Александр Филимонов

ПОСТРОЕНИЕ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ ETHERNET

Санкт-Петербург
«БХВ-Петербург»
2007

УДК 681.3.06
ББК 32.973.26
Ф53

Филимоиов А. Ю.

Ф53 Построение мультисервисных сетей Ethernet. — СПб.: БХВ-Петербург, 2007. — 592 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0007-4

Рассматривается применение технологии Ethernet для построения мультисервисных сетей нового поколения (Next Generation Network — NGN), используемых для объединиения телефонного и телевизионного сигналов в едином канале. Изложены базовые принципы построения локальных и магистральных сегментов NGN. Большое внимание уделяется описанию усовершенствованной технологии Ethernet (IEEE 802.3). Подробно рассматриваются современные протоколы Интернета и технические решения, обеспечивающие повышение надежности, эффективности и безопасности мультисервисных ЛВС. Приведены практические примеры использования программного обеспечения и оборудования известных производителей (Cisco Systems, 3COM, D-Link и Allied Telesyn).

Для системных администраторов, студентов и сотрудников IT-подразделений

УДК 681.3.06
ББК 32.973.26

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Григорий Добин*
Редактор	*Юрий Рожко*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Елены Беляевой*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 02.04.07.
Формат 70×100$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 47,73.
Тираж 2000 экз. Заказ № 1150
"БХВ-Петербург", 194354, Санкт-Петербург, ул. Есенина, 5Б.

Санитарно-эпидемиологическое заключение на продукцию
№ 77.99.02.953.Д.006421.11.04 от 11.11.2004 г. выдано Федеральной службой по надзору в сфере защиты прав потребителей и благополучия человека.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 978-5-9775-0007-4

© Филимоиов А. Ю., 2007
© Оформление, издательство "БХВ-Петербург", 2007

Оглавление

Введение 1

Структура книги 3
Использованные обозначения 6

ЧАСТЬ I. ЗАДАЧИ И СПОСОБЫ ПОСТРОЕНИЯ СОВРЕМЕННЫХ МСС 9

Глава 1. Способы построения МСС 11

Традиционные мультисервисные сети 11
Цифровые сети ISDN с интеграцией услуг 12
Типы услуг сети ISDN 12
Принципы построения и компоненты сетей ISDN 14
Магистраль подключения абонентов ISDN 14
Взаимодействие абонентов с сетью ISDN 16
Технология Frame Relay 19
Особенности построения сетей Frame Relay 19
Структура кадра Frame Relay 21
Параметры качества обслуживания Frame Relay 23
Спецификация LMI 23
Технология ATM и ее использование в мультисервисных сетях 24
Компоненты сетей ATM 25
Формат ячейки ATM 27
Интеграция трафика в сети ATM 28
Современные принципы создания МСС 30
Гибридные сети широкополосного доступа 31
Передача данных по сетям HFC 31
Спецификации DOCSIS 33
Универсальный шлюз DOCSIS 37
Сети беспроводного доступа 39
Спецификации IEEE 802.11 (Wi-Fi) 39
Спецификации IEEE 802.16 WiMAX 41
Интеграция разнородного трафика в сетях WiMAX 42

Мультисервисные ЛВС на основе Ethernet-технологий 44
Применение волоконно-оптических линий связи в сетях доступа 45
Пассивные оптические сети — PON 46
Спецификация EPON 48

Глава 2. Голосовые приложения мультисервисных сетей 52

Способы преобразования голосового сигнала 52
Принципы построения кодирующих устройств 53
Особенности голосового сигнала 53
Компенсация шума квантования 55
Типы и характеристики кодирующих систем 57
Голосовые кодеки PCM (G.711 и G.726) 57
Голосовые кодеки CELP (G.723.1, G.728 и G.729) 58
Передача голоса по пакетным сетям 61
Преимущества пакетной телефонии 61
Особенности пакетного преобразования голоса 62
Требования голосовых приложений к параметрам MCC 64
Архитектура и компоненты систем VoIP 64
Системы традиционной и пакетной телефонии 64
Традиционные и гибридные телефонные системы 65
Распределенные системы пакетной телефонии 68
Иерархические системы пакетной телефонии 70
Компоненты систем пакетной телефонии 72
Универсальные и абонентские шлюзы VoIP 72
Аппаратные и программные IP-телефоны 73
Приложения пакетной телефонии 74
Универсальные карточные системы 74
Центры обработки вызовов 77

