP, IGRP, EIGRP, OSRF или ISIS)?*

   Ответ: И да, и нет. Необходимо помнить, что информация о следующем узле от EBGP переносится в IBGP. Если у IBGP нет маршрута к следующему узлу, то маршрут отбрасывается. Обычно IGP необходим для обмена маршрутами к следующему узлу, однако есть возможность достичь того же, используя статические маршруты на всех маршрутизаторах, на которых выполняется IBGP. Так что на этот вопрос можно ответить положительно в случае, если вы хотите использовать и поддерживать статические маршруты. В противном случае ответ будет отрицательным.

2. *Предположим, что маршрутизатор BGP узнает об одинаковых маршрутах от двух разных узлов EBGP. Значение атрибута AS_path от узла 1 равно {2345,86,51}, а от узла 2 — {2346,51}. Какие атрибуты BGP могли бы быть скорректированы, чтобы принудить маршрутизатор предпочесть маршрут, о котором сообщил узел 1?*

   Ответ: Weight и Local Preference. Оба эти атрибута имеют больший приоритет по сравнению с длиной атрибута AS_path.

3. *Справедливо ли утверждение, что протокол BGP может использоваться только провайдерами службы Internet?*

   Ответ: Нет. BGP может использоваться для масштабирования сетей крупных предприятий. Большую сеть можно разбить на сегменты, на каждом из которых выполняется IGP. Обмен маршрутной информацией между сегментами может осуществляться с помощью BGP.

4. *Если непосредственно подключенный интерфейс перераспределяется в протокол BGP, то каково будет значение атрибута Origin для этого маршрута?*

   Ответ: Значение атрибута Origin для любого перераспределенного маршрута — Incomplete.

Глава 42

1. *Назовите четыре основные технологии, используемые протоколом EIGRP.*

   Ответ: В EIGRP используются четыре основные технологии: обнаружение/восстановление соседних маршрутизаторов, транспортный протокол с достоверной передачей (RTP), машина с конечным числом состояний алгоритма DUAL и модульная архитектура, которая обеспечивает поддержку новых протоколов, позволяя легко добавлять их в существующую сеть.

2. *Почему EIGRP эффективнее, чем IGRP?*

   Ответ: В отличие от большинства других протоколов маршрутизации по вектору расстояния, EIGRP не выполняет периодического обновления маршрутных таблиц между соседними маршрутизаторами. Вместо этого он использует механизм обнаружения/восстановления соседних маршрутизаторов, что позволяет им постоянно быть осведомленными о доступности друг друга. Пока маршрутизатор получает пакеты приветствия от соседних маршрутизаторов, он считает, что эти маршрутизаторы являются работоспособными. Важно и то, что он предполагает, что все его маршруты, зависящие от прохождения через соседние маршрутизаторы, являются корректными. Таким образом, EIGRP намного эффективнее, чем традиционные протоколы маршрутизации по вектору расстояния, так как он гораздо меньше нагружает маршрутизаторы и средства передачи данных в нормальном режиме работы.

3. *Каким образом RTP улучшает сходимость?*

   Ответ: RTP гарантирует доставку пакетов EIGRP между соседними маршрутизаторами. Однако не все пакеты EIGRP, которыми обмениваются соседние маршрутизаторы, должны отсылаться с гарантией. Некоторые пакеты, такие как пакеты приветствия, могут отсылаться без нее. Но, что более важно, они могут многоадресными, а это исключает необходимость в отправке отдельных дейтаграмм с той же полезной нагрузкой каждому маршрутизатору в отдельности. Указанное обеспечивает быструю сходимость сети EIGRP, даже если ее отдельные звенья имеют разные скорости передачи.

4. *Зачем EIGRP маркирует определенные маршруты?*

   Ответ: EIGRP поддерживает внутренние и внешние маршруты. Внутренние маршруты AS полностью содержатся в этой AS. Внешними маршрутами назы-

ваются те, информация о которых поступает от соседних маршрутизаторов, находящихся вне AS. Внешние маршруты маркируются информацией, которая идентифицирует их источник. Это позволяет сетевому администратору разрабатывать настраиваемую стратегию междоменной маршрутизации.

Глава 43

1. *Для чего предназначены сеансовые соединители SNA?*

   Ответ: Сеансовые соединители SNA IBM используются для связи между адресными пространствами, когда сеанс пересекает несколько таких пространств. Существует три типа сеансовых соединителей: граничные функции, межсетевые шлюзы SNA (SNA Network Interconnection — SNI) и функции промежуточной маршрутизации APPN.

2. *Что создается, когда сетевой узел посредством запроса LOCATE определяет, что два конечных узла подключены к общей среде передачи?*

   Ответ: Приемник запроса LOCATE определяется сетевым узлом (network node, NN). Если сетевой узел обнаруживает, что оба конечных узла (источник и приемник) подключены к одной среде передачи (например, Token Ring), то используется виртуальный узел (virtual node — VN), который соединяет эти две конечные точки и образует сеть соединений.

3. *Верно ли утверждение, что все NAU в пределах подзоны имеют одинаковый адрес элемента?*

   Ответ: Нет. Все NAU в пределах подзоны имеют общий адрес подзоны, но разные адреса элементов.

Глава 44

1. *Перечислите достоинства протокола IGRP, которые отсутствуют в протоколе RIP.*

   Ответ: Несмотря на свой долговременный успех в качестве протокола маршрутизации внутренних шлюзов, RIP имеет фундаментальные ограничения, которые нелегко обойти. Например, в нем (и в RIP 2) максимальное количество маршрутных пересылок равно 16. Это ограничивает размер и сложность сети, эффективно маршрутизируемой при помощи протокола RIP. Другими ограничениями RIP являются распределение нагрузки только методом равных затрат и единственная, простая маршрутная метрика (счетчик пересылок). IGRP разрабатывался специально как альтернатива RIP: он должен был так же легко реализоваться и администрироваться, как RIP, но не иметь его фундаментальных ограничений.

2. *Как администратор может влиять на выбор маршрута?*

   Ответ: Сетевой администратор может принять стандартные параметры IGRP или настроить производительность сети путем изменения четырех маршрутных метрик IGRP или изменения констант, определяющих их вес. Это математические компоненты составной маршрутной метрики IGRP предоставляют сетевому администратору значительную свободу маневра, позволяя ему придать боль-

шее или меньшее значение задержке, скорости передачи, надежности или степени загрузки канала при выборе оптимального маршрута.

3. *Что такое дисперсия и как она влияет на множественную маршрутизацию?*

   Ответ: Дисперсия представляет собой еще один параметр, который может устанавливаться или изменяться сетевым администратором для оптимизации сети IGRP. В сущности, дисперсия означает диапазон маршрутных затрат, используемых для выбора нескольких неравноценных избыточных маршрутов к данному получателю. Таким образом, дисперсия представляет собой механизм, благодаря которому IGRP поддерживает распределение нагрузки с разными затратами.

4. *Перечислите и опишите функции обеспечения стабильности IGRP.*

   Ответ: Для улучшения стабильности работы сети в IGRP используются интервалы задержки изменений, расщепление горизона и обратные обновления. Интервалы задержки изменений (holddowns) выбираются таким образом, чтобы не допустить восстановления информации о несуществующем маршруте. Расщепление горизонта (split horizon) исключает появление маршрутных петель, так как не позволяет маршрутизатору отправлять сообщения об обновлении маршрута соседнему маршрутизатору, от которого он первоначально получил эту информацию. Обратные обновления (poison-reverse updates) подобны расщеплению горизонта, но не ограничиваются смежными узлами. Таким образом, они предотвращают появление крупных маршрутных петель между несмежными маршрутизаторами.

5. *Какие таймеры используются в IGRP и каковы выполняемые функции?*

   Ответ: В IGRP применяется несколько функционально различных таймеров, в том числе таймер обновлений, таймер недействующих маршрутов, таймер периода задержки изменений и таймер исключения. Таймер обновлений маршрутов (update timer) определяет, насколько часто должны отправляться сообщения об обновлении маршрутов. Таймер недействующих маршрутов (invalid timer) определяет, сколько времени при отсутствии сообщений обновления маршрутизатор должен ожидать, прежде чем объявить этот маршрут недействующим. Таймер периода задержки изменений (hold-time period) определяет промежуток задержки внесения изменений. Наконец, таймер исключения (flush timer) определяет, сколько времени должно пройти до исключения маршрутизатора из таблицы маршрутизации. По умолчанию для IGRP это время в семь раз превышает период обновления маршрутизации.

Глава 45

1. *В каком диапазоне находятся доступные групповые IP-адреса?*

   Ответ: От 224.0.0.0 до 239.255.255.255.

2. *Каково назначение IGMP?*

   Ответ: IGMP используется для обмена данными между хостами и их локальным многоадресным маршрутизатором при присоединении и выходе из многоадресной группы.

3. *Каковы преимущества IGMP 2 по сравнению с IGMP 1*

   Ответ: В IGMP 2 есть сообщение о выходе из группы, благодаря которому значительно сокращается время ожидания за счет нежелательного трафика в LAN.

4. *Каковы возможные недостатки IGMP-прослушивания по сравнению с CGMP при использовании недорогих коммутаторов уровня 2*

   Ответ: IGMP-прослушивание требует, чтобы коммутатор проверял все многоадресные пакеты на наличие управляющего IGMP-сообщения. При использовании дешевых коммутаторов это может значительно снизить производительность.

5. *Каковы преимущества дерева кратчайших маршрутов (или источника) по сравнению с деревом общего доступа?*

   Ответ: Дерево источника обеспечивает оптимальный маршрут между каждым источником и каждым приемником, что сокращает простои в сети.

6. *Каковы преимущества дерева общего доступа?*

   Ответ: При использовании дерева общего доступа объем информации, хранимой в маршрутизаторах, минимален, следовательно, минимальны требования к памяти.

7. *Какую информацию использует маршрутизатор для RPF-проверки?*

   Ответ: Одноадресную таблицу маршрутизации.

8. *Почему независимая от протокола многоадресатная рассылка называется независимой?*

   Ответ: PIM работает с любыми одноадресатными IP-протоколами — RIP, EIGRP, OSPF, BGP или статическими маршрутами.

9. *В чем заключается основной недостаток MBGP?*

   Ответ: В возможном несоответствии одно- и многоадресатной топологии провайдеров.

10. *Как RP узнают об источниках от других RP при поморщи MSDP?*

    Ответ: RP настраиваются таким образом, чтобы быть равноправными MSDP-партнерами с другими RP. Каждая RP передает остальным сообщения об активном источнике (SA).

11. *Каково назначение альтернативных точек рандеву RP?*

    Ответ: Распределение нагрузки и отказоустойчивость.

Глава 46

1. *Для чего предназначен маршрутизатор 2-го уровня в схеме иерархической маршрутизации NLSP?*

   Ответ: Маршрутизатор 1-го уровня соединяет сегменты сети в пределах одной зоны маршрутизации. Маршрутизатор 2-го уровня соединяет зоны и действует в своей зоне как маршрутизатор 1-го уровня.

2. *В течение какого времени посылаются пакеты приветствия после того, как маршрутизатор инициализирован и начал работать?*

   Ответ: Пакеты приветствия рассылаются через активный интерфейс постоянно. По ним соседние маршрутизаторы узнают, что интерфейс или канал по-

прежнему активен и может быть использован. Если маршрутизатор не получает от соседнего маршрутизатора пакет приветствия в установленный промежуток времени, он считает, что интерфейс или канал более недоступны, и удаляет его из своей базы данных.

3. *Какой тип LSP посылается по WAN — одноадресатный или многоадресатный?*

   Ответ: Через WAN-сеть посылаются одноадресатные LSP-пакеты, содержащие IP-адрес соседнего маршрутизатора. В LAN-сетях посылаются многоадресные пакеты.

Глава 47

1. *Можно ли при использовании OSPF соединить две зоны, если интерфейс с зоной 0 есть только у одной AS?*

   Ответ: Да, можно, с помощью виртуального маршрута. У одной зоны есть интерфейс с зоной 0 (обычный). Создается еще одна AS — назовем ее зоной 2 — и соединяется с граничным маршрутизатором зоны 1. У зоны 2 нет интерфейса с зоной 0, поэтому нужно установить виртуальный маршрут с зоной 0 через зону 1. Когда такой маршрут будет создан, зона 2 будет вести себя так, как будто она связана с зоной 0 непосредственно. Когда потребуется послать пакет из зоны 1 в зону 2, этот пакет будет сначала отправлен в зону 0, которая перенаправит его в зону 2 по виртуальному маршруту, который снова проходит через зону 1.

2. *Зона 0 содержит пять маршрутизаторов (A, B, C, D и E), а зона 1 — три (R, S и T). О каких маршрутизаторах известно маршрутизатору T, если маршрутизатор S является граничным?*

   Ответ: Маршрутизатору T известно только о существовании маршрутизаторов R и S. Аналогично, маршрутизатору S известно только о существовании маршрутизаторов R и T, а также о граничных маршрутизаторах зоны 0. Зоны являются закрытыми, и обновления маршрутов содержат информацию только данной AS.

Глава 48

1. *Какие два типа сообщений передаются между системами по протоколу ES-IS?*

   Ответ: Между системами ES и IS через равные промежутки времени передаются сообщения приветствия IS и ES для поддержки соединения и обмена подсетевыми и сетевыми адресами.

2. *В чем состоит различие между маршрутизаторами IS-IS 1-го и 2-го уровней?*

   Ответ: маршрутизатор 1-го уровня видит только маршруты внутри данной зоны. Маршрутизатор 2-го уровня подсоединен как минимум к одному маршрутизатору 2-го уровня другой зоны.

3. *Опишите, каким образом маршрутизаторы протокола IS-IS осуществляют связь между собой в широковещательных сетях.*

   Ответ: Посредством отправки многоадресатных сообщений-приветствия маршрутизатор IS-IS с наивысшим приоритеттом становится DIS и анонсирует

псевдоузел. Все остальные маршрутизаторы IS-IS лишь отправляют и получают LSP от DIS. Процесс выбора DIS имеет наивысший приоритет.

4. *Каково первоначальное предназначение бита перегрузки?*

   Ответ: Этот бит является частью механизма, позволяющего маршрутизатору, которому недостаточно системных ресурсов, уведомить своих соседей от том, что далее его не следует рассматривать в качестве возможного маршрута для транзитных потоков данных.

5. *Что такое TLV?*

   Ответ: Аббревиатура TLV означает "значение типа длины" (Type Length Value). Это общий формат представления информации, которая передается в поле данных переменной длины пакетов приветствия и в модулях PDU протокола LSP. Типы TLV определены в первоначальной (исходной) ISO-спецификации и в нескольких расширениях RFC для IS-IS для данного поля, таких как CLNS и IPv4.

6. *Каким образом в каждом канале конфигурируется метрика протокола IS-IS?*

   Ответ: Протокол IS-IS использует одну стандартную обязательную метрику с максимальным значением оценки маршрута (maximum path value) равным 1024. Эта метрика произвольна и назначается сетевым администратором. Каждый отдельный канал имеет максимальное значение равное 64, а каналы маршрутов вычисляются путем суммирования значений для каналов.

Глава 49

1. *Каковы средства обеспечения устойчивости протокола RIP?.*

   Ответ: У RIP много средств обеспечения устойчивости, наиболее очевидным из которых является счетчик максимального количества узлов. Ограничение количества узлов маршрута уменьшает, если вообще не исключает, вероятность зацикливания в маршрутных петлях. Другими средствами обеспечения устойчивости являются разнообразные таймеры, способствующие тому, что в маршрутных таблицах хранятся только действующие маршруты. Кроме того, следует отметить расщепление горизонта и интервал задержки изменений, которые предотвращают распространение по сети ложной маршрутной информации.

2. *В чем состоит различие между маршрутизаторами IS-IS 1-го и 2-го уровней?*

   Ответ: Таймер ожидания предназначен для очистки RIP-узлов от некорректных маршрутов. Маршруты, которые не обновляются в течение заданного времени, скорее всего, являются неработоспособными из-за изменений, произошедших в сети. RIP поддерживает таймер ожидания для каждого известного маршрута. Когда время, определяемое этим таймером, истекает, маршрут помечается как неработоспособный, но сохраняется в таблице до тех пор, пока не истечет время, определяемое таймером сдвига.

3. *Какие две функции поддерживаются в версии RIP 2 и не поддерживаются в протоколе RIP?*

   Ответ: RIP 2 допускает использование простого механизма аутентификации для безопасного обновления таблиц. Но самое главное — RIP 2, в отличие от RIP, поддерживает маски подсети.

4. *Каков максимальный диаметр сети RIP?*

   Ответ: 15 узлов (транзитных участков). Если счетчик RIP принимает значение 16, это расценивается как ошибка.

Глава 50

1. *Обязательно ли переходить от существующего протокола маршрутизации к RSVP?*

   Ответ: RSVP *не является* протоколом маршрутизации. Он разработан для совместной работы с существующими протоколами маршрутизации. Поэтому переходить к новому протоколу маршрутизации для обеспечения совместимости с RSVP не нужно.

2. *Назовите три уровня служб RSVP и объясните, в чем состоит различие между ними.*

   Ответ: Существует три уровня служб RSVP: гарантированная доставка, гарантированная скорость и гарантированная задержка. Гарантированная доставка применяется для приложений, требующих не столько своевременной, сколько надежной доставки. Доставка с гарантированной скоростью используется для любого трафика, требующего постоянной полосы пропускания. Это такие приложения, как видеоконференции H.323, рассчитанные на постоянную скорость передачи. Третий уровень служб RSVP — с гарантированной задержкой — предназначен для трафика, требующего не столько надежной, сколько своевременной доставки данных.

3. *Какие существуют два класса резервирования RSVP и чем они отличаются друг от друга?*

   Ответ: Стиль резервирования представляет собой набор управляющих параметров, которые определяют механизм резервирования. RSVP поддерживает два основных типа стилей резервирования: раздельное и совместное. При раздельном резервировании каждому устройству-источнику в сеансе выделяется отдельный поток. При совместном резервировании для нескольких устройств-источников выделяется группа коммуникационных потоков. Каждый из этих стилей резервирования описывается набором фильтров.

4. *Что такое фильтры RSVP?*

   Ответ: Фильтр RSVP представляет собой специальный набор управляющих параметров, который определяет характеристики резервирования. Существуют следующие стили RSVP: групповой фильтр (wildcard-filter, WF), фиксированный фильтр (fixed-filter, FF) и явный совместный (shared-explicit, SE) фильтр.