Глава 3. Коммерческие и технологические видеоприложения мультисервисных сетей 79

Способы формирования и кодирования видеосигнала 79
Системы аналогового телевидения 80
Принципы формирования телевизионного изображения 80
Системы цветного телевидения 81
Форматы видеоизображения 83
Типы и характеристики кодирующих систем 85
Кодирование видеопотоков с использованием рекомендации H.261 86
Особенности кодирования согласно рекомендации H.263 89
Применение MPEG-1 для кодирования мультимедийных объектов 91
Основные принципы кодирования MPEG-2 92
Спецификация MPEG-4 96
Оценки эффективности и качества сжатия видеоизображений 102
Идентификация и защита цифровых продуктов MPEG 103
Спецификация MPEG-7 104
Спецификация MPEG-21 105

Видеоприложения современных мультисервисных сетей ... 107
Коммерческие видеоприложения ... 107
Форматы цифрового телевизионного вещания ... 108
Интерактивные видеосервисы VOD ... 110
Способы доставки цифрового телевизионного сигнала ... 111
Системы IPTV ... 113
Некоммерческие видеоприложения ... 115
Системы видеонаблюдения ... 116
Системы проведения видеоконференций ... 117

Глава 4. Организация обмена в мультисервисных сетях ... 119

Распределенные системы управления ... 120
Принципы организации и компоненты сетей H.323 ... 120
Терминальные устройства H.323 ... 122
Основные функции шлюза H.323 ... 123
Задачи привратника в сети H.323 ... 124
Управляющие сообщения H.323 ... 125
Управление доступом H.225 (RAS) ... 126
Управление вызовом H.225 (Q.931) ... 130
Управление логическими каналами H.245 ... 132
Протокол SIP ... 134
Компоненты SIP ... 135
Сообщения SIP ... 136
Организация информационного обмена SIP ... 140
Иерархические и гибридные системы управления ... 141
Системы управления MEGACO/MGCP ... 141
Протокол MEGACO ... 142
Протокол MGCP ... 143
Перспективные системы управления мультисервисным обменом ... 145
Недостатки систем управления второго поколения ... 145
Направления дальнейшего развития ... 146

Глава 5. Особенности построении современных МСС ... 147

Общие принципы построения мультисервисных сетей ... 148
Надежность и безопасность информационного обмена ... 149
Устойчивость к отказам компонентов МСС ... 149
Взаимная изоляция компоиентов мультимедийного трафика ... 153
Передача в едином канале разнородного трафика ... 153
Требования современных приложений к параметрам МСС ... 154
Реализация видеоприложений в мультисервисной ЛВС ... 155
Требования голосовых приложений к параметрам МСС ... 156
Особенности построения мультисервисных ЛВС ... 158
Реализация потокового обмена в пакетных МСС ... 159
Передача потоков данных в сетях с коммутацией пакетов ... 159
Принципы построения протокола RTP ... 160

Назначение протокола RTCP ... 164
Формат сообщений протокола RTP ... 165
Типы сообщений протокола RTCP ... 168
Режим многоадресного обмена ... 169
Реализация специальных требований потоковых приложений ... 170
Протокол STCP управления передачей потоков ... 170
Передача факсимильных сообщений по сети IP ... 172

ЧАСТЬ II. ТЕХНОЛОГИИ ПОСТРОЕНИЯ МУЛЬТИСЕРВИСНЫХ ЛВС ... 175

Глава 6. Управление потоками данных в ЛВС ... 177

Принципы информационного обмена в ЛВС ... 178
Уровни взаимодействия ... 178
Термины и определения ... 179
Протоколы современных ЛВС ... 181
Протокол канального уровня Ethernet ... 182
Протокол сетевого уровня IP ... 186
Транспортный протокол UDP ... 189
Транспортный протокол TCP ... 190
Структура информационных потоков ЛВС ... 194
Принципы построения и компоненты сегментированных ЛВС ... 196
Типы сегментов ЛВС ... 197
Физический сегмент ЛВС ... 198
Канальный сегмент ЛВС ... 199
Сетевой сегмент ЛВС ... 199
Основные функции коммутатора Ethernet ... 200
Формирование таблицы фильтрации ... 200
Обработка принимаемых кадров ... 200
Способы построения коммутаторов ... 202
Основные и вспомогательные функции маршрутизатора ... 204
Построение маршрута передачи пакетов ... 205
Взаимодействие абонентов различных VLAN ... 206
Вспомогательные функции маршрутизаторов ... 206
Задачи и способы многоуровневой коммутации ... 207
Методы аппаратной реализации функций маршрутизатора ... 208
Базовые принципы многоуровневой коммутации ... 210

Глава 7. Обеспечение безопасного подключения абонентов ... 211

Виртуальные сети ... 212
Принципы построения виртуальных сетей ... 212
Преимущества использования VLAN в МСС ... 215
Повышение производительности ЛВС ... 215
Создание виртуальных рабочих групп ... 216
Снижение затрат на эксплуатацию ... 217

Распределенные виртуальные сети ... 217
Технология маркирования ISL ... 219
Технология IEEE 802.1Q ... 220
Типы портов VLAN ... 222
Туннели IEEE 802.1Q ... 223
Управление виртуальными сетями ... 224
Протокол GARP ... 226
Динамические VLAN. Протокол GVRP ... 227
Протокол VTP Cisco Systems ... 229
Управление доступом абонентов к ресурсам МСС ... 232
Протокол PPP ... 234
Служебные протоколы PPP ... 235
Использование протокола PPP для управления абонентом ... 239
Протокол PPPoE ... 241
Основные принципы PPPoE ... 241
Особенности применения PPPoE в мультисервисных сетях ... 243
Протоколы L2TP и PPTP ... 247
Протокол PPTP ... 247
Протокол L2TP ... 250
Применение туннельных протоколов в мультисервисных сетях ... 252
Протокол IEEE 802.1X ... 253
Основные компоненты IEEE 802.1X ... 254
Сообщения протокола IEEE 802.1X ... 255
Особенности применения протокола IEEE 802.1X ... 256
Управление доступом групп абонентов ... 256
Асимметричные VLAN ... 257
Списки управления доступом ... 261
Функция Port Security ... 263

Глава 8. Повышение надежности магистралей мультисервисных ЛВС ... 266

Алгоритм Spanning Tree ... 267
Возникновение "шторма" в ЛВС с кольцевой топологией ... 267
Применение альтернативных маршрутов в сети прозрачных мостов ... 269
Основные принципы алгоритма Spanning Tree ... 270
Назначение корневого моста ... 272
Определение корневого и назначенных портов ... 275
Практическая реализация алгоритма Spanning Tree ... 278
Формирование сообщений Spanning Tree ... 279
Построение активной топологии ... 282
Состояния и режимы портов Spanning Tree ... 285
Изменение активной топологии Spanning Tree ... 288
Быстрый алгоритм Spanning Tree IEEE 802.1W ... 291
Основные принципы RSTP ... 292
Формирование сообщений RSTP ... 292
Значения параметров протокола RSTP ... 293

Построение активной топологии RSTP ... 295
Состояния портов моста RSTP ... 296
Режимы портов моста RSTP ... 297
Согласование активной топологии ... 297
Изменение активной топологии RSTP ... 299
Многоплановые протоколы Spanning Tree ... 300
Многоплановые протоколы STP Cisco Systems ... 301
Протокол PVST ... 302
Протокол PVST+ ... 302
Протокол MSTP (IEEE 802.1Q) ... 303
Основные понятия и определения MSTP ... 303
Принципы реализации MSTP ... 306
Структура сообщений протокола MSTP ... 308
Примеры использования Spanning Tree при построении мультисервисных ЛВС ... 312

Глава 9. Выравнивание загрузки резервироваиных узлов мультисервисных ЛВС ... 314

Динамическое резервирование компонентов ЛВС ... 315
Протокол динамического резервирования HSRP ... 316
Особенности резервирования маршрутизаторов ЛВС ... 316
Принципы реалнзации протокола HSRP ... 317
Основные параметры протокола HSRP ... 319
Формат и типы сообщений HSRP ... 322
Особенности применения протокола HSRP ... 323
Протокол VRRP ... 324
Компоненты протокола VRRP ... 324
Структура сообщений VRRP ... 325
Особенности применення протокола VRRP ... 327
Использование протокола динамического резервирования ... 327
Протоколы распределения нагрузки между компонентами ЛВС ... 330
Протокол GLBP ... 331
Назначение протокола GLBP ... 332
Организация взаимодействия компонентов GLBP ... 333
Способы выравнивания нагрузки ... 334
Особенности применения протокола GLBP в мультисервисных ЛВС ... 335
Протокол CARP ... 335
Основные особенности протокола CARP ... 336
Область применения протокола CARP ... 337
Альтернативные способы распределения нагрузки ... 337
Серверные кластеры ... 338
Стеки многоуровневых коммутаторов ... 339

Глава 10. Увеличение пропускной способности каиалов ЛВС ... 340

Применение агрегированных каналов в мультисервисных ЛВС ... 341
Агрегирование магистральных каналов коммутаторов ... 342
Принципы построения агрегированных интерфейсов ... 342