5. *Как можно использовать RSVP, если в сети есть области, не поддерживающие RSVP?*

   Ответ: RSVP допускает туннелирование через сетевые области, не поддерживающие RSVP. Эта функция предназначена для поэтапного внедрения RSVP.

Глава 51

1. *Что представляет собой SMRP-адрес?*

   Ответ: SMRP-адресация основана на локальной сети создателя конечной точки. SMRP-адрес состоит из двух частей: 3-байтового номера сети и

1-байтового номера сокета. Каждая локальная сеть имеет диапазон уникальных сетевых номеров.

2. *Сообщение какого типа посылается при запросе между конечной точкой и узлом? Между узлом и конечной точкой?*

   Ответ: Запросы между конечной точкой и узлом являются многоадресатными, а запросы между узлом и конечной точкой могут быть как много-, так и одноадресатными.

3. *Как узел становится назначенным первичным узлом в сети?*

   Ответ: Основной процесс определения первичного и вторичного узлов начинается при запуске. Сначала новый узел пытается стать назначенным вторичным узлом в каждой локальной сети по очереди. Если это удается, он пытается стать назначенным первичным узлом. Передача данных начинается по запросу первичного или вторичного узла. Отсутствие ответа на запрос говорит об успешном, а положительный ответ — о неудачном согласовании.

Глава 52

1. *Чем обусловлена важность обеспечения безопасности в сети?*

   Ответ: Этого требуют широкое использование Internet-приложений, более быстрый доступ к Internet и законодательная база.

2. *Как повлияли на проблемы безопасности в сетях рост Internet и новые технологии?*

   Ответ: Рост Internet привел к появлению новых приложений, таких как потоковое видео и IP-телефония. Использование этих приложений и технологий привело к проявлению новых уязвимых точек в сети, которые повышают уровень угроз безопасности сети.

3. *Как влияет на работу сети компании проводимая в ней политика безопасности?*

   Ответ: Политика обеспечения безопасности определяет действия сотрудников компании и реализует соответствующие меры во всей сети.

4. *Приведите пример последовательного решения проблемы безопасности?*

   Ответ: Под эшелонированной защитой сети понимается расширение технологий обеспечения безопасности на всю сеть для защиты от угроз безопасности, которые могут возникнуть в любых точках сети. Одним из возможных решений является использование брандмауэра и установка программного обеспечения IDS для отдельных станцийна web-серверах. Брандмауэр защищает Web-сервер от нежелательных потоков данных, а программное обеспечение защищает сервер от поступления на него разрешенных данных.

5. *Каковы основные типы атак на сеть?*

   Ответ: Несанкционированный доступ, ненадежная аутентификация, пароли, анализаторы пакетов, атаки на уровне приложений, вирусы, черви, "троянскике кони", кража IP-адресов и отказ в обслуживании (DoS).

6. *Какой тип атак на сеть приводит к лавинообразному заполнению сети нежелательными пакетами?*

Ответ: Атаки DoS нацелены на нарушение работы сети путем истощения доступной полосы пропускания.

7. *Какой тип атак включает в себя рассылку приложений к сообщениям электронной почты? Каким образом отражается такая атака*

   Ответ: Вирус или " "троянский конь" могут быть внедрены в приложение к сообщению электронной почты. Для ослабления такой угрозы рекомендуется использовать антивирусное программное обеспечение.

8. *Каким образом отражаются атаки, связанные с подделкой IP-адресов?*

   Ослабление угрозы кражи IP-адресов достигается путем фильтрации адресов RFC 1918 и реализации входных и выходных фильтров, как это рекомендуется в RFC 2827.

9. *Каким образом коммутируемая инфраструктура позволяет отражать атаки, связанные с использованием анализаторов пакетов?*

   Ответ: Анализаторы пакетов перхватывают потоки данных в одном и том же широковещательном домене. В использующих коммутацию сетях каждый порт создаст отдельный широковещательный домен.

10. *Какое средство обеспечения безопасности обнаруживает доступные в сети устройства и службы?*

    Ответ: Сканер порта, такой, например, как Nmap, используется для обнаружения устройств и сетевых служб путем использования пакетов протокола ICMP и пакетов SYN протокола TCP. Nmap также использует усовершенствованные методы для обнаружения как устройств, так и сетевых служб.

11. *Какое средство обеспечения безопасности обнаруживает уязвимые места сетевых устройств?*

    Ответ: Сканер сетевой безопасности или средство аудита сетевой безопасности, такое как Nessus, идентифицирует точки уязвимости в сети.

12. *Какое средство обеспечения безопасности обнаруживает ненадежные пароли?*

    Ответ: Взломщик паролей, такой как John the Ripper, может обнаруживать слабо защищенные пароли.

Глава 53

1. *Что такое DEN?*

   Ответ: Модель сетевых каталогов (Directory-Enabled Networks — DEN) представляет собой спецификацию, описывающую различные объекты в управляемой системе с использованием объектно-ориентированной информационной модели, не зависящей от хранилища и протокола доступа. DEN также определяет способ преобразования данных информационной модели в форму, пригодную для хранения и извлечения из каталога с протоколом доступа (L)DAP.

2. *Требует ли DEN использования каталога?*

   Ответ: Нет. DEN представляет собой в первую очередь объектно-ориентированную информационную модель.

3. *Является ли DEN обычным средством моделирования сетевых устройств и служб?*

Ответ: Нет. Хотя основное внимание в DEN и уделяется созданию надежной и расширяемой инфраструктуры, которая может моделировать различные сетевые элементы и службы, одним из ее главных достоинств является то, что все типы объектов управляемой среды рассматриваются в ней как равноправные объекты.

4. *Что такое объектно-ориентированная информационная модель?*

   Ответ: Объектно-ориентированная информационная модель представляет собой объектно-ориентированный способ создания классов и описания их взаимоотношений, моделирующих различные объекты управляемой среды.

5. *Перечислите некоторые основные преимущества DEN.*

   Ответ: Во-первых — и это самое главное — DEN является объектно-ориентированной информационной моделью, которая единообразно описывает различные компоненты управляемой среды. Это позволяет устанавливать близкие отношения между классами, описывающими элементы сети, а также службами и классами, описывающими другие объекты. Это основной механизм, определяющий, какой вид услуг нужен данному клиенту.

   Во-вторых, поскольку стандарт DEN является объектно-ориентированной моделью, он по своей природе расширяем. Следовательно, концепции, еще не определенные в DEN, могут быть легко смоделированы и добавлены к этому стандарту.

6. В-третьих, DEN дает возможность разработчикам приложений и сетей рассматривать сеть как провайдера интеллектуальных услуг. Это позволяет разработчикам приложений описывать функции и процедуры обработки трафика приложений в терминах, непосредственно реализуемых сетью. Таким образом, если некоторое приложение имеет определенные требования к задержкам и дребезгу, DEN можно использовать для определения набора служб, которые удовлетворят эти требования.

   Четвертое преимущество близко связано с предыдущим и заключается в том, что DEN позволяет предприятиям предоставлять сетевые ресурсы приложениям в зависимости от их приоритета. Это дает возможность администратору составить политику, согласно которой, например, приложения SAP и PeopleSoft должны обслуживаться раньше, чем FTP-трафик. Указанное позволяет спроектировать сеть так, чтобы работа приложений согласовывалась с производственными правилами предприятия.

   Наконец, отметим еще одно преимущество DEN (впрочем, далеко не последнее) — DEN является стандартом, который может быть использован производителями сетевого оборудования, системными интеграторами и другими для описания общей структуры, определения, совместного и повторного использования информации.

7. *Как DEN моделирует отношения между объектами?*

   Ответ: Одним из самых значительных преимуществ DEN является то, что DEN представляет собой не просто набор моделей данных, описывающих характеристики управляемых объектов. DEN также определяет множество взаимоотношений между этими объектами. Без такого множества отношений нельзя выделить набор служб для предоставления разным пользователям разных приложений. Кроме того, в DEN эти отношения описаны в виде классов и, таким образом, пользуются всеми преимуществами объектно-ориентированного подхода

(такими, как наследование, описание свойств и методов непосредственно в описаниях отношений и т.д.). Следует обратить внимание на то, что DEN является уникальным в этом отношении методом моделирования.

Глава 54

1. *Какая концепция лежит в основе сетевого кэширования?*

   Ответ: Предположение, что пользователи многократно обращаются к одному и тому же содержимому.

2. *Назовите два дополнительных преимущества от внедрения технологии кэширования.*

   Ответ: Вот эти преимущества:

   — Безопасность доступа и управления.

   — Оперативная регистрация — администраторы могут регистрировать количество посещений той или иной страницы.

3. *Назовите два дополнительных преимущества от внедрения технологии кэширования.*

   Ответ: Технология интегрированного сетевого кэширования использует программное обеспечение системного уровня и аппаратные средства. Система интегрированного сетевого кэширования управляется как сетевое оборудование, разрабатывается как сложное аппаратное обеспечение и прозрачно встраивается в сеть.

4. *Дайте краткое описание технологии интегрированного сетевого кэширования.*

   Ответ: С помощью стандартов HTTP-кэширования, определяющих, какие элементы страницы подлежат кэшированию, а какие нет. Элементы, не подлежащие кэшированию, поступают с сервера-источника при каждом обращении.

5. *Как с помощью кэш-процессоров Cisco гарантировать обновление Web-страниц?*

   Ответ: В кэше сохраняются анимированные баннеры, изображения в форматах GIF и JPEG, панели инструментов, навигационные панели. Не подлежат кэшированию отклики CGI.

Глава 55

1. *Что представляет собой сеть хранения (SAN)?*

   Ответ: Сеть SAN представляет собой коммуникационную сеть, которая используется для соединения таких устройств, как конечные станции приложений с устройствами хранения, такими как дисковые и ленточные накопители.

2. *Какие два основных транспортных протокола используются в SAN-сетях?*

   Ответ: Первым и преобладающим является протокол оптоволоконного канала (Fibre Channel). Вторым транспортным протоколом является протокол iSCSI, который наследует функции TCP/IP и Ethernet.

3. *Данные какого коммуникационного протокола обычно передаются по сетям SAN?*

   Ответ: Данные протокола SCSI.

4. *Каковы две основных роли устройств протокола SCSI?*

Ответ: Роль инициирующего устройства и целевого устройства. Инициатором называется узел, ответственный за генерирование команд протокола SCSI, а целевым называется узел, отвечающий на эти команды.

5. *Какие три протокола верхнего уровня кроме SCSI были адаптированы для передачи их данных по протоколу Fibre Channel?*

   Ответ: Протоколы IP, IPI-3 (используемый для преобразования HIPPI в Fibre Channel), а также протокол SBCCS (Single-Byte Command Code Set), используемый для поддержки FICON в сетях SAN.

6. *Какой управляющий орган руководит разработкой проектов и стандартов протокола Fibre Channel?*

   Ответ: Рабочая группа ANSI T11.

7. *Когда был принят первый стандарт протокола Fibre Channel и как он назывался?*

   Ответ: Первым был принят в 1994 году стандарт FC-PH (ANSI X3.230:1994).

8. *Какой уровень протокола Fibre Channel отвечает за установку связи между двумя портами в сети SAN?*

   Ответ: Уровень FC-2.

9. *Каковы три основные топологии сети Fibre Channel?*

   Ответ: Nопология "точка-точка", конкурентная петля и топология коммутируемых структур

10. *Сколько устройств может поддерживать топология конкурентной петли?*

    Ответ: 126 устройств

11. *В чем состоит разница между топологиями частной конкурентной петли и публичной конкурентной петли?*

    Ответ: Частная конкурентная петля поддерживает только 8-битовую схему адресации, а подсоединенные устройства не могут осуществлять связь вне локальной петли. Общедоступная конкурентная петтля поддерживает полную 24-битовую иерархическую адресацию, которая позволяет осуществлять связь вне локальной петли.

12. *Что понимается под обозначением "B_Port"?*

    Ответ: Мостовой порт или B_Port, расширяет ISL протокола Fibre Channel за пределы сети FibreChannel. Порты B_Port подсоединяются только к портам типа E_Port и участвую только в работе базового набора канальных служб

13. *Как называется основной протокол маршрутизации протокола Fibre Channel и какую часть FC_ID он использует для принятия решений о маршрутизации?*

    Ответ: Первичным протоколом маршрутизации для Fibre Channel является протокол кратчайшего пути в структуре (Fabric Shortest Path First — FSPF). Он использует идентификатор домена (Domain_ID, 8 битов) для построения таблиц маршрутизации и принятия решений о маршрутах в структуре.

14. *Что представляет собой IDLE протокола Fibre Channel и для чего он используется?*

    Ответ: IDLE протокола Fibre Channel представляют собой 4-байтовые команды или упорядоченные наборы, передаваемые от одного устройства другому. Они используются для синхронизации и выравнивания слов между передатчиком и

приемником. IDLE указывают на готовность к передаче и передаются непрерывно, если отсутствуют другие данные для передачи

15. *Какой класс обслуживания протокола Fibre Channel не обеспечивает подтверждения доставки?*

    Ответ: 3-й класс, который является единственным широко используемым классом передачи данных, не обеспечивает подтверждения получения.

16. *Каково основное правило определения количества буферных кредитов, требуемых для поддержки скорости передачи 1 Гбит/с по каналу протокола Fibre Channel?*

    Ответ: Базовым правилом является то, что на каждые 2 км растояния между передатчиком и приемником требуется один кредит BB_Credit.

17. *Что называется мягким зонированием?*

    Ответ: Мягкое зонирование включает в себя фильтрацию запросов службы каталогов для того, чтобы были видимы только определенные устройства, что является средством изоляции передачи данных между конечными узлами протокола Fibre Channel. Мягкое зонирование не обеспечивает полной безопасности, поскольку одному конечному устройству для обхода зоны и связи с другим конечным устройством необходим идентификатор FC_ID.

18. *Верно ли утверждение: "индивидуальный iSCSI-обмен может происходить по нескольким TCP-соединениям"?*

    Ответ: Не верно. Хотя инициатор iSCSI может осуществлять несколько обменов по нескольким соединениям протокола TCP, однако каждый конретный обмен может использовать только одно TCP-соединение.

19. *Какой стандартный номер порта используется для протокола iSCSI?*

    Ответ: Номер порта TCP/3260.

20. *Какие два механизма используются для аутентификации инициатора протокола iSCSI?*

    Ответ: Первичным методом является использование протокола CHAP, который требуется стандартом iSCSI и является общим механизмом, используемым в соединениях удаленного доступа протокола IP. Вторым базовым методом является использование протокола SRP.

Глава 56

1. *Каковы пять этапов устранения сетевых отказов?*

   Ответ: Устранение отказа происходит в пять этапов: выявление отказа, диагностика отказа, блокировка отказа и восстановление работы, устранение отказа, поиск причин и контроль за возникновением новых отказов.

2. *Как работает средство управления программы NetView?*

   Ответ: Средство управления осуществляет управление сетью при помощи основных операторов и команд файлового доступа к приложениям VTAM (Virtual Telecommunications Access Method), контроллерам, операционным системам и устройствам NetView/PC (играющим роль интерфейса между устройствами NetView и устройствами, не поддерживающими SNA).

3. *Что требуется для активизации и деактивизации ресурсов, отмены команд и синхронизации удаленных систем?*

   Ответ: Управление операциями IBM заключается в управлении распределенными сетевыми ресурсами из центрального узла с использованием двух наборов функций: служб управления и служб общих операций. Службы управления позволяют централизованно управлять удаленными ресурсами, используя следующие функции: активация и деактивация ресурсов, отмена команд и синхронизация.

Глава 57

1. *Какова функция группы Matrix RMON?*

   Ответ: Эта группа хранит статистические данные о диалогах между наборами двух адресов. Как только устройство обнаруживает новый диалог, оно создает новую запись в таблице.

2. *Что такое RMON?*

   Ответ: Удаленный мониторинг (Remote Monitoring, RMON) является спецификацией стандартных средств контроля, позволяющей различным сетевым контрольным устройствам и консольным системам обмениваться данными мониторинга сети.

3. *Компонентами какой группы RMON являются многоадресатные пакеты, ошибки CRC, карликовые и гигантские пакеты, фрагменты и "мусор"?*

   Ответ: Группы статистики.

Глава 58

1. *Что такое агент SNMP?*

   Ответ: Под агентом протокола SNMP понимается модуль программного обеспечения, установленный в управляемом устройстве. Агенту доступна локальная управляющая информация, которую он преобразует в форму, соответствующую форматам протокола SNMP.

2. *Что такое база MIB и как получить к ней доступ?*

   Ответ: *База управляющей информации* (Management Information Base — MIB) представляет собой совокупность иерархически организованной информации. Доступ к базам MIB осуществляется посредством протокола управления сетью, например SNMP. Базы MIB состоят из управляемых объектов, обращение к которым происходит посредством идентификаторов.

3. *Назовите несколько протокольных операций, доступных в протоколе SNMPv2.*

   Ответ: В версии SNMPv2 доступны операции Get, GetNext, Set и Trap. Они также доступны в версии SNMPv1. В версии SNMPv2 также введены две новых протокольных операции: GetBulk и Inform.

4. *Каков основной недостаток версий SNMPv3 и SNMPv2, устраненный в SNMPv3?*

   Ответ: Недостаточный уровень безопасности. Первоначальные версии протокола SNMP не обеспечивали шифрование и аутентификацию сообщения протокола SNMP.

Глава 59

1. *В чем заключается основное назначение QoS?*

   Ответ: QoS обеспечивает приоритетную обработку идентифицированных потоков. При этом необходимо обеспечить достаточное обслуживание других потоков для их успешной передачи. Предоставлять приоритетность одним потокам за счет прерывания работы других приложений нежелательно.

2. *Какие существуют типы средств QoS?*

   Ответ: Существуют такие типы средств QoS:

   - Классификация. Идентификация и (если необходимо) маркирование потоков.
   - Управление перегрузкой. Организация очередей и дифференцированное обслуживание потоков с целью приоритетной обработки определенных потоков.
   - Избежание перегрузок. Предотвращение заполнения очередей, чтобы в них попадал трафик с высоким приоритетом, а также принятие мер для общего снижения вероятности перегрузок в Internet и интранет.
   - Формирование трафика и настройка политик. Ограничение полосы пропускания, используемой потоком.
   - Повышение эффективности канала. Методы уменьшения задержек на низкоскоростных каналах.

3. *Что такое управляющая сигнализация?*

   Ответ Это уведомление сети о приоритете потоков. Чаще всего это делается при помощи битов IP-приоритета в байте ToS, битов класса обслуживания для Ethernet и протокола RSVP для сквозного резервирования.

4. *Что такое IP-приоритетность?*

   Ответ: IP-приоритетность определяется тремя старшими битами байта ToS в IP-заголовке. Они используются для маркирования пакета, который служит для уведомления сетевых устройств о важности пакета. Три бита позволяют присвоить приоритет от 0 до 7 (значения 6 и 7 зарезервированы и не могут назначаться сетевым администратором).

5. *What is Differentiated Services Code Point (DSCP)*

   Ответ:Точка DSCP является модификацией байта типа службы, в котором шесть старших битов переназначены как поле DSCP. Каждое такое поле задает действия на отдельном переходе, которые выполняются над пакетом.

6. *What is Modular QoS CLI (MQC)?*

   Ответ: Интерфейс MQS представляет собой модульную основу конфигурации для выполнения функций качества обслуживания QoS, которая разделяет такие функции, как классификация, определение политики и применение политики на маршрутизаторе Cisco. В конечном итоге все функции QoS Cisco должны конфигурироваться в рамках MQS.

7. *Чем отличается потоковая WFQ от классовой WFQ (CBWFQ)?*

   Ответ: Существуют такие отличия:

- WFQ предоставляет очередь для каждого потока. CBWFQ создает классы, состоящие из одного или нескольких потоков.
- WFQ обеспечивает равноправие всех потоков (с равным IP-приоритетом). Классам потоков CBWFQ предоставляется гарантированная минимальная полоса пропускания, размер которой определяется пользователем.
- CBWFQ поддерживает WRED.

8. *Какое средство используется для управления очередями во избежание перегрузок? Каким образом избегаются перегрузки?*

   Ответ: Для предупреждения перегрузок используется алгоритм взвешенного раннего случайного распознавания (Weighted Early Random Detect — WRED), который выполняет следующие действия.

   - Старается гарантировать наличие в очереди свободного места для пакетов с высоким приоритетом.
   - Обеспечивает систему отбрасывания пакетов с более низким приоритетом прежде, чем пакетов с более высоким приоритетом.

9. *Каковы два основных назначения CAR?*

   Ответ: Двумя основными целями использования *CAR* являются:

   - Классификация пакетов по IP-приоритету или группам QoS (для D-WFQ).
   - Ограничение объема передачи данных(или организация системы политик) для передачи потока.

10. *Какое средство QoS следует использовать для обеспечения минимально необходимой полосы пропускания?*

    Ответ: CBWFQ.

11. *Каким средством QoS необходимо пользоваться для ограничения максимальной полосы пропускания потока?*

12. Ответ: CAR или GTS/FRTS.

13. *Что делает NBAR и в чем заключаются его две уникальные особенности?*

    NBAR расширяет возможности идентификации пакета. Путем более глубокого анализа пакета NBAR распознает такие потоки, как URL (вместо обычного порта 80 HTTP).

    Ответ: Особенности NBAR заключаются в следующем.

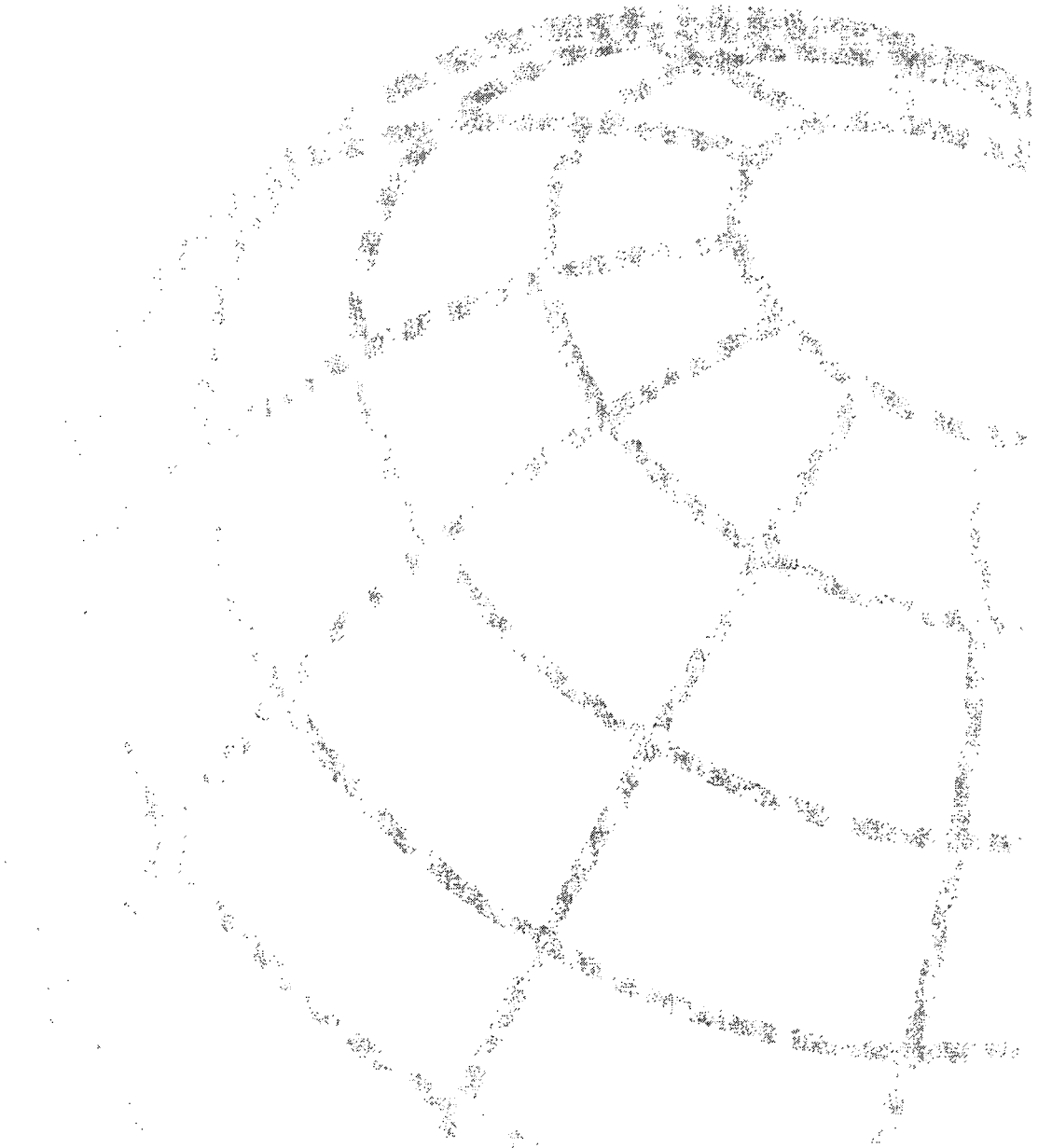
    - Анализ протокола, благодаря чему маршрутизатор идентифицирует протоколы и собирает статистические данные о каждом из них.
    - PDLM, обеспечивающий легкое обновление протоколов, распознаваемых NBAR.

14. *В каких случаях, как правило, применяется формирование трафика?*

    Ответ: Одной из областей использования является топология "звезда", когда один высокоскоростной канал в центральном узле связан с несколькими более медленными удаленными каналами. В такой топологии трафик часто формируется на центральном узле во избежание перегрузки более медленных удаленных каналов и отбрасывания пакетов.

15. *Какое средство используется для интегрированного QoS?*

    Ответ: RSVP



Приложение Б

Традиционные технологии

В настоящем приложении обсуждаются три традиционные технологии: Token Ring/IEEE 802.5, Xerox Network Systems и Banyan VINES.

Сети Token Ring/IEEE 802.5

Сеть Token Ring была первоначально разработана корпорацией IBM в начале 70-х годов XX века. Она по-прежнему остается первичной технологией локальных сетей (local-area network — LAN) этой корпорации. Связанная с ней спецификация IEEE 802.5 почти идентична Token Ring и полностью совместима с ней. Фактически спецификация IEEE 802.5 была смоделирована по образцу спецификации Token Ring корпорации IBM и продолжает отражать ее развитие. Термин *Token Ring* в общем смысле используется для обозначения как сетей Token Ring IBM, так и сетей IEEE 802.5. Приводимый в настоящей главе материал относится к обоим этим типам сетей.

По основным своим характеристикам, сети Token Ring и IEEE 802.5 совместимы, хотя их спецификации в некоторых несущественных аспектах различаются. Сеть Token Ring IBM имеет звездообразную топологию, в которой все конечные станции подсоединяются к устройству, называемому модулем множественного доступа (multistations access unit — MSAU). В отличие от сетей Token Ring, в сетях IEEE 802.5 топология заранее не определена, хотя фактически все реализации IEEE 802.5 основываются на звездообразной топологии. Существуют и другие различия, включая тип передающей среды (спецификация IEEE 802.5 не определяет тип среды, в то время как Token Ring IBM использует витую пару) и размер информационного поля маршрутизации. На рис. Б.1 приведены основные параметры спецификаций сетей Token Ring и IEEE 802.5.

	IBM Token Ring	IEEE 802.5
Скорость передачи данных	4,16 Мбит/с	4,16 Мбит/с
Количество станций в сегменте	260 (экранированная витая пара) 72 (неэкранированная витая пара)	250
Топология	Звездообразная	Не определено
Среда передачи	Витая пара	Не определено
Вид сигналов	Немодулированная передача	Немодулированная передача
Метод доступа	Маркерный	Маркерный
Кодирование	Дифференциальный манчестерский код	Дифференциальный манчестерский код

Рис. Б.1. Хотя сети Token Ring и IEEE 802.5 в некоторых аспектах различаются, в целом они совместимы

Физические соединения

Сетевые станции IBM Token Ring подключаются непосредственно к модулям MSAU, которые могут быть соединены друг с другом, образуя одно большое кольцо (рис. Б.2). Модули MSAU подключаются к соседним модулям соединительными кабелями (patch cables), а к станциям — кабелями ответвления (lobe cables). В состав MSAU входят обводные реле для удаления станций из кольца.

Функционирование сети Token Ring

Сети Token Ring и IEEE 802.5 представляют собой два основных примера сетей с передачей маркера (другим примером являются сети FDDI). В *сетях с передачей маркера (token-passing networks)* по сети перемещается небольшой фрейм, называемый маркером. Обладание маркером дает право на передачу. Если узел, получающий маркер, не имеет информации для передачи, то он передает маркер следующей конечной станции. Каждая станция может удерживать маркер лишь в течение установленного максимального времени.

Если же станция, обладающая маркером, имеет информацию для передачи, то она захватывает маркер, изменяет его первый бит (что превращает его в последовательность символов, обозначающих начало фрейма), добавляет информацию, которую требуется передать, и отправляет эту последовательность по кольцу в направлении следующей станции. Во время перемещения такого фрейма по кольцу маркер в сети отсутствует, поэтому остальным станциям, у которых есть информация для передачи, приходится ожидать (кроме случая, когда кольцо поддерживает раннее создание маркера). Поэтому в сети Token Ring коллизии невозможны. Если в кольце поддерживается функция раннего создания маркера, то новый маркер может быть создан, когда передача фрейма завершена.

Информационный фрейм циркулирует по кольцу до тех пор, пока он не достигнет станции-получателя, которая копирует данную информацию для дальнейшей обработки.

Этот информационный фрейм продолжает двигаться по кольцу и в конечном итоге удаляется, когда поступает на отправившую его станцию. Эта станция может исследовать возвратившийся фрейм для проверки того, что он был просмотрен и скопирован станцией пункта назначения.

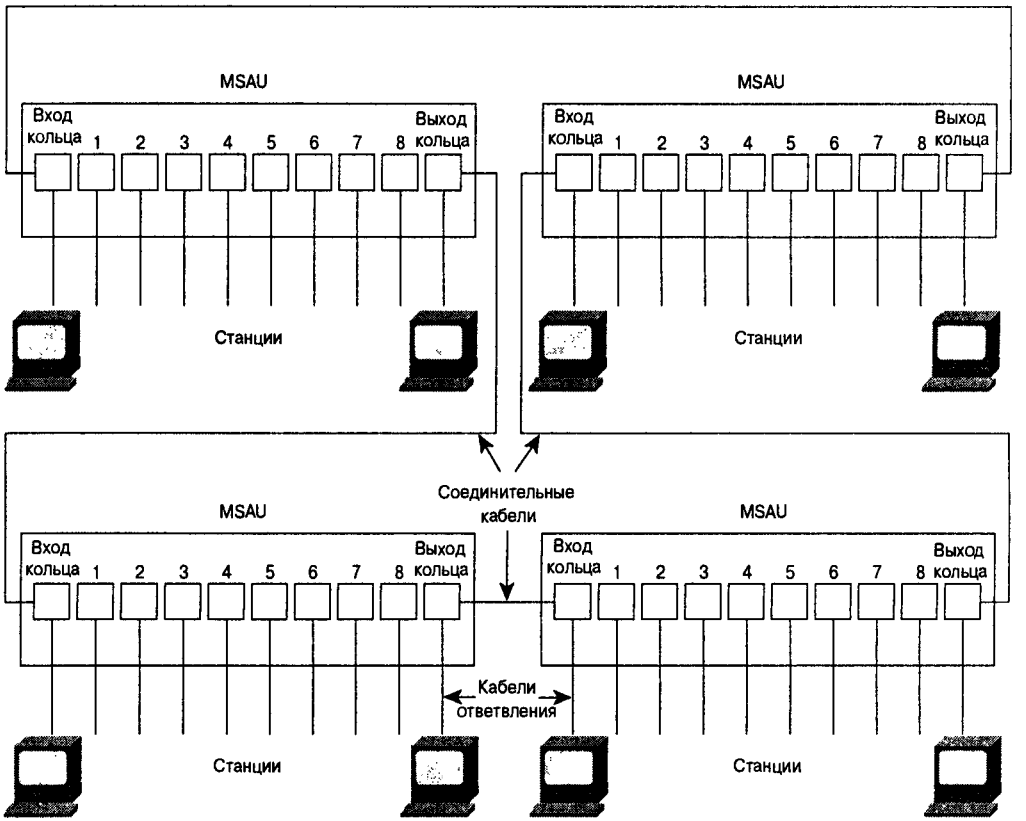


Рис. Б.2. В сети Token Ring IBM модули MSAU могут быть соединены между собой с образованием одного большого кольца

В отличие от сетей CSMA/CD, таких как Ethernet, сети с передачей маркера являются *детерминистическими*. Это означает, что можно вычислить максимальное время, которое пройдет до того, как любая станция получит возможность передавать данные. Эта функция, а также некоторые другие функции обеспечения надежности, обсуждаемые в разделе "Механизмы ликвидации сбоев в сети" далее в настоящей главе, делают сети Token Ring идеальными для приложений, в которых задержка должна быть предсказуема и важно устойчивое функционирование сети. Примером подобных приложений может быть автоматизированная производственная линия.

Система приоритетов

В сетях Token Ring применяется сложная система приоритетов, позволяющая станциям, которым пользователь присвоит более высокий приоритет, использовать

сеть чаще других. Фреймы сети Token Ring имеют два поля, которые управляют приоритетами: поле приоритета и поле резервирования.

Только станции с приоритетом, равным или более высоким, чем значение приоритета, содержащееся в маркере, могут захватить маркер. После того как маркер перехвачен и превращен в информационный фрейм, только станции со значением приоритета выше, чем приоритет передающей станции, могут зарезервировать маркер для следующего прохождения по сети. При генерации следующего маркера ему присваивается максимальный приоритет среди резервирующих станций. Станции, которые поднимают приоритет маркера, должны по окончании передачи вернуть его предыдущее значение.

Механизмы ликвидации сбоев в сети

Сети Token Ring используют несколько механизмов для обнаружения и компенсации сбоев в сети. В частности, одна станция в сети Token Ring выбирается в качестве *активного монитора (active monitor)*. Эта станция, которой в принципе может быть любая станция сети, служит централизованным источником информации о синхронизации для других станций и выполняет ряд функций по поддержанию работы кольца. Одной из этих функций является удаление из кольца непрерывно циркулирующих фреймов. Если в передающем устройстве происходит сбой, то его фрейм может продолжать двигаться по кольцу, не давая другим станциям возможности передать свои фреймы, чем полностью блокирует работу сети. Активный монитор обнаруживает подобные фреймы, удаляет их из кольца и генерирует новый маркер.

Звездообразная топология сети IBM Token Ring также вносит свой вклад в общую надежность сети. Поскольку вся информация в сети Token Ring просматривается активными модулями MSAU, эти устройства могут быть запрограммированы на обнаружение проблем и, при необходимости, выборочное удаление станций из кольца.

Алгоритм Token Ring, называемый *испусканием маяка (beaconing)*, обнаруживает и пытается устранить некоторые сетевые сбои. Каждый раз, когда какая-либо станция обнаруживает в сети серьезную проблему (например, обрыв кабеля), она посылает фрейм-маяк, который определяет домен, в котором произошел сбой. Этот домен включает в себя станцию, сообщающую о сбое, ее ближайшее активное соседнее устройство в восходящем направлении (Nearest Active Up-Stream Neighbor — NAUN) и все станции, находящиеся между ними. Испускание маяка инициирует процесс, называемый *автоматическим реконфигурированием*, в котором узлы, находящиеся в домене сбоя, автоматически выполняют диагностику, пытаясь реконфигурировать сеть вокруг областей со сбоями. Физически модуль MSAU может выполнить это путем электрической реконфигурации.

Формат фрейма

В сетях Token Ring и IEEE 802.5 поддерживаются два основных типа фреймов: маркеры и фреймы данных/управления. Маркер состоит из признака начала, байта управления доступом и признака конца. Размер фреймов данных и фреймов управления не является постоянным и изменяется в зависимости от размера информационного поля. Фреймы данных переносят информацию протоколов верхних уровней, а фреймы управления содержат только управляющую информацию и не включают в себя данных верхних уровней. Оба эти формата фреймов показаны на рис. Б.3.