Ускорение процедуры распределения кадров ... 343
Особенности агрегирования каналов IEEE 802.3 ... 344
Управление агрегированным каналом ... 345
Создание и удаление агрегированного канала на коммутаторе ... 345
Добавление дополнительного интерфейса к агрегированному каналу ... 346
Удаление интерфейса из агрегированного канала ... 346
Распределение трафика в объединенном канале ... 347
Использование признаков канального уровня ... 347
Использование признаков сетевого уровня ... 348
Комбинирование признаков ... 349
Протокол LACP IEEE 802.3AD ... 350
Принципы реализации протокола LACP ... 351
Компоненты протокола LACP ... 351
Структура блока данных LACP ... 353
Принципы взаимодействия партнеров LACP ... 357
Рекомендации по созданию и использованию объединенных каналов мультисервисных ЛВС ... 359
Применение протокола STP в ЛВС с агрегированными каналами ... 360
Передача группового трафика по агрегированным каналам ... 361
Примеры построения агрегированных каналов ... 362

Глава 11. Организация группового вещания в мультисервисных ЛВС ... 364

Особенности режима группового обмена ... 365
Групповые адреса TCP/IP ... 367
Локальные групповые адреса ... 368
Глобальные Multicast-адреса TCP/IP ... 368
Принципы организации группового обмена ... 370
Особенности формирования группового адреса ... 370
Определение состава группы ... 370
Организация доставки группового трафика ... 371
Групповое взаимодействие на канальном уровне ... 372
Протокол IGMP ... 372
Формат сообщения IGMP ... 373
Дополнительные функции протокола IGMP ... 377
Практическая реализация протокола IGMP в современных сетях ... 377
Прослушивание сообщений IGMP коммутаторами ЛВС ... 378
Групповое взаимодействие на сетевом уровне ... 380
Способы доставки группового трафика ... 381
Доставка группового трафика в режиме DENSE ... 381
Доставка группового трафика в режиме SPARSE ... 382
Применение процедуры RPF ... 382
Протокол групповой маршрутизации PIM ... 383
Использование протокола PIM в режиме DENSE ... 383
Применение протокола PIM в режиме SPARSE ... 384

Глава 12. Управление трафиком приложений мультисервисных ЛВС....387

Элементы систем управления трафиком....388
Планирование трафика приложений....389
Модели управления клиентским трафиком....390
Объединенное управление трафиком (IntServ)....392
Протокол RSVP....392
Механизмы управления трафиком протокола RSVP....392
Формы и методы резервирования ресурсов....394
Сообщения протокола RSVP....397
Формат сообщений протокола RSVP....399
Распределенное управление трафиком (DiffServ)....401
Способы разделения трафика приложений....402
Классификация по признакам канального уровня....403
Классификация по признакам сетевого уровня....403
Основные принципы маркирования трафика мультисервисных ЛВС....406
Реализация классификации в ЛВС....409
Методы и способы нормирования трафика приложений....410
Алгоритм Leaky Bucket....410
Административное ограничение клиентского трафика....411
Регулирование параметров клиентского трафика....413
Управление нормированием абонентского трафика....416
Рекомендации по управлению трафиком приложений....417
Управление трафиком в чрезвычайных ситуациях....417
Предотвращение перегрузок на порту коммутатора....418
Предотвращение широковещательных штормов....419

ЧАСТЬ III. СТРУКТУРА И КОМПОНЕНТЫ МУЛЬТИСЕРВИСНЫХ ЛВС....421

Глава 13. Способы и схемы построения мультисервисных ЛВС....423

Типы и разновидности топологий ЛВС....424
Шинная топология ЛВС....424
Принципы построения ЛВС шинной топологии....425
Особенности ЛВС с разделяемой средой передачи данных....426
Иерархические структуры ЛВС....426
Задачи, решаемые на уровне доступа....427
Функции, выполняемые на уровне распределения....430
Назначение активного оборудования ядра ЛВС....432
Применение иерархических технологий при построении мультисервисных ЛВС....433
Кольцевые топологии ЛВС....434
Технологии Token Ring/IEEE 802.5....435
Технология FDDI....439
Магистральные технологии второго поколения....444
Использование гибридных технологий для построения мультисервисных ЛВС...450

Глава 14. Построение магистральных соединений мультисервисных ЛВС ... 452

Технологии Gigabit Ethernet ... 453
Спецификации 1000Base X ... 454
Особенности организации информационного обмена 1000Base X ... 454
Контроль паритета передаваемого кода ... 457
Оптические вариаиты PMD 1000Base X ... 459
Протокол физического уровня 1000Base CX ... 462
Спецификация 1000Base T ... 463
Принципы организации информационного обмена 1000Base T ... 463
Особенности практической реализации 1000Base T ... 465
Технологии построения магистралей 10Gigabit Ethernet ... 468
Параллельные магистрали 10GBase-X ... 469
Организация информационного обмена 10GBase-X ... 469
Оптические WDM-магистрали 10GBase-LX4 ... 471
Параллельная магистраль 10GBase-CX4 ... 473
Последовательные магистрали 10Gigabit Ethernet ... 473
Организация информационного обмена 10GBase-R ... 474
Специфика построения магистральных соединений 10GBase-W ... 475
Характеристики последовательных магистралей 10Gigabit Ethernet ... 476
Применение модульных трансиверов в магистралях ЛВС ... 477