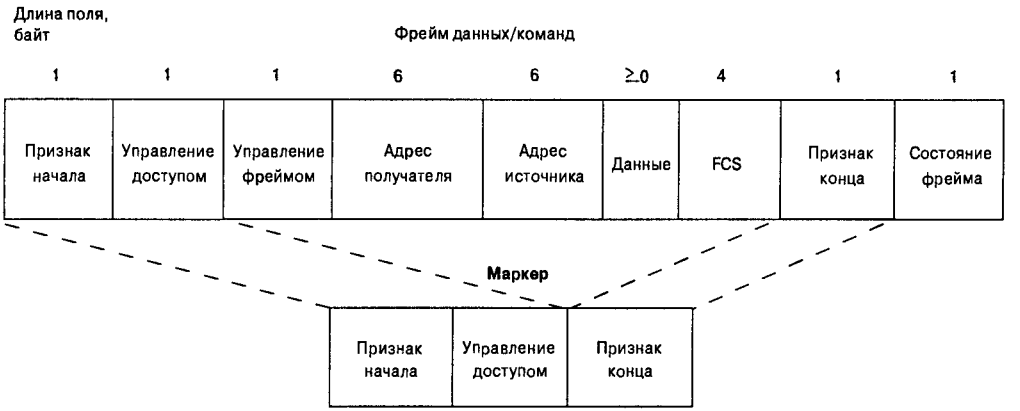


Рис. Б.3. В спецификациях IEEE 802.5 и Token Ring определены форматы фреймов маркеров и фреймов данных/управления

Поля фрейма Token Ring

Ниже описаны три поля фрейма маркера, показанные на рис. Б.3.

- **Признак начала.** Сообщает каждой станции о поступлении маркера (или фрейма данных/управления). Это поле включает в себя сигналы, которые отличают его от оставшейся части фрейма тем, что они используют иную схему кодировки, чем в других полях.
- **Байт управления доступом.** Этот байт содержит поле приоритета (priority field) — 3 старших бита, поле резервирования (reservation field) — младшие 3 бита, а также бит маркера (используется для того, чтобы отличить его от фрейма данных/управления) и бит монитора (используется активным монитором для того, чтобы выяснить, не движется ли этот фрейм по кольцу бесконечно).
- **Признак конца.** Указывает на конец фрейма маркера или фрейма данных/управления. В этом поле также содержится бит, который может указывать на то, что фрейм поврежден, и бит, свидетельствующий о том, что фрейм является последним в логической последовательности.

Поля фрейма данных/управления

Фреймы данных/управления имеют те же три поля, которые предусмотрены у маркера Token Ring, а также несколько дополнительных полей. Ниже описаны поля фрейма данных/управления, показанные на рис. Б.3.

- **Признак начала.** Сообщает каждой станции о поступлении маркера (или фрейма данных/управления). Это поле включает в себя сигналы, которые отличают его от оставшейся части фрейма тем, что используют иную схему кодировки, чем в других полях.
- **Байт управления доступом.** Этот байт содержит поле приоритета (priority field) — 3 старших бита, поле резервирования (reservation field) — младшие 3 бита, а также бит маркера (используется для того, чтобы отличить его от фрейма

данных/управления) и бит монитора (используется активным монитором для того, чтобы выяснить, не движется ли этот фрейм по кольцу бесконечно).

- **Байт управления фрейма.** Это поле указывает, какую информацию содержит фрейм — данные или управляющую информацию. Во фреймах управления этот байт также указывает тип управляющей информации.
- **Поле адресов пункта назначения и отправителя.** Это поле содержит два 6-байтовых подполя, задающих адреса отправителя и получателя.
- **Поле данных.** В этом поле указано, что длина поля ограничена временем удержания маркера, установленным в кольце, которое определяет максимальное время, в течение которого станция может удерживать маркер.
- **Контрольная последовательность фрейма. (Frame-Check Sequence — FCS).** В это поле станция-источник вставляет вычисленное значение, зависящее от содержимого фрейма. Станция-получатель заново вычисляет это значение для проверки того, не был ли фрейм поврежден при передаче. Если фрейм был поврежден, то он отбрасывается.
- **Признак конца.** Указывает на конец фрейма маркера или фрейма данных/управления. В этом поле также содержится бит, который может указывать на то, что фрейм поврежден, и бит, свидетельствующий о том, что фрейм является последним в логической последовательности.
- **Поле состояния фрейма.** Однобайтовое поле, заканчивающее фрейм данных/управления. Поле статуса фрейма включает в себя индикатор распознавания адреса и индикатор копирования фрейма.

Резюме

Технология Token Ring была разработана корпорацией IBM в 70-х годах XX века. В сетях с передачей маркера по сети постоянно передается небольшой фрейм, называемый маркером. Обладание маркером дает право на передачу. Если узел, получающий маркер, не имеет информации для передачи, то он передает маркер следующей конечной станции. Каждая станция может удерживать маркер лишь в течение установленного максимального времени.

Если же станция, обладающая маркером, имеет информацию для передачи, то она захватывает маркер, изменяет его первый бит (что превращает маркер в признак начала фрейма), добавляет информацию, которую требуется передать, и отправляет эту последовательность по кольцу в направлении следующей станции.

Сетевые системы Xerox

Введение

Протоколы сетевых систем Xerox (Xerox Network Systems — XNS) были разработаны корпорацией Xerox в конце 70-х-начале 80-х годов XX века. Предполагалось их использование с разнообразными средами коммуникации, с различными процессора-

ми и офисными приложениями. Некоторые протоколы XNS аналогичны Internet-протоколу (Internet Protocol — IP) и протоколу управления передачей (Transport Control Protocol — TCP). Последние были разработаны управлением перспективных исследовательских программ (Defence Advanced Research Project Agency — DARPA) для министерства обороны США (Department of Defence — DoD).

Благодаря своей доступности и раннему появлению на рынке протокол XNS был принят в качестве рабочего протокола локальных сетей LAN во многих компаниях, включая Novell Inc., Ungermann-Bass Inc. (в настоящее время подразделение корпорации Tandem Computers) и корпорацию 3Com Corporation. С тех пор каждая из этих компаний вносила в протоколы XNS различные изменения. Корпорация Novell добавила к нему протокол анонсирования службы (Service Advertisement Protocol — SAP), позволяющий анонсировать ресурсы, и модифицированные протоколы OSI 3-го уровня, (которые Novell переименовала в IPX — Internetwork Packet Exchange) для работы преимущественно в сетях IEEE 802.3, а не в сетях Ethernet. Корпорация Ungermann-Bass модифицировала протокол RIP для учета задержки и подсчета количества переходов, а также внесла другие небольшие изменения. С течением времени XNS-реализации для сетей персональных компьютеров PC стали более популярными, чем первоначально разработанные корпорацией Xerox протоколы XNS. В настоящей главе приведен обзор стека протоколов XNS в контексте эталонной модели OSI.

Иерархия стека протоколов XNS

Хотя цели разработки протокола XNS были теми же, что и цели эталонной модели OSI, концепция иерархии протоколов XNS несколько отличается от используемой в модели OSI, как показано на рис. Б.4.

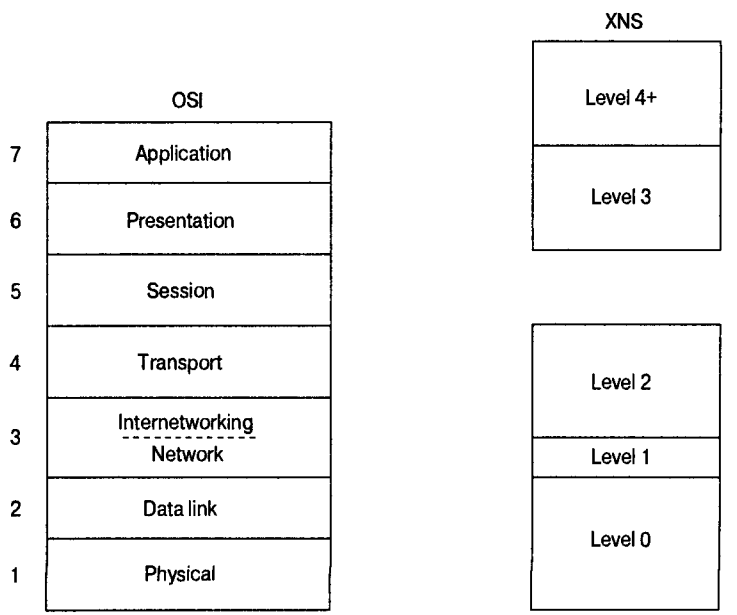


Рис. Б.4. Корпорация Xerox приняла 5-уровневую модель передачи пакетов

Как показано на рис. Б.4, корпорация Xerox приняла 5-уровневую модель передачи пакетов. Уровень 0 (нулевой уровень) приближенно соответствует 1-му и 2-му уровням эталонной модели OSI, управляя доступом к каналу и потоками битов. 1-й уровень примерно соответствует 3-му уровню модели OSI в части, касающейся сетевых потоков данных. 2-й уровень соответствует части 3-го уровня модели OSI, относящейся к межсетевой маршрутизации и 4-му уровню модели OSI, относящейся к передаче данных между процессами. 3-й и 4-й уровни примерно соответствуют двум верхним уровням модели OSI, обеспечивая структурирование данных, взаимодействие процессов и приложений. В стеке протоколов XNS отсутствует протокол, соответствующий 5-му уровню эталонной модели OSI (сеансовому уровню).

Доступ к среде передачи

Хотя в документации XNS упоминаются протоколы X.25, Ethernet и высокоуровневый протокол управления каналом (High-Level Data Link Control — HDLC), стек протоколов XNS не определяет явным образом, что подразумевается под протоколом нулевого уровня. Как и многие другие стеки протоколов, XNS оставляет вопрос о доступе к среде открытым, неявно позволяя использовать любой такой протокол для передачу пакетов XNS в физической среде.

Сетевой уровень

Протокол сетевого уровня стека XNS называется протоколом межсетевых дейтаграмм (Internet Datagram Protocol — IDP). Протокол IDP выполняет стандартные функции 3-го уровня, включая логическую адресацию и сквозную доставку дейтаграмм в объединенной сети. На рис. Б.5 показан формат пакета в протоколе IDP.

Ниже описываются поля IDP-пакета, показанные на рис. Б.5.

- **Контрольная сумма (Checksum)**. 16-битовое поле, которое позволяет проверить целостность пакета после его прохождения по сети.
- **Длина пакета (Lenght)**. 16-битовое поле, в котором содержится общая длина текущей дейтаграммы (включая поле контрольной суммы).
- **Управление передачей (Transport control)**. 8-битовое поле, содержащее подполя количества переходов и максимального времени существования (Maximum Packet Lifetime — MPL) пакетов. Значение подполя количества переходов (Hop Count) устанавливается равным нулю самим источником, и увеличивается на единицу при каждом прохождении пакета через маршрутизатор. Когда значение поля Hop Count достигает 16, дейтаграмма отбрасывается в предположении, что возникла петля маршрутизации. Подполе MPL устанавливает максимальное время (в секундах), в течение которого пакет может оставаться в объединенной сети.
- **Тип пакета (Packet type)**. 8-битовое поле, задающее формат поля данных.
- **Номер сети пункта назначения (Destination Network Number)**. 32-битовое поле, уникальным образом идентифицирующее сеть-получатель в объединенной сети.
- **Номер узла-получателя (Destination Host Number)**. 48-битовое поле, уникальным образом идентифицирующее узел-получатель.

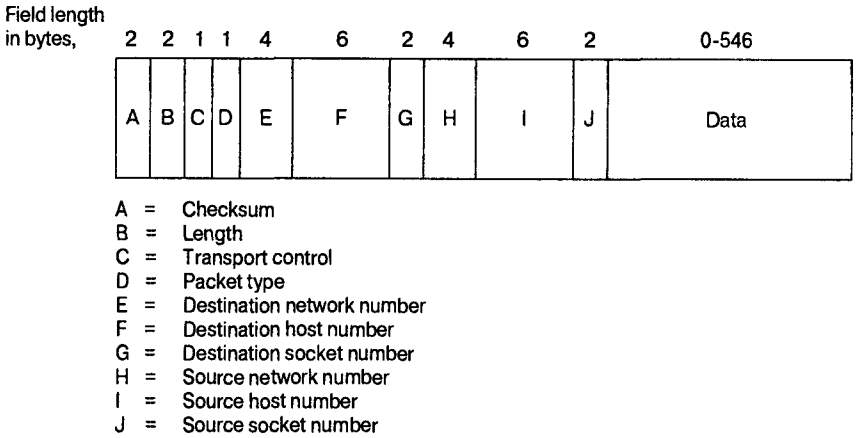


Рис. Б.5. IDP-пакет содержит 11 полей

- **Номер сокета (процесса) пункта назначения (Destination socket number)**. 16-битовое поле, уникальным образом идентифицирующее сокет (процесс) в узле-получателе.
- **Номер сети-источника (Source Network Number)**. 32-битовое поле, уникальным образом идентифицирующее сеть-источник в распределенной сети.
- **Номер узла-источника (Source Host Number)**. 48-битовое поле, уникальным образом идентифицирующее узел-источник.
- **Номер сокета (процесса) источника (Source Socket Number)**. 16-битовое поле, уникальным образом идентифицирующее сокет (процесс) в узле-источнике.

Адреса IEEE 802 эквивалентны номерам узлов, поэтому узлы, которые подсоединены более чем к одной сети IEEE 802.5, имеют во всех сегментах один и тот же адрес. Это делает сетевые номера избыточными, но тем не менее полезными для процесса маршрутизации. Некоторые номера сокетов являются общеизвестными; это означает, что выполняемые ими функции задаются статически использующим их программным обеспечением. Все остальные номера сокетов могут использоваться для выполнения различных функций.

Протокол XNS поддерживает Ethernet-инкапсуляцию версии 2.0 для сетей Ethernet и три типа инкапсуляции для сетей Token Ring: 3Com, протокол доступа SubNet (SubNet Access Protocol — SNAP) и Ungermann-Bass.

XNS поддерживает одноадресатную рассылку пакетов (соединения типа "точка-точка"), многоадресатную и широковещательную рассылки. Адреса многоадресатной и широковещательной рассылки далее подразделяются на направленные (directed) и глобальные. При направленной многоадресатной рассылке пакеты доставляются членам группы многоадресатной рассылки, указанной адресом многоадресатной рассылки указанной сети. При широковещательной направленной рассылке пакеты направляются всем членам указанной сети. При глобальной многоадресатной рассылке пакеты направляются всем членам группы во всей сети, в то время как глобальная широковещательная рассылка отправляет пакеты по всем адресам объединенной сети. Установка одного из битов в номере узла указывает на одноадресатную рассылку, в отличие от многоадресатной. Если все биты в поле узла равны единице, то адрес является широковещательным.

Для маршрутизации пакетов в объединенной сети протокол XNS использует схему динамической маршрутизации протокола RIP. В настоящее время протокол RIP является

наиболее часто используемым в Internet-сообществе протоколом внутреннего шлюза (Interior Gateway Protocol — IGP). Более подробная информация о протоколе RIP приведена в главе 47, "Протокол OSPF".

Транспортный уровень

Функции транспортного уровня эталонной модели OSI в стеке протоколов XNS выполняются несколькими протоколами. Все приведенные ниже протоколы описаны в спецификации XNS как протоколы 2-го уровня.

Протокол последовательных пакетов (Sequenced Packet Protocol — SPP) обеспечивает надежную, ориентированную на соединение передачу пакетов, при которой управление потоком осуществляется клиентом процесса. По выполняемым функциям он аналогичен протоколу управления передачей (Transmission Control Protocol — TCP), входящему в стек протоколов IP (Internet Protocol) и транспортному протоколу 4 (Transport Protocol 4 — TP4), входящему в стек протоколов OSI. Более подробная информация о протоколе TCP приведена в главе 35 "Протоколы Internet", а протокол TP4 описан в главе 34 "Протоколы взаимодействия открытых систем".

Каждый SPP-пакет включает в себя последовательный номер, который используется для упорядочения пакетов и проверки дублирования или потери пакета. SPP-пакеты также содержат два 16-битовых идентификатора соединения. Идентификатор соединения определяется для каждой стороны соединения; вместе эти два идентификатора соединения уникальным образом характеризуют логическое соединение между процессами клиента. Пакеты протокола SPP не могут иметь длину, превышающую 576 байт. Процессы клиента могут "обсуждать" длину пакета при установке соединения, однако протокол SPP не определяет конкретный характер такого обсуждения.

Протокол обмена пакетами (Packet Exchange Protocol — PEP) представляет собой протокол типа "запрос-ответ", предназначенный для обеспечения большей надежности, чем обычная дейтаграммная служба (например, служба, предоставляемая протоколом IDP), однако меньшей, чем у протокола SPP. Протокол PEP по выполняемым функциям аналогичен протоколу пользовательских дейтаграмм (User Datagram Protocol — UDP), входящему в стек протоколов IP (Internet Protocol). (Более подробная информация о протоколе UDP приведена в главе 35 "Протоколы Internet". Протокол PEP основан на передаче отдельных пакетов и обеспечивает повторную передачу (ретрансмиссию), однако не обнаруживает удвоения (дублирования) пакетов. В этом качестве он полезен в приложениях, где транзакции "запрос-ответ" могут быть повторены без повреждения данных или в тех случаях, когда надежность передачи обеспечивается на другом уровне.

Протокол обнаружения ошибок (Error Protocol — EP) может быть использован любым клиентским процессом для уведомления другого процесса о том, что в сети произошел сбой. Этот протокол используется, например, в ситуациях, когда реализация SPP обнаружила дублирование пакета.

Протоколы верхних уровней

Стек протоколов XNS предлагает несколько протоколов верхних уровней. Протокол печати (Printing Protocol) предоставляет службы печати, протокол работы с файлами (Filing Protocol) обеспечивает службы доступа к файлам, а протокол Clearinghouse обеспечивает службу назначения имен. Каждый из этих трех протоколов работает над протоколом

Courier Protocol, который обеспечивает соглашения по структурированию данных и взаимодействию процессов.

Стек протоколов XNS также определяет протоколы 4-го уровня, которые являются протоколами уровня приложений. Но поскольку они мало связаны с реальным процессом коммуникации, спецификация XNS не включает в себя каких-либо относящихся к этому определений.