Глава 15. Организация подключения абонентов к оборудованию мультисервисных ЛВС ... 480

Контроль и согласование параметров линии ... 481
Процедура проверки целостности линии ... 481
Автоматическое согласование параметров обмена ... 482
Основные принципы автоматического согласования параметров ... 483
Сообщения Auto-Negotiation ... 486
Особенности организации процесса согласования ... 488
Критерии выбора технологии ... 492
Управление потоком данных в сегменте Ethernet ... 492
Формат кадра управления потоком ... 493
Режимы использования процедуры управления потоком ... 494
Электропитание абонентов мультисервисных ЛВС ... 495
Протокол PoE ... 496
Особенности электропитания абонентов мультисервисных ЛВС ... 496
Основные принципы PoE ... 497
Реализация протокола PoE ... 498
Протокол PoEP ... 501
Обеспечение совместимости с PoE ... 501
Планируемые характеристики PoEP ... 502
Особенности организации электропитания абонентов мультисервисных ЛВС ... 503
Особенности конфигурации активного оборудования PoE ... 503

Глава 16. Программные компоненты мультисервисных ЛВС 505
Технологическое программное обеспечение 505
Контроль состояния и управление компонентами мультисервисных ЛВС 506
Протокол SNMP 507
Принципы построения системы управления сетью SNMP 508
Идентификация объектов MIB 509
Описание управляемых объектов MIB 511
Взаимодействие компонентов SNMP 514
Мониторинг состояния сети 516
Анализ и документирование трафика мультисервисной ЛВС 520
Технология NetFlow 521
Особенности применения NetFlow 522
Принципы и программное обеспечение тарификации абонентов 525
Функциональное программное обеспечение 527
Клиентские приложения VoIP 528
Назначение и состав программного call-центра 528
Виртуальная телефонная станция 529
Программный IP-телефон 531
Вспомогательные программы систем пакетной телефонии 532
Серверные и клиентские видеоприложения 535
Протокол анонсирования потоков — протокол SAP 536
Формирователь мультимедийных потоков VLC 538
Программный мультимедийный плеер VLC 539
Рекомендации по использованию программных компонентов 540

Перечень сокращений 541

Предметный указатель 564

Введение

Предметом книги является рассмотрение основных принципов и способов построения локальных и магистральных сегментов современных мультисервисных сетей — сетей нового поколения — *NGN* (Next Generation Network). Принято полагать, что назначение мультисервисной сети (МСС) состоит в интеграции телефонного и телевизионного сигналов в едином канале передачи данных, и именно поэтому такие сети также называют сетями тройного применения — *3Play* (Triple-Play). В более широком, современном понимании мультисервисная сеть представляет собой интегральную телекоммуникационную инфраструктуру, которая имеет достаточно ресурсов для того, чтобы обеспечить все формы информационного обмена, выполняемого в интересах поставщика или потребителя разнообразных услуг.

Исторически телекоммуникации развивались в трех независимых направлениях, что привело к возникновению специализированных инфраструктур, каждая из которых была предназначена для решения ограниченного комплекса задач.

- *Телефонные сети общего назначения.*

  Они обеспечивают прямое двухстороннее общение удаленных абонентов и передачу факсимильных сообщений. Дополнительные услуги, реализуемые в телефонных сетях общего назначения, позволяли организовать многосторонние телефонные конференции и разнообразные формы обработки и переадресации входящих телефонных вызовов.

- *Сети эфирного и кабельного телевидения.*

  Основное назначение таких сетей состоит в обеспечении вещания и приема государственных и коммерческих телевизионных информационных каналов и видеопрограмм.

- *Сети передачи данных и доступа к информационным ресурсам общего пользования (Интернет).*

В этих сетях обеспечивались прием и передача файлов, оперативный обмен текстовыми сообщениями и сообщениями электронной почты.

Наследование и дальнейшее развитие удачных решений являются неотъемлемыми чертами процесса развития телекоммуникационных технологий, как, впрочем, и любого другого эволюционного процесса. Черты нового постепенно накапливаются в существующих технологических комплексах, после чего происходят их качественные изменения или возникают новые технологии. К факторам, стимулирующим ускорение этих процессов в сфере телекоммуникаций, можно отнести появление новых требований или сфер применения, которые сами, в свою очередь, непосредственно связаны с развитием технологий.