Протокол 2-го уровня Echo Protocol используется для проверки достижимости узлов XNS-сети и для поддержки функций, предоставляемых командой `ping` в UNIX и других операционных средах.

Резюме

В настоящее время XNS используется в качестве протокола только в сетях производителей, которые приняли часть стандартов, предоставляемых XNS. Однако их число постоянно сокращается и лишь немногие новые сети базируются на протоколе XNS.

Сетевая служба Banyan Vines

Введение

Виртуальная интегрированная сетевая служба Banyan (Banyan Virtual Integrated Network Service — VINES) реализует операционную систему распределенной сети, основанную на семействе фирменных протоколов, полученных из протоколов сетевых систем Xerox (Xerox Network Systems — XNS) корпорации Xerox. Служба VINES использует архитектуру "клиент/сервер", в которой клиент запрашивает у сервера определенные службы, такие как доступ к файлам и печать. В настоящей главе приводится общий обзор коммуникационных протоколов VINES. Стек протоколов VINES показан на рис. Б.6.

Доступ к передающей среде

Нижние два уровня стека протоколов VINES реализуются с помощью нескольких широко известных механизмов доступа к среде, включающих в себя высокоуровневый протокол управления каналом (High-Level Data Link Control — HDLC), протоколы X.25, Ethernet и Token Ring.

Сетевой уровень

Для выполнения функций сетевого уровня (включая межсетевую маршрутизацию) служба VINES использует межсетевой протокол VINES (Vines Internet Protocol — VIP). VINES также поддерживает собственный протокол преобразования адресов (Address Resolution Protocol — ARP), собственную версию протокола маршрутной информации (Routing Information Protocol — RIP), называемую протоколом таблицы маршрутизации (Routing Table Protocol — RTP) и протокол межсетевого управления (Internet Control Protocol — ICP), который обеспечивает обработку исключений и предоставляет информацию об оценках специальной маршрутизации. Пакеты протоколов ARP, ICP и RTP инкапсулируются в VIP-заголовок.

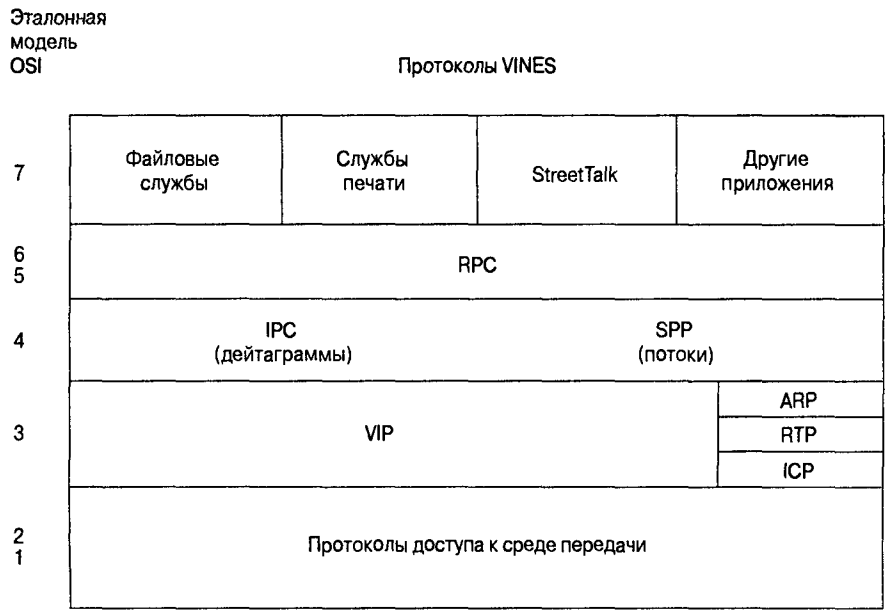


Рис. Б.6. Стек протоколов VINES состоит из пяти отдельных уровней

Межсетевой протокол VINES

Адреса службы VINES сетевого уровня представляют собой 48-битовые конструкции, подразделяемые на сетевую часть (32 битов) и часть, относящуюся к подсети (16 бит). Сетевой номер правильнее было бы назвать адресом (номером) сервера, поскольку он получается непосредственно из ключа сервера (server's key) (аппаратный модуль, который идентифицирует уникальный номер и опции программного обеспечения для данного сервера). Часть VINES-адреса, относящуюся к подсети, можно было бы назвать адресом узла, поскольку она используется для идентификации узла в сети VINES. На рис. Б.7 показан формат VINES-адреса.

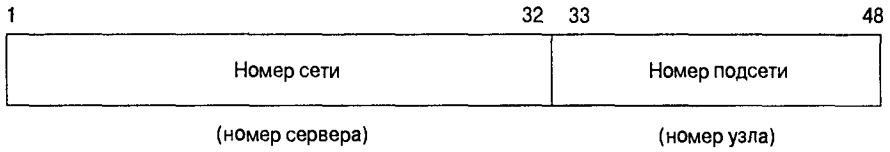


Рис. Б.7. VINES-адрес состоит из номера сети и номера подсети

Сетевой адрес идентифицирует логическую сеть VINES, которая представляется двухуровневым деревом с корнем в узле (node) службы. Узлы службы, которыми обычно являются серверы, обеспечивают преобразование адресов и службы маршрутизации клиентам, которые являются листьями дерева. Узел службы назначает клиентам адреса межсетевого протокола VINES (VINES Internet Protocol — VIP).

При включении питания на узле клиента, с него происходит рассылка широковещательного запроса всем серверам, и серверы, получившие этот запрос, отвечают соответствующим сообщением. Узел клиента выбирает первый ответ и запрашивает у

этого сервера адрес подсети (адрес узла). Сервер отвечает отправкой адреса, состоящего из его собственного сетевого адреса (полученного из ключа) и адреса подсети (узла), выбранного им по своему усмотрению. Адреса подсетей клиента обычно назначаются последовательно, начиная с адреса 8001H. Адреса подсети сервера всегда равны 1. На рис. Б.1 показан процесс выбора адресов.

Динамическое назначение адресов в протоколе VINES не является уникальным случаем (этот процесс используется также протоколом AppleTalk), однако, конечно, оно не так широко распространено, как статическое назначение адресов. Поскольку адреса выбираются исключительно (эксклюзивно) конкретным сервером (чей адрес является уникальным ввиду его аппаратного характера), вероятность дублирования адресов весьма мала. Это обстоятельство имеет большое положительное значение, поскольку дублирование адресов может привести к разрушительным последствиям для сетей протокола IP (Internet Protocol) и для сетей иных типов.

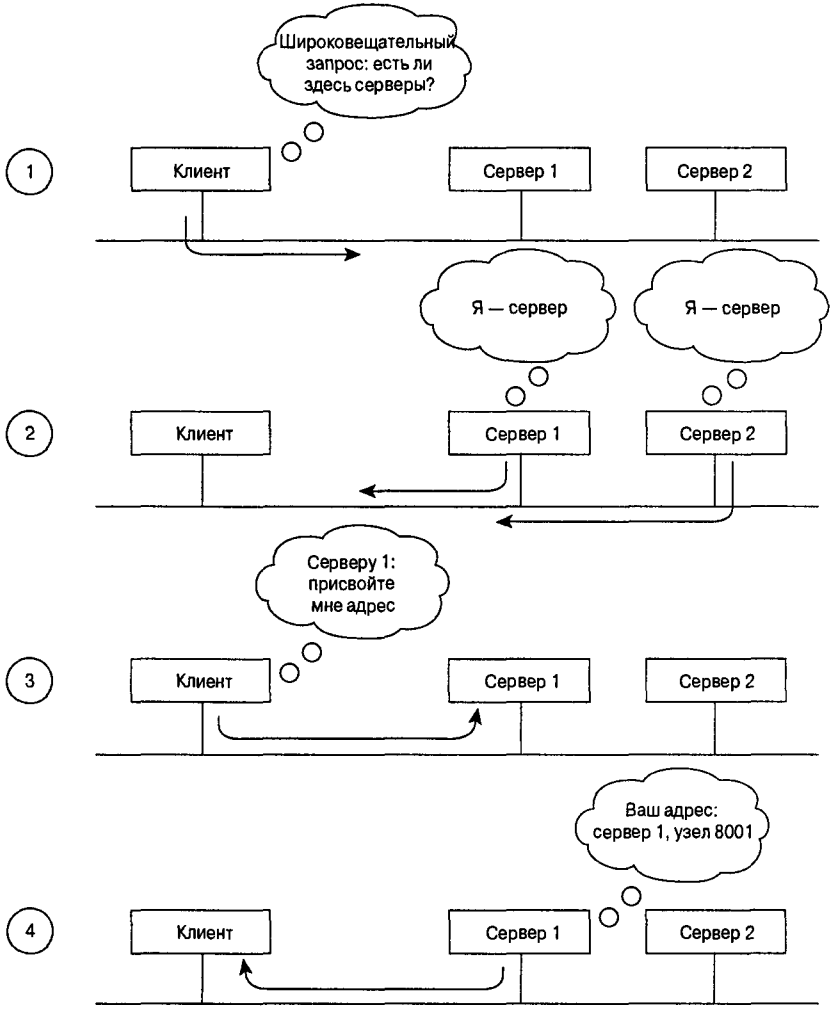


Рис. Б.8. Выбор VINES-адреса осуществляется в четыре этапа

В схеме сетей VINES все серверы с несколькими интерфейсами, как правило, являются маршрутизаторами. Клиенты всегда выбирают свой собственный сервер в качестве маршрутизатора первого перехода, даже если другой сервер на том же кабеле предоставляет лучший маршрут к окончательному пункту назначения. Клиенты могут узнать о других маршрутизаторах путем получения косвенных сообщений от своего сервера. Поскольку при первом переходе клиенты полагаются на свои серверы, VINES-серверы поддерживают таблицы маршрутизации для помощи узлам клиентов при поиске удаленных адресов.

Таблицы маршрутизации VINES состоят из пар "узел/оценка", в которых параметр "узел" соответствует сетевому узлу, к которому можно получить доступ, а оценка соответствует задержке (выраженной в миллисекундах), возникающей при достижении этого узла. Протокол RIP помогает службе VINES находить соседних клиентов, соседние серверы и маршрутизаторы.

Все клиенты периодически анонсируют свои адреса сетевого уровня и MAC-адреса с помощью эквивалента пакета приветствия (hello packet), который свидетельствует о том, что клиент по-прежнему функционирует и готов ко взаимодействию с сетью. Сами серверы периодически посылают другим серверам сообщения об обновлениях маршрутов для извещения их об изменениях в адресах узлов и топологии сети.

Когда VINES-сервер получает пакет, он проверяет, не предназначен ли этот пакет другому серверу и не является ли он широковещательным. Если данный сервер является пунктом назначения этого пакета, то он обрабатывается соответствующим образом. Если же пунктом назначения является другой сервер, то пакет пересылается непосредственно (если сервер-получатель является соседним) или направляется на следующий сервер линии. Если пакет является широковещательным, то сервер проверяет, пришел ли этот пакет по маршруту с наименьшей оценкой. Если это не так, то пакет отбрасывается. Если же маршрут оказался кратчайшим (с наименьшей оценкой), то пакет отправляется на все интерфейсы, кроме того, на который он поступил. Такой подход позволяет уменьшить количество широковещательных лавин (broadcast storm), которые являются типичной проблемой других сетевых сред. На рис. Б.9 показан алгоритм маршрутизации протокола VINES.

На рис. Б.10 показан формат пакета VIP.

Поля VIP-пакета содержат информацию о контрольной сумме, длине пакета, транспортном управлении, типе протокола, номере сети-получателя, номере подсети-получателя, номере сети-источника и номере подсети-источника.

Поле контрольной суммы используется для проверки целостности пакета. Поле длины пакета указывает длину всего VIP-пакета.

Поле транспортного управления (Transport Control) состоит из нескольких подполей. Если пакет является широковещательным, то используются два подполя: класс пакета (биты с 1-го по 3-й) и количество переходов (биты 4-7). Если пакет не является широковещательным, то присутствуют четыре подполя: подполе ошибки, метрики, перенаправления и количества переходов. Подполе класса задает тип узлов, которые должны получать широковещательное сообщение. С этой целью узлы делятся на различные категории, в соответствии с типом узла и типом канала, в котором находится данный узел. Задавая тип узлов, которые должны получать широковещательные сообщения, подполе класса уменьшает количество нарушений нормальной работы сети, вызываемых широковещанием. Подполе числа переходов отображает количество переходов (между маршрутизаторами), которые прошел данный пакет. Подполе ошибки определяет, следует ли использовать протокол ICP, который должен посылать пакет уведомления-

исключения источнику полученного пакета, в случае, если пакет не удается маршрутизировать. Подполе метрики устанавливается равным 1 протоколом транспортного уровня в случае, когда необходимо узнать оценку перемещения пакета между узлом службы и соседним устройством. Подполе перенаправления устанавливает, должен ли маршрутизатор генерировать перенаправление в соответствующих ситуациях.

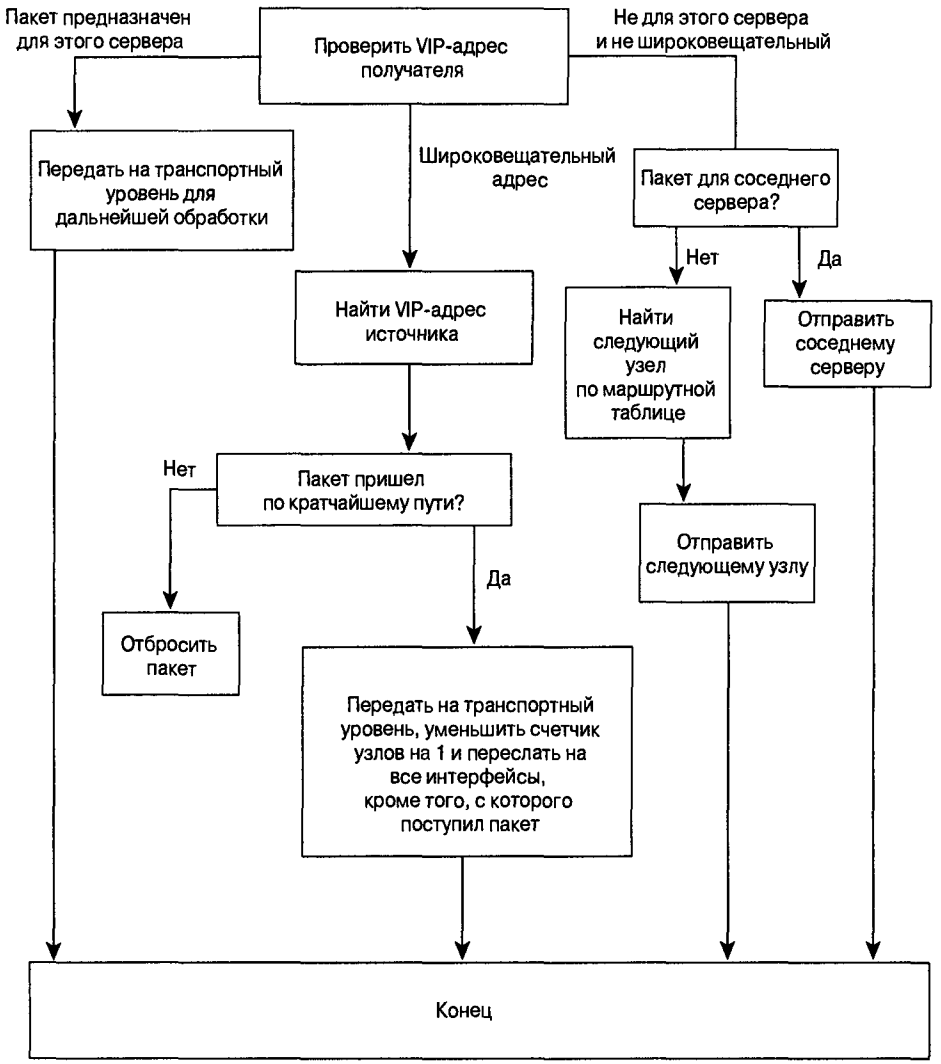


Рис. Б.9. Алгоритм VINES-маршрутизации определяет соответствующий маршрут к пункту назначения

Поле типа протокола указывает протокол сетевого или транспортного уровня, для которого предназначен пакет метрики или пакет исключения-уведомления.

В конечном итоге все поля: номер сети-получателя, номер подсети-получателя, номер сети-источника и номер подсети-источника образуют адресную информацию протокола VIP.

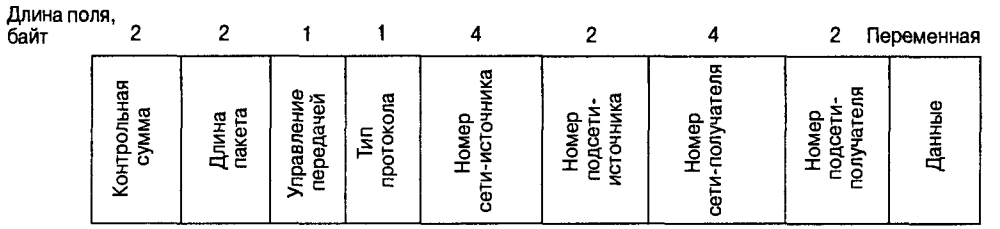


Рис. Б.10. VIP-пакет состоит из девяти индивидуальных полей

Протокол таблицы маршрутизации

Протокол таблицы маршрутизации (Routing Table Protocol — RTP) распространяет информацию о сетевой топологии. Широковещательные пакеты с обновлениями маршрутов периодически рассылаются как клиентскими узлами, так и узлами серверов. Эти пакеты информируют соседние устройства о существовании рассылающего эти сообщения узла, а также о его типе как клиента или сервера. В каждый пакет обновления маршрутов служба включает список всех известных сетей и соответствующие оценки (значения метрики), связанные с достижением этих сетей.

При этом поддерживаются две таблицы маршрутизации: таблица всех известных сетей и таблица соседних устройств. Для узлов службы таблица всех известных сетей содержит соответствующую позицию для каждой известной сети, за исключением собственной сети узла службы. Каждая позиция таблицы содержит номер сети, метрику маршрутизации и указатель позиции в таблице следующего перехода к этой сети в таблице соседних устройств. Таблица соседних устройств содержит позицию для каждого соседнего узла службы и для каждого узла клиента. Каждая позиция включает в себя номер сети, номер подсети, протокол доступа к передающей среде (например Ethernet), используемый для достижения этого узла, адрес локальной сети (local area-network — LAN), если средой, соединяющей с соседним устройством, является LAN, и метрику для соседнего устройства.

Протокол RTP определяет четыре типа пакетов: пакеты обновления маршрутов, запрос о маршрутизации, ответ на запрос о маршрутизации и пакет перенаправления маршрутизации. Пакеты обновления маршрутов используются для уведомления соседних устройств о существовании данного узла. Запросами о маршрутизации соседние устройства обмениваются в тех случаях, когда необходимо быстро изучить топологию сети. Ответы на запросы о маршрутизации содержат топологическую информацию и используются узлами службы для ответа на пакеты запросов о маршрутизации. Пакеты перенаправления маршрутизации предоставляют улучшенную информацию о маршрутах узлам, использующим неэффективные маршруты.

Пакеты протокола RTP имеют 4-байтовый заголовок, состоящий из следующих однобайтовых полей: поля типа операции (указывающего тип пакета), поля типа узла (указывающего, пришел ли пакет с узла службы или с иного узла), поля типа контроллера (указывающего, является ли контроллер узла, передающего RTP-пакет, многобуферным) и поля типа машины (Machine Type), указывающего, является ли процессор RTP-отправителя быстрым или медленным.

Оба поля — типа контроллера и типа машины — используются для регулирования скорости передачи данных (pacing).

Протокол преобразования адресов

Протокол преобразования адресов (Address Resolution Protocol — ARP) работает с объектами, которые классифицируются как клиенты преобразования адресов или службы преобразования адресов. Клиенты преобразования адресов обычно реализуются в клиентских узлах, в то время как службы преобразования адресов обычно представляются узлами службы.

Пакеты протокола ARP имеют 8-байтовый заголовок, состоящий из 2-байтового типа пакета, 4-байтового номера сети и 2-байтового номера подсети. Существуют четыре типа пакетов: запрос (используемый для обращения к ARP-службе), отклик службы (являющийся ответом на запрос), запрос о назначении (посылаемый ARP-службе для запроса межсетевого адреса VINES) и ответ на запрос о назначении (посылаемый службой ARP как ответ на запрос о назначении). Поля номера сети и номера подсети имеют значение только в пакетах ответа на запрос о назначении.

Клиенты и службы протокола ARP в начале работы клиента реализуют следующий алгоритм: сначала клиент широковещательно рассылает пакеты запроса, затем каждая служба, которая является соседней по отношению к данном узлу, отвечает пакетом ответа службы на запрос. После этого клиент посылает пакет с запросом о назначении первой службе, которая ответила на его пакет запроса. Служба отвечает пакетом ответа-назначения, в котором содержится назначенный межсетевой адрес.

Межсетевой протокол управления

Межсетевой протокол управления (Internet Control Protocol — ICP) определяет форматы пакетов исключения-уведомления (exception-notification packets) и пакетов уведомления о метрике (metric-notification packets). Пакеты исключения-уведомления предоставляют информацию об исключениях сетевого уровня, а пакеты уведомления о метрике содержат информацию о последней передаче, которая использовалась для достижения клиентского узла.

Пакеты исключения-уведомления посылаются в тех случаях, когда VIP-пакет не может быть маршрутизирован обычным образом и активизировано подполе ошибки в поле VIP-заголовка транспортного контроля. Эти пакеты также содержат поле, идентифицирующее данную конкретную ошибку ее кодом.

Элементы протокола ICP в узлах службы генерируют сообщения уведомления о метрике в тех случаях, когда активизировано подполе метрики в поле транспортного контроля VIP-заголовка, а адрес пункта назначения в пакете узла службы задает одно из соседних устройств узла службы.

Транспортный уровень

Протокол VINES предоставляет три службы транспортного уровня: службу негарантированной доставки дейтаграмм, службу гарантированной доставки сообщений и службу передачи потоков данных.

Служба негарантированной доставки дейтаграмм отправляет пакеты по принципу негарантированной доставки без подтверждения их получения в пункте назначения.

Служба гарантированной доставки сообщений является службой виртуального канала, которая обеспечивает гарантированную доставку сообщений от одного узла другому в соответствующем порядке с подтверждением получения.

Служба передачи потока данных поддерживает управляемые потоки данных между двумя процессами. Служба передачи потока данных является службой виртуального канала с подтверждением получения, которая обеспечивает передачу сообщений произвольного размера.

Протоколы верхних уровней

Являясь распределенной сетью, VINES-сеть использует модель вызова удаленной процедуры (Remote Procedure Call — RPC) для связи между клиентами и серверами. Модель RPC является основой среды распределенных служб. Протокол NetRPC (5-й и 6-й уровни) предоставляет пользователю язык программирования высокого уровня, который позволяет получить доступ к удаленным службам прозрачно как для пользователя, так и для приложения.

На 7-м уровне VINES предоставляет приложения файловой службы и службы печати, а также протокол StreetTalk, который обеспечивает службу глобально согласованных имен для всей объединенной сети.

Протокол VINES также обеспечивает среду интегрированной разработки приложений при работе в различных операционных системах, включая DOS и UNIX. Эта среда разработки позволяет другим пользователям разрабатывать как клиентские, так и серверные службы, работающие в среде VINES.

Резюме

Возможно, что это последняя книга, в которой рассматривается протокол VINES. Сообщество пользователей этого протокола практически распалось, ОС сервера и программное обеспечение VINES уже не продаются, а преобразование сети VINES в сеть IP/TCP больше не обеспечивается.

Дополнительные источники

- http://products.banyan.com/

Предметный указатель

A

AAL, ATM Adaptation Layer, 515; 516
AAL1, ATM Adaptation Layer 1, 289
AARP, AppleTalk Address Resolution Protocol, 622; 623
ABM, Asynchronous Balanced Mode, 249
ABR, Available Bit Rate, 289
ACF/VTAM, Advanced Communication Facility/Virtual Telecommunication Access Method, 637
ACSE, Association Control Service Element, 576
Address Gleaning, 623
Adjacent endpoint, 778
Adjacent node, 778
ADPCM, adaptive differential pulse code modulation, 294
ADSL, Asymmetric Digital Subscriber Line, 361
ADSP, AppleTalk Data Stream Protocol, 629
AEP, AppleTalk Echo Protocol, 629
AFI, Authority and Format Identifier, 290
AFP, AppleTalk Filing Protocol, 629; 631
ALO, At-Least-Once, 628
AMT, Address Mapping Table, 622
ANSI, American National Standards Institute, 70
Anycast, 599
AppleTalk, 613
APPN, Advanced Peer-to-Peer Networking, 642
Area, 60; 740
ARM, Asynchronous Response Mode, 249
ARP, Address Resolution Protocol, 64; 587
AS, Autonomous System, 60
ASE, Application Service Element, 658
ASP, AppleTalk Session Protocol, 630
ATDM, asynchronous time-division multiplexing, 69
ATM, Asynchronous Transfer Mode, 59; 509
ATM-адресация, 519
ATM-соединение, 521
ATP, AppleTalk Transaction Protocol, 628
AURP, AppleTalk Update-Based Routing Protocol, 627
A-закон, 294

B

BECN, backward-explicit congestion notification, 189; 194
BER, Bit-Error Rate, 335
Best-effort traffic, 764
BGP, Border Gateway Protocol, 665
BIA, Burned-In Address, 63
BIS, Border Intermediate System, 752
B-ISDN, Broadband ISDN, 509
BIU, Basic Information Unit, 646
BPDU, bridge protocol data unit, 60; 482
BPSK, binary phase shift keying, 334
BRI, Basic Rate Interface, 205; 209; 232
Broadcast transmission, 76
BTA, Basic Trading Area, 355
Bus topology, 76
BUS, Broadcast and Unknown Server, 528
B-канал, 205; 232

C

CA, Call Agent, 306
Canureach, 558
CAP, Carrierless Amplitude and Phase, 366
CAS, Channel Associated Signaling, 233
CASE, Common-Application Service Element, 576
CATV, Cable Television System, 375
CBR, Constant Bit Rate, 288

CBWFQ, Class-Based Weighted Fair Queuing, 927
CCRSE, Commitment, Concurrence, and Recovery Service Element, 576
CDDI, Copper Distributed Data Interface, 171; 180
CDMA, Code Division Multiple Access, 338; 355
CGMP, Cisco Group Management Protocol, 709
CHAP, Challenge Handshake Authentication Protocol, 237
child endpoint, 778
Child node, 778
Child port, 778
Cisco Catalyst 2924XL, 104
Cisco Catalyst 6500, 104
Cisco IOS QoS, 910
CLNP, Connectionless Network Protocol, 571
CLP, Cell Loss Priority, 513
CMIP, Common Management-Information Protocol, 577
Collection point, 882
CONP, Connection-Oriented Network Protocol, 571
Containment, 809
CoS, Class of Service, 687
CPE, Customer Premises Equipment, 217
CQ, Custom Queuing, 923
CRC, cyclic redundancy check, 68; 190
Creator endpoint, 778
Creator node, 778
CSMA/CD, Carrier Sense Multiple Access/Collision Detect, 75; 131
CSU/DSU, Channel Service Unit/Digital Service Unit, 86
Cut-through, 504
Cut-through switching, 107

D

DA, Destination Address, 136
DAC, Dual-Attached Concentrator, 174; 175
DAP, Data-Access Protocol, 658; 659
DAS, Dual-Attachment Station, 174
DAT, Digital Audio Tape, 283
Data unit, 60
Datagram, 59
dBi, 356
DCE, Data Communication Equipment, 132; 186; 195; 253
DDP, Datagram Delivery Protocol, 623
DDP-пакет
  формат, 632
DDR, Dial-on-Demand Routing, 85
DE, Discard Eligibility, 190; 194
DECnet, 651
  Phase IV, 652
  Phase V, 654
DECnet/OSI, 654
Delay-sensitive traffic, 765
DEN, Directory-Enabled Networks, 807; 986
Designated node, 778
Destination tree, 777
DFE, Decision Feedback Equalizer, 337
DHCP, Dynamic Host Configuration Protocol, 383
Dial backup, 85
Dialer, 239
Dialup, 229
Distance vector, 118
DIT, Directory Information Tree, 813
DLC, Data Link Control, 638; 639
DLCI, Data-Link Connection Identifier, 187; 189; 191; 193; 196
DLSw, Data-Link Switching, 553
DLUR/S, Dependent Logical-Unit Requester/Server, 692
DNA, Digital Network Architecture, 652
DNS, Domain Name System, 594
DOCSIS 1.0, Data Over Cable Service Interface Specification, 375
Domain, 740
DOS, denial of service, 61
DQDB, Distributed Queue Dual Bus, 220
DS, Directory Services, 577
DSL, Digital Subscriber Line, 361
DSP, Digital Signal Processor, 282
DSSS, direct sequence spread spectrum, 338
DTE, Data Terminal Equipment, 132; 186; 195; 253
DTL, Designated Transit List, 525

Dual homing, 178
D-канал, 205; 206; 232

E

E&M, ear and mouth, 287
EA, Extended Address, 193
EIA, Electronic Industries Association, 70
EIGRP, Enhanced Internet Gateway Routing Protocol, 677
EIRP, Effective Isotropic Radiated Power, 356
ELAP, EtherTalk Link Access Protocol, 618
EN, End Node, 643
Endpoint, 778
Entry point, 882
ES, End System, 60; 114; 739
ESCON, Enterprise Systems CONnection, 640
ES-IS, End System-to-Intermediate System, 741
Ethernet, 131
  1000Base?, 953
  1000BaseT, 154; 952
  1000BaseX, 156
  100BaseT2, 151
  100BaseT4, 150
  100BaseX, 148
  10BaseT, 147
  10-Gigabit, 131
  Fast Ethernet, 148
  Gigabit Ethemet, 153
  многоскоростная, 164
EtherTalk, 617

F

Fast Ethernet, 148
FCS, Frame Check Sequence, 136; 180; 247
FDDI, Fiber Distributed Data Interface, 171
FDDITalk, 620
FDDI-концентратор, 175
FDM, frequency-division multiplexing, 69; 339
FEC, Forward Error Correction, 335
FECN, forward-explicit congestion notification, 189; 193
FEP, Front-End Processor, 639
FF, Fixed-Filter, 767
FHSS, frequency hopping spread spectrum, 338; 339
FIFO, First-In, First-Out, 922
FLAP, FDDITalk Link Access Protocol, 621
Flat address space, 66
Flat routing, 117
Flow, 909
Flow specification, 764
FLP, fast link pulse, 160
Flush timer, 700
Focal point, 882
Footprint, 356
FQDN, Fully Qualified Distinguished Name, 813
Frame, 58
Frame Relay, 185
  передача речи, 285; 292
Freshness factor, 847
FRTS, Frame Relay Traffic Shaping, 933
FTAM, File Transfer, Access, and Management, 577
FTP, File Transfer Protocol, 594
FXO, Foreign Exchange Office, 287
FXS, Foreign Exchange Service, 287

G

G.711, 295
G.723.1, 295
G.726, 295
G.728, 295
G.729, 295
Gatekeeper, 303
Gateway, 588
GFC, Generic Flow Control, 513
GFI, General Format Identifier, 257
Gigabit Ethernet, 153
Granted units, 560
Group, 777

H

H.323, 293; 302

HDLC, High-Level Data Link Control, 245; 248; 250
HDSL, High-speed Digital Subscriber Line, 369
HDSL-2, High-speed Digital Subscriber Line, 369
Header, 53
HEC, Header Error Control, 513
Hello packet, 681
Hello protocol, 64
Hierarchical address space, 66
HIPPI, HIgh-Performance Parallel Interface, 200
Holddown, 698
Hold-time period, 700
HPR, High-Performance Routing, 691
HSSI, High-Speed Serial Interface, 199
Hub, 78

I

IAB, Internet Activities Board, 70
Icanreach, 559
ICMP, Internet Control Message Protocol, 589
IDRP, InterDomain Routing Protocol, 751
IEEE 802.2, 249; 251
IEEE, Institute of Electrical and Electronic Engineers, 70
IFCM, Independent Flow Control Message, 561
Iframe, 561
IGMP, Internet Group Management Protocol, 706
IGMP-прослушивание, 709
IGRP, Interior Gateway Routing Protocol, 697
ILMI, Integrated Local Management Interface, 525
internetwork, 47
Internetwork address, 62
Invalid timer, 700
IPv6, 597
IPX, Internetwork Packet Exchange, 606
IPX-пакет
  формат, 610
IP-адресация, 582
  групповая, 703
IP-маршрутизация, 588
IP-пакет
  формат, 580
IP-протокол, 580
IP-сеть
  передача голоса, 285
IP-сеть
  передача речи, 293
IRDP, ICMP Router-Discovery Protocol, 589
IS, Intermediate System, 60; 114; 739
ISDL, ISDN Digital Subscriber Line, 370
ISDN, Integrated Services Digital Network, 82; 203
ISI, InterSymbol Interference, 336
ISO 8348, 571
ISO 8648, 570
ISO TR 9575, 571
ISO, International Organization for Standardization, 70
ISR, Intermediate Session Routing, 691
ITU-T, International Telecommunication Union Telecommunication Standardization Sector, 70
IWF-плата, 341
I-фрейм, 257

J

Joining path, 778
JTAPI, Java Telephony API, 314

L

LAN extender, 78
LAN, Local-Area Network, 47; 73
LANE, LAN Emulation, 526
LAPB, Link Access Procedure, Balanced, 257
LAPB, Link-Access Procedure, Balanced, 249; 250
LAPD, Link Access Procedure, D channel, 206
LCI, Logical Channel Identifier, 257
LDP, Label distribution protocol, 539
LEC, LAN Emulation Client, 527

LECS, LAN Emulation Configuration Server, 528
LEN, Low-Entry Node, 643
LES, LAN Emulation Server, 528
Link aggregation, 166
Link-state algorithms, 117
LLAP, LocalTalk Link Access Protocol, 619
LLC, Logical Link Control, 56; 106; 249
LMDS, Local Multipoint Distribution Service, 357
LMI, Local Management Interface, 190; 954
LNM, LAN Network Manager, 884
Load sharing, 116
Lobe cable, 996
Local net, 777
LocalTalk, 619
LOS, Line Of Sight, 357
Low Cost Fibre Interface Connector, 149
LSC, Label switch controller, 539
LSP, Label-switched path, 538
LSR, Label Switch Router, 538
LU, Logical Unit, 641
LVC, Label virtual circuit, 539

M

MAC, Media Access Control, 106; 135; 173
  Ethernet, 135
MAC-адрес, 56; 63; 64
MADCAP, Multicast Address Dynamic Client Allocation Protocol, 718
MAN, Metropolitan-Area Network, 220
MBGP, Multiprotocol Border Gateway Protocol, 715
MC, Multipoint Controller, 303
MCU, Mutipoint Control Unit, 303
MDI, medium-dependent interface, 147
Media Access Control, 56
Member endpoint, 778
Member node, 778
MG, Media Gateway, 305
MGC, Media Gateway Controller, 305
MGCP, Media Gateway Control Protocol, 304
MHS, Message Handling System, 577
MIB, Management Information Base, 893
MLP, MultiLink Point-to-point protocol, 238
MMDS, Multichannel Multipoint Distribution Service, 357
MMP, Multichassis Multilink PPP, 238
MP, Multipoint Processor, 303
MPC, MultiProtocol Client, 533
MPLS, MultiProtocol Label Switching, 537; 939
MPOA, MultiProtocol Over ATM, 532
MPS, MultiProtocol Server, 533
MTP, Multicast Transaction Protocol, 780
Multicast, 599
Multicast transmission, 76
Multipath, 331
mu-закон, 294
MZAP, Multicast-Scope Zone Announcement Protocol, 718

N

NAU, Network Addressable Unit, 641
NBP, Name Binding Protocol, 625
NCP, NetWare Core Protocol, 609
neighbor node, 778
NET, Network Entity Title, 573
NetView, 883
NetWare MHS, 610
NetWare RPC, 609
NFS, Network File System, 594
NIC, network interface card, 132
NICE, Network Information and Control Exchange, 657
NIU, network interface unit, 341
NLOS, Non-Line-Of-Sight, 357
NLP, normal link pulse, 148
NLSP, NetWare Link-Services Protocol, 721
NMS, Network Management System, 124; 342
NMS, Network-Management System, 892
NN, Network Node, 643
Node, 778
NRM, Normal Response Mode, 249
NSP, Network-Services Protocol, 656