Процесс конвергенции телекоммуникационных инфраструктур, представляющий собой взаимное проникновение сетей различного назначения путем использования единых компонентов и совмещения выполняемых функций, уже имеет достаточно богатую историю. Этот процесс одновременно развивался в нескольких направлениях. С одной стороны, активно разрабатывались технологии, способные обеспечить эффективную интеграцию разнородного трафика в единой телекоммуникационной инфраструктуре. Ярким примером подобных технологий можно считать технологии *ISDN* (Integrated Services Digital Network), *ATM* (Asynchronous Transfer Mode) и, с некоторыми ограничениями, *Frame Relay*. С другой стороны, технические средства и ресурсы в каждой из независимых сетей начинали все более активно использоваться для доступа к ресурсам или получения услуг другой сети. Коммутируемые каналы стационарных телефонных сетей, например, еще в конце прошлого века широко использовались для организации информационного обмена и доступа к ресурсам сетей общего пользования. Так же успешно для этих целей сети могут быть использованы и современные мобильные телефонные сети.

Современный этап развития телекоммуникационных технологий характеризуется взрывным ускорением процессов взаимной конвергенции, которые проходят в каждой из отмеченных ранее специализированных инфраструктур. В первую очередь это объясняется расширением номенклатуры и логическим развитием предоставляемых и принимаемых услуг; а также резким увеличением возможностей абонентских терминалов, которые используются для подключения к сети. Границы, еще недавно казавшиеся незыблемыми, размываются, и на смену прежним специализированным сетям с ограниченными функциями приходят новые гибридные мультисервисные инфраструктуры, со значительно более широким перечнем предоставляемых услуг.

По мнению автора, пока еще нет однозначного ответа на вопрос о том, какая из коммуникационных инфраструктур должна быть положена в основу еди-

ной мультисервисной сети, да и целесообразность постановки такого вопроса также не кажется бесспорной. В большинстве случаев мультисервисные структуры строятся на основе и с использованием компонентов уже существующих сетей, путем внедрения новых технологий и способов организации информационного обмена. В то же время нельзя не отметить, что сегодня достаточно отчетливо обозначается тенденция преобладания технологий пакетной коммутации (Ethernet, Интернет) для организации информационного обмена в мультисервисных сетях. В последние несколько лет эти технологии особенно бурно развиваются, причем значительная часть последних усовершенствований направлена именно на повышение эффективности применения классических технологий пакетной коммутации при построении мультисервисных сетей. Высокие эксплуатационные характеристики, повсеместное распространение и низкая стоимость компонентов — именно эти характеристики дают все основания полагать, что технологии пакетной коммутации будут и впредь занимать достойное место в мультисервисных системах.

Структура книги

Весь материал книги можно условно разделить на три части:

- Вступительная часть I, в которую входят главы с 1 по 5;
- Основная часть II, которая включает в себя главы с 6 по 12;
- Заключительная часть III — главы с 13 по 16.

Каждая из глав, в свою очередь, содержит два или более тематических разделов. Как правило, в начале главы помещается небольшое вступление, в котором излагаются основные тезисы или кратко освещается тематика этой главы.

Первая, вступительная, часть книги посвящена основополагающим принципам построения мультисервисных сетей.

В *главе 1 "Способы построения МСС"* рассматриваются технологические идеи, которые были положены в основу классических мультисервисных сетей — ISDN, Frame Relay и ATM. Заключительная часть главы посвящена рассмотрению альтернативных технологий, которые используются для построения современных мультисервисных сетей — *DOCSIS* (Data-Over-Cable Service Interface Specifications), *WiMAX* (Worldwide Interoperability for Microwave Access) и *EPON* (Ethernet over Passive Optical Networks).

Глава 2 "Голосовые приложения мультисервисных сетей" посвящена рассмотрению способов реализации и компонентов современных сетей пакетной телефонии. Рассмотрены принципы и способы преобразования голосового сигнала, которые обеспечивают передачу телефонного трафика по сети с коммутацией пакетов *VoIP* (Voice over IP).

Глава 3 "Коммерческие и технологические видеоприложения мультисервисных сетей" дает представление о базовых принципах формирования и основных алгоритмах кодирования видеосигнала классических и современных телевизионных систем и особенности реализации приложений *IPTV* (Internet Protocol Television) в современных мультисервисных сетях.