O

OFDM, Orthogonal Frequency-Division Multiplexing, 339
ONA, Open-Network Architecture, 882
OSI, Open System Interconnection, 569
OSPF, Open Shortest Path First, 731
OSS, Operational Support System, 342

P

P2MP, Point-To-MultiPoint, 358
P2P, Point-To-Point, 358
PAD, Packet Assembler/Disassembler, 254
PAP, Password Authentication Protocol, 237
PAP, Printer Access Protocol, 630
PAR, Positive Acknowledgment and Retransmission, 591
Parent node, 778
parent port, 778
Patch cable, 996
PCM, pulse code modulated, 294
PCS, physical coding sublayer, 146
PDU, protocol data unit, 60
PGM, Pragmatic General Multicast, 719
PHY, PHYsical layer protocol, 173
PIM, Protocol-Independent Multicast, 714
PIM-DM, PIM Dense Mode, 714
PIM-SM, PIM Sparse Mode, 715
PIU, Path Information Unit, 647
PLP, Packet-Layer Protocol, 256
PMA, physical medium attachment, 146
PMD, Physical Medium-Dependent, 515
PMD, Physical-Medium Dependent, 173
PNNI, Private Network-Network Interface, 525
PNNI, Private Network-to-Network Interface, 291
PN-код, 338
Poison-reverse update, 699
Port, 778
Port parent, 777
POTS, Plain Old Telephone Service, 231
PPP, Point-to-Point Protocol, 214; 236
PQ, Priority Queuing, 922
PRE, preamble, 136
PRI, Primary Rate Interface, 205; 209; 233
Primary node, 778
PSE, packed-switching exchange, 253
PSK, Phase Shift Keying, 334
PSN, packet-switched network, 187
PT, Payload Type, 513
PTI, Packet Type Identifier, 257
PU, Physical Unit, 641
PVC, Permanent Virtual Circuit, 84; 188; 196; 255; 513; 954

Q

QAM, Quadrature Amplitude Modulation, 334
QLLC, Qualified Logical Link Control, 250; 251
QoS, Quality of Service, 766; 909
QPSK, Quadrature Phase Shift Keying, 334

R

Rate-sensitive traffic, 764
RD, Routing Domain, 752
RDI, Routing Domain Identifier, 752
RDN, Relative Distinguished Name, 813
RED, Random Early Detection, 929
Repeater, 78
Reverse path, 778
RF, Radio Frequency, 358
RIB, Routing Information Base, 752
Ring topology, 76
RIP, Routing Information Protocol, 757
RMON, Remote Monitoring, 887
ROSE, Remote Operations Service Element, 576
Routed protocol, 119
Routing, 111
Routing protocol, 119
RP, Rendezvous Point, 716
RPF, Reverse Path Forwarding, 713
RPF-проверка, 713
RS, Redirect Server, 309
RSVP, Resource Reservation Protocol, 763
RTMP, Routing Table Maintenance Protocol, 625
RTP, Reliable Transport Protocol, 678

RTSE, Reliable Transfer Service Element, 576
RTU, rooftop unit, 341

S

s/n, signal-to-noise, 335
SA, Source Address, 136
SAC, Single-Attached Concentrator, 174
SAP, Service Access Point, 53
SAP, Service Advertisement Protocol, 608
SAS, Single-Attachment Station, 174
SASE, Specific-Application Service Elements, 577
SCP, Session Control Protocol, 658; 659
SC-разъем, 149
SDLC, Synchronous Data Link Control, 245; 556
SDSL, Symmetric Digital Subscriber Line, 368
SDU, service data unit, 60
SE, Shared-Explicit, 767
Secondary node, 778
Service point, 882
Shaping, 913
SIP, Session Initiation Protocol, 293; 308
SIP, SMDS Interface Protocol, 218; 225; 956
SMDS, Switched Multimegabit Data Service, 59; 217; 225
SMI, Structure of Management Information, 896
SMRP, Simple Multicast Routing Protocol, 777
SMT, Station ManagemenT, 173
SMTP, Simple Mail Transfer Protocol, 594
SNA, Systems Network Architecture, 637
SNI, Subscriber Network Interface, 217; 220; 225
SNMP, Simple Network Management Protocol, 167; 594; 891
SOF, Start-of-Frame Delimiter, 136
Soft state, 768
Source routing, 117
Source tree, 777
Source-route bridging, 103
Source-route transparent bridging, 103
Spanning tree, 777
SPF, Shortest Path First, 733
Split horizons, 699
SPX, Sequenced Packet Exchange, 609
SRB, Source-Route Bridging, 495
SSP, Switch-to-Switch Protocol, 556
STA, Spanning-Tree Algorithm, 480
Star topology, 77
Store-and-forward, 504
Store-and-forward switching, 107
STP, shielded twisted-pair, 132
SVC, Switched Virtual Circuit, 84; 188; 195; 255; 513; 954
SystemView, 882
S-фрейм, 257

T

T1/E1, 232
TAPI, Telephony API, 314
TC, Transmission Convergence, 515
TCP, Transmission Control Protocol, 590
TCP-пакет
формат, 592
TDM, Time Division Multiplexing, 232
TDM, time-division multiplexing, 69; 510
TDMA, Time-Division Multiple Access, 358
TDU, Topology Database Update, 645
Teardown message, 771
Telnet, 594
TFIB, Tag Forwarding Information Base, 538
TFTP, Trivial File Transfer Protocol, 383
TG, Transmission Group, 645; 686
Three-way handshake, 590
Tick, 607
TLAP, TokenTalk Link Access Protocol, 620
TOD, Time of Day, 383
Token, 75
Token-passing network, 75
TokenTalk, 620
TP-DDI, Twisted-Pair Distributed Data Interface, 180
TP-PMD, Twisted-Pair Physical Medium-Dependent, 180
Trailer, 53

Translational bridging, 103
Transparent bridging, 103
Tree topology, 77
TSAPI, Telephony Services API, 314
TTL, Time-To-Live, 847
Tunnel, 778

U

UART, Universal Asynchronous Receiver/Transmitter, 235
UBR, Unspecified Bit Rate, 289
UDP, User Datagram Protocol, 593
Unicast, 599
Unicast transmission, 76
U-NII, Unlicensed National Information Infrastructure, 358
Update timer, 700
UTP, unshielded twisted-pair, 132
U-фрейм, 257

V

V.110, 230
V.21, 230
V.23, 230
V.25, 230
V.25bis, 230
V.25ter, 230
V.27ter, 230
V.29, 230
V.32bis, 230
V.34, 230
V.8, 230
V.90, 230
VBR, Variable Bit Rate, 288; 517
VCI, Virtual Channel Identifier, 513; 514
Virtual circuit, 255
VLAN, Virtual Local Area Network, 502
VoATM, Voice over ATM, 285; 288
VOFDM, Vectored OFDM, 340
VoFR, Voice over Frame Relay, 292
VoIP, Voice over IP, 285; 293
VPI, Virtual Path Identifier, 513; 514
VTP, Virtual Terminal Protocol, 577

W

WAN, Wide-Area Network, 48; 81
WAP, Wireless Access Protocol, 358
WCCP multihoming, 841
Web-кэширование, 834
WF, Wildcard-Filter, 766
WFQ, Weighted Fair Queuing, 924

X

X Windows, 594
xDSL, 361
XmplsATM, 539
XO, eXactly-Once, 628

Z

ZIP, Zone Information Protocol, 630

А

AAA, Authentication, Authorization, and Accounting, 238
Абонентская сеть, 341
Абонентский канал
  цифровой, 361
    ISDN, 370
    асимметричный, 361
    сверхскоростной, 371
    симметричный, 368
Автономная система, 60
Автономный кэш, 836
Автосогласование, 159
Агент, 124; 892
  вызова, 306
Адаптационный уровень ATM, 515; 516
Адаптер
  сетевой
    многоскоростной, 162
  терминала ISDN, 87
Адаптивная дифференциальная импульсно-кодовая модуляция, 294
Адаптивное пошаговое продвижение, 559
Адаптивный компенсатор, 367
Административно ограниченный адрес, 705

Адрес
MAC, 56; 63; 64
аппаратный, 62
глобальный, 705
групповой, 137; 706
динамический, 66
индивидуальный, 137
канального уровня, 62
локальный, 705
межсетевой, 62; 67
множественный, 137
ограниченного радиуса действия, 705
одиночный, 137
прошитый, 63
расширенный, 193
родительский, 777
сетевой, 56; 64; 65
статический, 66; 705
физический, 62; 104
широковещательный, 137
Адресация
ATM, 519
Адресуемый сетевой модуль, 641
Активный приемник, 680
Алгоритм
Дейкстра, 731
маршрутизации, 114
связующего дерева, 480
Альтернативная точка рандеву, 717
Американский национальный институт стандартов, 70
Амплитуда, 354
Аналоговый сигнал, 354
Антенна, 355
коэффициент усиления, 355
параболическая, 357
Аппаратный адрес, 62
Архитектура
сетевая
открытая, 882
Асимметричный коммутатор локальной сети, 505
Асимметричный цифровой абонентский канал, 361
Асинхронное мультиплексирование с разделением времени, 69
Ассоциация электронной промышленности, 70
Атака
отказ в обслуживании, 61
Аутентификация, 237

Б

База
управляющей информации, 893
База данных
маршрутная, 752
сетевой топологии, 645
Базовая территория обслуживания, 355
Базовый информационный модуль, 646
Беспроводная сеть
фиксированная, 356
Беспроводная система
мобильная, 357
Бит
BECN, 190
FECN, 189
сброса, 190; 194
Буферизация, 67

В

Вектор расстояния, 118
Верхние уровни модели OSI, 51
Взвешенная справедливая очередность
классовая, 927
потоковая, 924
Видимость
непрямая, 357
прямая, 357
Виртуальный канал, 84; 187; 255; 514
коммутируемый, 84; 188; 195; 255; 513
постоянный, 84; 188; 196; 255; 513
Виртуальный маршрут, 514; 686
Витая пара
неэкранированная, 132
экранированная, 132
Внешняя промежуточная система, 752
Внутренний модуль, 341
Внутридоменная маршрутизация, 117

Внутридоменная промежуточная
система, 114
Время жизни, 847
Вторичный узел, 246; 778
Вызов, 306

Г

Гарантированная доставка, 914
Гарантированное обслуживание, 915
Гибкое состояние, 768
Гигант, 504
Глобальная объединенная сеть, 722
Глобальный адрес, 705
Голосовой кодек, 282; 293
Горизонт, 699
Горизонтальная кабельная проводка,
166
Граничный узел, 693
Группа, 777
RMON, 887
многоадресатная, 703
передачи, 686
трансмиссионная, 645
Групповая IP-адресация, 703
Групповая фильтрация, 766
Групповой адрес, 137; 706

Д

дБ, 356
дБВт, 356
дБм, 356
Двоичная фазовая модуляция, 334
Двойное кольцо FDDI, 175
Двойное подключение, 178
Двухпортовая станция, 174
Двухпортовый концентратор, 174; 175
Дейтаграмма, 59
Демодулятор, 356
Демультиплексирование, 68
Дерево
источника, 710; 777
общего доступа, 710
получателей, 777
связное, 777
многоадресное, 710
связующее, 480
Децибел, 356
Динамическая маршрутизация, 116
Динамический адрес, 66
Дисперсия
модовая, 173
Дифференцированное обслуживание,
915
Длина исходящей очереди, 560
Длина маршрута, 118
Домен, 722; 740
коллизионный, 138
маршрутизации, 114; 752
широковещательный, 502
Допустимый маршрутизатор, 679
Доставка
гарантированная, 914
Доступ
множественный, 138
с кодовым разделением каналов,
338
множественный, с кодовым
разделением, 355
множественный, с разделением
времени, 358
Доступность
буфера, 560
Дочерний порт, 778
Дочерний узел, 778
Дочерняя конечная точка, 778
Драйвер шлюза, 303
Древовидная топология, 77
Дуплексная передача, 140

Е

ECL, Emitter-Coupled Logic, 200

З

Заголовок, 53; 58
Загрузка
канала, 560
Задержка
изменений, 698; 700
при маршрутизации, 119
Замкнутая конфигурация, 246
Запрашивающая сторона, 237
Запрос

на резервирование, 770
Звездообразная топология, 77; 133
Зона, 60; 722; 740
Зона сети AppleTalk, 616

И

Идентификатор
ASN.1, 814
домена маршрутизации, 752
канального соединения, 187; 189; 193; 196
Иерархическая маршрутизация, 117; 546; 722
Иерархическое пространство адресов, 66
Иерархическое развертывание, 839
Имя
межсетевое, 67
отличительное
определенное, 813
относительное, 813
Индивидуальный адрес, 137
Инкапсуляция данных, 168
Институт инженеров по электротехнике и радиоэлектронике, 70
Интегрированный сетевой кэш, 835
Интеллектуальный контроллер шлюза среды передачи, 305
Интервал
задержки изменений, 698
Интервал таймера, 607
Интерфейс
абонента, 217; 220; 225
локального управления, 190
обмена
первичный, 233
Информационная модель, 807
Информационный фрейм, 257
Информация
управляющая, 53
Исходная конечная точка, 778
Исходный узел, 778

К

Кабель
коаксиальный, 355
ответвления, 996
соединительный, 996
Кампус, 164
Канал, 355
виртуальный, 84; 187; 255; 514
коммутируемый, 513
постоянный, 513
коммутируемый, 82
виртуальный, 84; 188; 195; 255
локальный, 777
открытие, 558
постоянный
виртуальный, 84; 188; 196; 255
смежный, 354
цифровой абонентский, 361
ISDN, 370
асимметричный, 361; 368; 371
Канальный уровень, 55; 58; 62; 104; 569
Карлик, 504
Каталог, 813
сетевой, 807
Качество
обслуживания, 909
Качество обслуживания, 766
Квадратурно-амплитудная модуляция, 334
с обратной связью, 336
Квадратурно-фазовая модуляция, 334
Класс
доступа SMDS, 221
обслуживания, 687
объектный, 813
Классовая взвешенная справедливая очередность, 927
Кластеризация
масштабируемая, 839
Кластерный контроллер, 639
Клиент
многопротокольный, 533
Клиентское оборудование, 217
Коаксиальный кабель, 355
Код
псевдослучайный шумоподобный, 338
Кодек
голосовой, 282; 293

по источнику, 294
по форме сигнала, 294
Кодирование
манчестерское, 144
передаваемого сигнала, 143
Коллизионное окно, 138
Коллизионный домен, 138
Кольцевая топология, 76
Комитет по вопросам деятельности в Internet, 70
Коммуникационный контроллер, 639
Коммуникационный процессор, 639
Коммутатор, 103; 104; 107; 511; 951
ATM, 107
локальной сети
асимметричный, 505
многоуровневый, 506
симметричный, 505
локальных сетей, 501
сетевой, 161
Коммутатор локальных сетей, 107
Коммутатор распределенной сети, 85
Коммутация, 113
без буферизации пакетов, 107; 504
каналов, 82; 553
меток, 545
многопротокольная, 537
с промежуточным хранением, 107; 504
тегов, 939
Коммутация пакетов, 83
Коммутируемое соединение, 229
Коммутируемый виртуальный канал, 84; 188; 195; 255; 513
Компенсатор
адаптивный, 367
Комфортный шум, 297
Конвертор, 355
Конечная система, 60; 114; 739
Конечная станция, 124
Конечная точка, 306; 511; 778
дочерняя, 778
исходная, 778
смежная, 778
член группы, 778
Конечный узел, 643
Конструирование трафика, 550
Контракт трафика, 523
Контроллер
кластерный, 639
коммуникационный, 639
многопортовый, 303
установки, 639
шлюза среды передачи, 305
Контроль
петлевой, 200
Контроль несущей, 138
Контрольная последовательность фрейма, 136; 247
Контрольная точка, 641
Конфедерация, 752
Конференция по схеме, 304
Конфигурационное сообщение, 483
Конфигурация
замкнутая, 246
концентраторная, 246
многоточечная, 246
Концентратор, 78
FDDI, 175
двухпортовый, 174; 175
однопортовый, 174
Концентраторная конфигурация, 246
Корневой маршрут, 481
Корневой мост, 481
Корневой порт, 481
Коррекция ошибок
упреждающая, 335
Коэффициент
активности, 388
пика, 388
усиления антенны, 355
устаревания, 847
Коэффициент усиления, 357
Кратчайший маршрут, 532
Кэш
автономный, 836
сетевой
интегрированный, 835
Кэширование
сетевое, 833
прозрачное, 838
совместное, 837

Л

Линейная маршрутизация, 117
Линейное пространство адресов, 66
Лицензия, 357
Логический модуль, 641
Локализация, 809
Локальная сеть, 47; 73
Локальный адрес, 705
Локальный канал, 777
Локальный мост, 105; 951

М

Магистральный режим, 503
Манчестерское кодирование, 144
Маркер, 75
Маршрут
  виртуальный, 514; 686
  корневой, 481
  кратчайший, 532
  многоадресный, 782
  обратный, 778
  передачи, 514
  присоединения, 778
  явный, 686
Маршрутизатор
  допустимый, 679
Маршрутизация, 111
  APPN, 689
  DLUR/S, 692
  внутридоменная, 117
  динамическая, 116
  иерархическая, 117; 546
  иерархическая, 722
  линейная, 117
  междоменная, 117
  мостовая
    прозрачная от источника, 492; 495
  на источнике, 103; 117
  по вектору расстояния, 118; 697
  по состоянию канала, 117
  подзональная, 689
  промежуточного сеанса, 691
  с предоставлением канала по требованию, 85
  скоростная, 691
  статическая, 116
  уровня 1, 740
  уровня 2, 740
Маршрутизируемый протокол, 119
Маршрутная база данных, 752
Маршрутный информационный модуль, 647
Маска IP-подсети, 584
Масштабируемая кластеризация, 839
Машина
  с конечным числом состояний алгоритма DUAL, 679
Междоменная маршрутизация, 117
Междоменная промежуточная система, 114
Международная организация по стандартизации, 70
Международный союз по телекоммуникациям, сектор стандартизации, 70
Межсетевое имя, 67
Межсетевой адрес, 62; 67
Межсимвольные помехи, 336
Местная многоабонентская служба распределения, 357
Метрика, 112; 118
Микросегментация, 501
Многоадресатная передача, 76
Многоадресатная группа, 703
Многоадресатная передача, 522; 599
Многоадресатная пересылка, 712
Многоадресатное связное дерево, 710
Многоадресатный маршрут, 782
Многоканальная многоабонентская служба распределения, 357
Многомодовое оптоволокно, 173
Многоопорный многосвязный протокол, 238
Многопортовый контроллер, 303
Многопортовый процессор, 303
Многопортовый управляющий модуль, 303
Многопротокольная коммутация меток, 537
Многопротокольная схема, 532
Многопротокольный клиент, 533
Многопротокольный сервер, 533
Многосвязный протокол, 238
Многоскоростная сеть Ethernet, 164