В *главе 4 "Организация обмена в мультисервисных сетях"* представлены различные подходы, которые могут быть использованы для управления информационным взаимодействием в мультисервисных сетях. В этой главе на примере комплекса протоколов H.323 и SIP (Session Initiation Protocol) рассмотрены принципы построения распределенных систем управления и возможные направления дальнейшего развития технологий управления вызовами в МСС.

Значительная часть *главы 5 "Особенности построения современных МСС"* посвящена рассмотрению различных вариантов структурного построения мультисервисных систем. В этой главе рассматриваются также особенности реализации информационных подсистем МСС с применением комплекса технологий пакетной коммутации Ethernet — Интернет и, в частности, использование протоколов *RTP* (Real-Time Transport Protocol) и *STCP* (Stream Control Transmission Protocol) для передачи потокового трафика в пакетных сетях.

Вторая часть книги содержит материалы по общим вопросам построения сегментов мультисервисных сетей с использованием перспективных технологий пакетной коммутации.

В *главе 6 "Управление потоками данных в ЛВС"* рассматриваются основные компоненты и принципы организации информационного обмена, применяемые в современных ЛВС. В этой главе приведены также определения и краткие описания терминов и понятий, которые используются во второй части книги.

Глава 7 "Обеспечение безопасного подключения абонентов" содержит описание способов логического сегментирования вычислительной сети путем построения виртуальных сетей — *VLAN* (Virtual Local Area Network) для достижения эффективной изоляции трафика различных приложений. Подробно рассмотрены разнообразные способы управления доступом групп абонентов к сетевым ресурсам МСС.

Глава 8 "Повышение надежности магистралей мультисервисных ЛВС" посвящена вопросам динамического резервирования компонентов ЛВС с использованием расширенных модификаций протокола Spanning Tree — *RSTP* (Rapid Spanning Tree Protocol) и *MSTP* (Multiple Spanning Tree Protocol).

Глава 9 "Выравнивание загрузки резервированных узлов мультисервисных ЛВС" представляет собой логическое продолжение предыдущей, поскольку в этой главе рассматриваются способы и протоколы автоматического перерас-

пределения нагрузки (Load Balancing) между основным и резервными компонентами ЛВС.

В *главе 10 "Увеличение пропускной способности каналов ЛВС"* рассматриваются алгоритмы и способы повышения пропускной способности соединений ЛВС путем объединения нескольких параллельных каналов.

Глава 11 "Организация группового вещания в мультисервисных ЛВС" целиком посвящена рассмотрению особенностей использования группового обмена (Multicast) для передачи данных в мультисервисных сетях.

Глава 12 "Управление трафиком приложений мультисервисных ЛВС" содержит описание теоретических положений и современных принципов обеспечения требуемых значений параметров информационного обмена путем регулирования трафика приложений в мультисервисной ЛВС.

Заключительная часть книги посвящена особенностям реализации мультисервисных сетей с использованием технологий Ethernet. В ней рассматриваются вопросы практического характера, такие, например, как организация каналов передачи данных или подключение абонентского оборудования.

В *главе 13 "Способы и схемы построения мультисервисных ЛВС"* рассматриваются особенности использования различных схем взаимного соединения компонентов при построении мультисервисных ЛВС. Подробно изложены принципы реализации надежных кольцевых соединений компонентов ЛВС с использованием технологий *RPR* (Resilient Packet Ring).

Глава 14 "Построение магистральных соединений мультисервисных ЛВС" содержит описание принципов построения и основные технические характеристики компонентов, используемых при создании магистральных соединений Gigabit Ethernet и 10Gigabit Ethernet.

Глава 15 "Организация подключения абонентов к оборудованию мультисервисных ЛВС" посвящена рассмотрению различных аспектов подключения абонентских устройств — контроля целостности линий, автоматического согласования параметров обмена и управления электропитанием.

Глава 16 "Программные компоненты мультисервисных ЛВС" содержит описание технологий и программных решений, применяемых для управления сетевыми компонентами по протоколу *SNMP* (Simple Network Management Protocol). Также рассматриваются особенности применения решений Cisco Systems NetFlow для учета трафика абонентов и примеры реализации программного комплекса обработки телефонных вызовов.

В процессе подготовки настоящего издания для иллюстрирования излагаемого материала были использованы:

- телекоммуникационное оборудование и эксплуатационная документация компаний Cisco Systems, 3COM, D-Link и Allied Telesyn;

- демонстрационные и свободно распространяемые версии программного обеспечения компаний Castle Rock Computing, NCH Swift Sound, SoftPerfect Research и VideoLAN Team (**www.VideoLAN.org**).