Многоскоростной сетевой адаптер, 162
Многоточечная конфигурация, 246
Многоточечная система, 358
Многоуровневый коммутатор
локальной сети, 506
Множественная WCCP-адресация, 841
Множественный адрес, 137
Множественный доступ, 138
с кодовым разделением, 355
с кодовым разделением каналов, 338
Множественный доступ с разделением времени, 358
Мобильная беспроводная система, 357
Мод, 172
Модель
ATM, 515
OSI, 49
адресации
подсетевая, 519
данных, 807
информационная, 807
политик DEN, 819
управления сетью
ISO, 124
Модем, 86; 234
Модовая дисперсия, 173
Модуляция
двоичная фазовая, 334
квадратурно-амплитудная, 334
квадратурно-амплитудная с обратной связью, 336
квадратурно-фазовая, 334
широкополосная, 338
фазовая, 334
широкополосная, 337
методом частотных скачков, 339
Модуль
внутренний, 341
информационный
базовый, 646
маршрутный, 647
логический, 641
наружный, 341
сетевого интерфейса, 341
сетевой
адресуемый, 641
физический, 641
Модуль данных, 60
Мониторинг
удаленный, 887
Мост, 103; 104
корневой, 481
локальный, 105; 951
назначенный, 482
удаленный, 105; 951
уровня MAC, 106
Мостовая маршрутизация
прозрачная
от источника, 492; 495
Мостовая петля, 480
Мостовое соединение
прозрачное, 103
с маршрутизацией на источнике, 103
с маршрутизацией на источнике, 103
с трансляцией, 489
трансляционное, 103
Мощность
эффективная, изотропного излучателя, 356
Мультиплексирование, 68
с разделением времени
асинхронное, 69
с разделением частоты, 69
Мультиплексирование, статистическое, 69
Мультиплексор, 69

H

Нагрузка
маршрутизатора, 119
распределение, 116
Надежность
алгоритма маршрутизации, 118
Назначенный мост, 482
Назначенный порт, 482
Назначенный узел, 778; 781
Наложение сигналов, 331
Наружный модуль, 341
Настраиваемая очередность, 923
Нелицензируемая национальная информационная инфраструктура, 358

Ненумерованный фрейм, 257
Непрямая видимость, 357
Нерасширенная сеть AppleTalk, 615
Неэкранированная витая пара, 132
Нижние уровни модели OSI, 51
Низкоуровневый узел, 643
Номеронабиратель, 239

О

Обмен
  сведениями о функциях, 558
Обнаружение и восстановление
  соседних узлов, 678
Обнаружение коллизий, 138
Обновление
  обратное, 699
Оборудование
  клиентское, 217
  передающего тракта, 217; 220
  терминальное, 132; 186; 195; 203; 253
Оборудование передачи данных, 132; 186; 195; 253
Обратная передача, 713
Обратное обновление, 699
Обратное прокси-кэширование, 844
Обратный маршрут, 778
Обслуживание
  гарантированное, 915
  дифференцированное, 915
Обслуживание с гарантированной доставкой, 914
Объединение
  каналов, 166
Объединенная сеть, 47
  глобальная, 722
Объект
  каталога, 813
  скалярный, 894
  табличный, 894
Объектный класс, 813
Ограниченный адрес, 705
Одиночный адрес, 137
Одноадресатная передача, 76
Одноадресная передача, 599
Одномодовое оптоволокно, 173
Однопортовая станция, 174
Однопортовый концентратор, 174
Окно, 67
  коллизионное, 138
  скользящее, 591
Опорная сеть
  здания, 165
  кампуса, 165
Определенное отличительное имя, 813
Оптический обходной переключатель, 177
Оптоволокно
  многомодовое, 173
  одномодовое, 173
Отказ в обслуживании, 61
Открытая сетевая архитектура, 882
Открытая сеть, 191
Открытие канала, 558
Отличительное имя
  определенное, 813
  относительное, 813
Относительное отличительное имя, 813
Отношение сигнал/шум, 335
Очередность
  взвешенная справедливая
    классовая, 927
    потоковая, 924
  настраиваемая, 923
  приоритетная, 922

П

Пакет, 59
  запроса, 681
  коммутируемый, 83
  обновления, 681
  ответа, 681
  подтверждения, 681
  приветствия, 681; 724; 726
Параболическая антенна, 357
Пассивный приемник, 680
Первичный интерфейс обмена, 233
Первичный узел, 245; 778
Передача
  дуплексная, 140
  многоадресатная, 76
  многоадресная, 522; 599
  обратная, 713
  одноадресатная, 76

одноадресная, 599
полудуплексная, 138
широковещательная, 76; 355; 599
широкополосная, 355
Передача голоса
по IP-сетям, 285
по сетям ATM, 288
Передача голоса по Frame Relay, 292
Передача голоса по сетям Frame Relay, 285
Передача речи
по IP-сетям, 293
по сетям ATM, 285
Переключатель
оптический обходной, 177
Переполнение, 189
Пересылка
многоадресная, 712
Период
задержки изменений, 700
Петлевой контроль, 200
Петля
мостовая, 480
Плата
межсетевого взаимодействия, 341
Плоскость
контроля, 515
пользователя, 515
управления, 515
Плотный режим PIM, 714
Площадь
покрытия, 356
Повторитель, 78
Повторное использование частоты, 356
Подзональная маршрутизация, 689
Подключение
двойное, 178
Подсетевая модель адресации, 519
Подуровень
автосогласования, 147
дополнения физической среды передачи, 146
управления доступом к среде передачи, 56; 106; 135
Ethernet, 135
управления логическим каналом, 56; 106
физического кодирования, 146
Политика, 914
Полоса
частот, 355
Полоса пропускания, 119
Полудуплексная передача, 138
Пользователь службы, 53
Помехи
межсимвольные, 336
Порт, 778
дочерний, 778
корневой, 481
назначенный, 482
родительский, 778
Постоянный виртуальный канал, 84; 188; 196; 255; 513
Потери
при передаче, 358
Поток, 909
Потоковая взвешенная справедливая очередность, 924
Преобразование адресов, 64
Приемник
активный, 680
пассивный, 680
Признак
начала фрейма, 136
Приоритет, 997
трафика, 561
Приоритетная очередность, 922
Провайдер службы, 53
Прозрачная мостовая маршрутизация от источника, 492; 495
Прозрачное мостовое соединение, 103
с маршрутизацией на источнике, 103
Прозрачное сетевое кэширование, 838
Прокси-кэширование
обратное, 844
Прокси-сервер, 309; 835
Прокси-система, 303
Прокси-служба, 532
Промежуточная система, 60; 114; 739
внешняя, 752
внутридоменная, 114
междоменная, 114
Промежуточный узел, 132
Прослушивание
IGMP, 709

Простая импульсно-кодовая
модуляция речи, 294
Пространство адресов
иерархическое, 66
линейное, 66
Протокол, 51
беспроводного доступа, 358
коммутации тегов, 538
локальных сетей, 51
маршрутизации, 51
маршрутизируемый, 119
преобразования адресов, 64
приветствия, 64
распределенных сетей, 51
сетевой, 51
Протокол маршрутизации, 119
Процессор
коммуникационный, 639
Процессор, многопортовый, 303
Прошитый адрес, 63
Прямая видимость, 357
Псевдослучайный шумоподобный код,
338
Пункт коммутации пакетов, 253

P

Рабочая станция, 639
Радиочастота, 358
Разреженно-плотный режим PIM, 715
Разреженный режим PIM, 715
Разрешенные модули, 560
Распределение нагрузки, 116
Распределенная сеть, 48; 81
Распределитель
здания, 164
кампуса, 164
этажный, 164
Расширенная сеть AppleTalk, 616
Расширенный адрес, 193
Расширитель локальной сети, 78
Расщепление
горизонтов, 699
Режим
PIM
плотный, 714
разреженно-плотный, 715
разреженный, 715
доступа, 503
магистральный, 503
Резервирование, 766
явное совместное, 767
Резервный телефонный канал, 85
Родительский адрес, 777
Родительский порт, 778
Родительский узел, 778

C

Мультиплексирование, 69; 232
Сбор адресов, 623
Сборщик/разборщик пакетов, 254
Сверхскоростной цифровой
абонентский канал, 371
Связное дерево, 777
многоадресное, 710
Связующее дерево, 480
Связывание
имен, 626
Сеанс
X.25, 255
Сеансовый соединитель, 685
Сеансовый уровень, 57; 574; 659
Сегмент, 59
Сервер
доступа, 85; 230
многопротокольный, 533
переадресации, 309
размещения, 309
регистратор, 309
Сетевая архитектура
открытая, 882
Сетевое кэширование, 833
прозрачное, 838
совместное, 837
Сетевой адаптер
многоскоростной, 162
Сетевой адрес, 56; 64; 65
Сетевой интерфейс абонента, 217; 220;
225
Сетевой каталог, 807
Сетевой коммутатор, 161
Сетевой кэш
интегрированный, 835
Сетевой модуль
адресуемый, 641

Сетевой протокол, 51
Сетевой терминатор, 203
Сетевой узел, 643
Сетевой уровень, 56; 59; 570
Сеть
AppleTalk, 615
нерасширенная, 615
расширенная, 616
ATM, 511
абонентская, 341
беспроводная
фиксированная, 356
доступа, 341
локальная, 47; 73
объединенная, 47
глобальная, 722
открытая, 191
Распределенная, 48; 81
с коммутацией пакетов, 187
с передачей маркера, 75
соединений APPN, 693
центральная, 342
частная, 192
Сигнал, 307
аналоговый, 354
Сигнал/шум, 335
Симметричный коммутатор локальной сети, 505
Симметричный цифровой абонентский канал, 368
Синтаксис
атрибута, 814
Синхронизация
трехэтапная, 590
Система
конечная, 739
многоточечная, 358
мобильная
беспроводная, 357
промежуточная, 739
внешняя, 752
телевизионная кабельная, 375
управления
сетями IBM, 879
управления сетью, 124; 342; 892
Скалярный объект, 894
Скользящее окно, 591
Скоростная маршрутизация, 691
Скорость
развития, 388
Служба
каталогов, 577; 812; 815
APPN, 644
конфигурации APPN, 643
представлений, 638
распределения
многоканальная
многоабонентская, 357
распределения, местная
многоабонентская, 357
сеансов, 646
топологии и маршрутизации APPN, 645
транзакций, 638
Служба, ориентированная на соединение, 61
Смежная конечная точка, 778
Смежность, 723
Смежный канал, 354
Смежный узел, 778; 781
Событие, 307
Совместное резервирование
явное, 767
Совместное сетевое кэширование, 837
Содержательный трафик, 240
Соединение, 306
ATM, 521
коммутируемое, 229
мостовое
прозрачное, 103
с маршрутизацией на источнике, 103
с маршрутизацией на источнике, 103
с трансляцией, 489
трансляционное, 103
Соединитель
сеансовый, 685
Соединительный кабель, 996
Сокет
AppleTalk, 614
Сообщение, 59
конфигурационное, 483
об изменении топологии, 483
снижающее скорость передачи данных, 67

Соседний узел, 778
Состояние
гибкое, 768
Спектр
электромагнитный, 356
Спецификация
потока, 764
CP, Control Point, 641
Станция
двухпортовая, 174
конечная, 124
однопортовая, 174
рабочая, 639
Статистическое мультиплексирование, 69
Статическая маршрутизация, 116
Статический адрес, 66; 705
Стиль
групповой фильтрации, 766
резервирования, 766
явное совместное, 767
фиксированной фильтрации, 767
Супервизорный фрейм, 257
Схема, 807
контроля ошибок, 68
многопротокольная, 532
Сходимость, 115

T

Таблица
маршрутизации, 118
соответствия адресов, 622
топологическая, 680
Табличный объект, 894
Таймер
исключения, 700
недействующих маршрутов, 700
обновлений, 700
обновления маршрутов, 758
ожидания, 758
смещения маршрута, 758
Тегирование, 142
Телевизионная кабельная система, 375
Терминал, 303; 639
Терминальное оборудование, 132; 186; 195; 253
Терминальное оборудование, 203
Терминатор
сетевой, 203
Территория обслуживания
базовая, 355
Топологическая таблица, 680
Топология
древовидная, 77
звездообразная, 77; 133
кольцевая, 76
шинная, 76
Точка
входа, 882
доступа к службе, 53; 882
конечная, 306; 511; 778
дочерняя, 778
исходная, 778
смежная, 778
член группы, 778
контрольная, 641
рандеву, 716
альтернативная, 717
сбора, 882
фокусная, 882
Трансляционное мостовое соединение, 103
Трансмиссионная группа, 645
Транспортный уровень, 57; 573; 656
Трафик
гарантированной доставки, 764
гарантированной скорости, 764
содержательный, 240
Трафик гарантированной задержки, 765
Трейлер, 53; 58
Трехэтапная синхронизация, 590
Туннелирование
RSVP, 769
Туннель, 778
Туннельный узел, 781

У

Удаленные мосты, 105; 951
Удаленный мониторинг, 887
Удостоверяющая сторона, 237
Узел, 639; 778
AppleTalk, 615
SNA, 641

вторичный, 246; 778
граничный, 693
дочерний, 778
исходный, 778
конечный, 643
назначенный, 778; 781
низкоуровневый, 643
первичный, 245; 778
промежуточный, 132
родительский, 778
сетевой, 643
смежный, 778; 781
соседний, 778
туннельный, 781
член группы, 778
Управление
безопасностью, 127; 952
доступом к среде передачи, 56
каналом, 638; 639
конфигурацией, 125; 127; 952
логическим каналом, 56; 106
маршрутом, 638
отказоустойчивостью, 126; 127; 952
передачей, 638
потоком, 140; 558; 638
производительностью, 124; 127; 952
сетевое, 123
учетными записями, 126; 127; 952
Управление потоком, 67
Управление сетью, 123; 342
Управляемое устройство, 124; 892
Управляющая информация, 53
Управляющий модуль
многопортовый, 303
Управляющий элемент, 124
Упреждающая коррекция ошибок, 335
Уровень
ATM, 515
адаптационный, 515; 516
канальный, 55; 58; 62; 104; 569
пользователя, 657
представлений, 574; 659
представления, 57
приложений, 58; 575; 658
сеансовый, 57; 574; 659
сетевой, 56; 59; 570
сетевых приложений, 658
транспортный, 57; 573; 656
управления сеансом, 658
управления сетью, 657
физический, 55; 515; 569
Ethernet, 143; 145
Уровень обслуживания, 914
Устройство
управляемое, 124; 892

Ф

Фазовая модуляция, 334
двоичная, 334
Физический адрес, 62; 104
Физический модуль, 641
Физический уровень, 55; 515; 569
Ethernet, 143; 145
Фиксированная беспроводная сеть, 356
Фиксированная фильтрация, 767
Фильтр обратной связи, 337
Фильтрация, 480
групповая, 766
фиксированная, 767
Фокусная точка, 882
Формат
DDP-пакета, 632
IP-пакета, 580
TCP-пакета, 592
пакета IPX, 610
пакета OSPF, 734
пакета RSVP, 772
пакета SMRP, 785
Формат фрейма
Ethernet, 136
FDDI, 178
Frame Relay, 193
LAPB, 258
LMI, 194
SDLC, 246
Формирование трафика, 523; 913
Фрейм, 58
информационный, 257
ненумерованный, 257
супервизорный, 257
формат Ethernet, 136
формат FDDI, 178
формат Frame Relay, 193
формат LAPB, 258
формат LMI, 194

формат SDLC, 246
Фрейм-пауза, 141

X

X.21bis, 258
X.25, 253

Ц

Центральная сеть, 342
Цифровой абонентский канал, 361
ISDN, 370
асимметричный, 361
сверхскоростной, 371
симметричный, 368

Ч

Частная сеть, 192
Частота
ошибок по битам, 335
Частотное уплотнение, 339

Ш

Шинная топология, 76
Широковещательная передача, 76; 355; 599
Широковещательный адрес, 137
Широковещательный домен, 502
Широкополосная модуляция, 337
методом прямой последовательности, 338
Широкополосная модуляция методом частотных скачков, 339
Широкополосная передача, 355
Шлюз, 303; 588
среды передачи, 305
Шум
комфортный, 297

Э

Экранированная витая пара, 132
Электромагнитный спектр, 356
Элемент
пользователя, 575
управляющий, 124
Эмиттерно-связанная логика, 200
Эмуляция LAN, 526
Этажный распределитель, 164
Эталонная модель
OSI, 49
Эталонная модель ATM, 515
Эффективная мощность изотропного излучателя, 356

Я

Явное совместное резервирование, 767
Явный маршрут, 686
Ячейка, 59; 510

Научно-популярное издание

Cisco Systems, Inc.

Руководство по технологиям объединенных сетей
4-е издание

Литературный редактор	*С.Г. Татаренко*
Верстка	*О.В. Линник*
Художественный редактор	*В.Г. Павлютин*
Корректоры	*З.В. Александрова, Л.А. Гордиенко, Л.В. Чернокозинская*

Издательский дом "Вильямс".
101509, Москва, ул. Лесная, д. 43, стр. 1.

Подписано в печать 17.03.2005. Формат 70×100/16.
Гарнитура Times. Печать офсетная.
Усл. печ. л. 65,0. Уч.-изд. л. 62,4.
Тираж 3000 экз. Заказ № 1107.

Отпечатано с диапозитивов в ФГУП "Печатный двор"
Министерства РФ по делам печати,
телерадиовещания и средств массовых коммуникаций.
197110, Санкт-Петербург, Чкаловский пр., 15.

Руководство по технологиям объединенных сетей

4-е издание

Настольный справочник специалиста по сетевым технологиям