Использованные обозначения

Расшифровка большинства терминов и аббревиатур, использованных в тексте книги, приведена в *перечне сокращений*. В дополнение к этому, некоторые из используемых терминов достаточно подробно раскрыты в соответствующих главах.

Курсив использован в тексте книги для обозначения стандартных устоявшихся терминов в сфере телекоммуникаций, ссылки на которые представлены в глоссарии данного издания, например, протокол *STP* (Spanning Tree Protocol).

Прописные буквы в тексте книги обычно используются для обозначения названий полей блоков данных различных протоколов, например, поле TYPE.

Шрифт Courier использован в представленных листингах для обозначения примеров управляющих инструкций, которые передаются на устройства для изменения их конфигурации. Этот же шрифт использован для выделения наименований сообщений, например, сообщение `SETUP`. Кроме того, курсивный шрифт Courier используется для обозначения ответных сообщений конфигурируемого устройства, например:

```
ST-2811#sh clock
18:46:15.178 None Mon Feb 12 2007
```

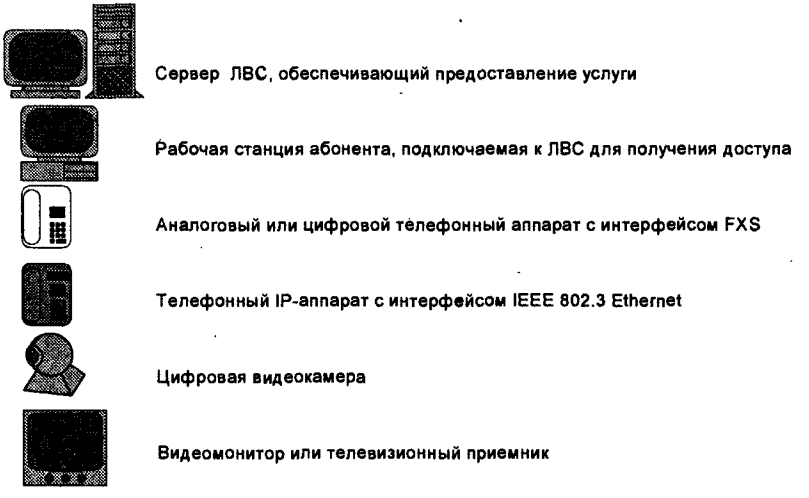
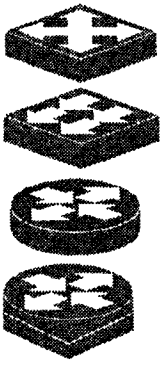


Рис. В1. Графические обозначения абонентов мультисервисных ЛВС

На рис. В1 приведены наиболее часто употребляемые в книге графические обозначения абонентов мультисервисных ЛВС.

На следующем рисунке (рис. В2) представлены графические обозначения, которые в тексте книги применяются для обозначения активных компонентов ЛВС.



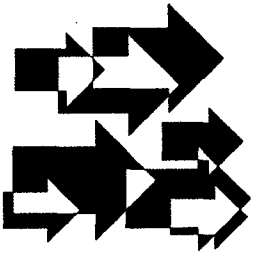
Сетевое устройство, выполняющее обработку данных на физическом уровне информационного взеимодействия - повторитель, репитер, HUB

Сетевое устройство, выполняющее обработку данных на канальном уровне информационного взаимодействия - мост, коммутатор Ethernet

Сетевое устройство, выполняющее обработку данных на сетевом уровне информационного взаимодействия - маршрутизатор, router

Сетевое устройство, выполняющее обработку данных на нескольких уровнях информационного взаимодействия - многоуровневый коммутатор Ethernet

Рис. В2. Графические обозначения активных компонентов ЛВС



ЧАСТЬ I

Задачи и способы построения современных МСС

Глава 1. Способы построения МСС

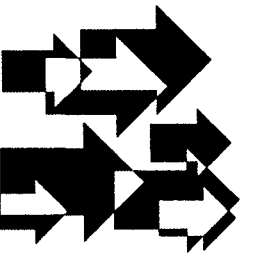
Глава 2. Голосовые приложения мультисервисных сетей

Глава 3. Коммерческие и технологические видеоприложения мультисервисных сетей

Глава 4. Организация обмена в мультисервисных сетях

Глава 5. Особенности построения современных МСС

ГЛАВА 1



Способы построения МСС

Эта глава представляет обзор наиболее популярных технологий построения мультисервисных сетей. Не все из представленных технологий одинаково успешно развиваются в настоящее время, однако каждая из них имеет свои достоинства и особенности, которые позволяют успешно применять ее для построения МСС. Кроме того, более современные технологии, как правило, используют многие принципы и механизмы, апробированные на более ранних технологиях.

В первом разделе данной главы рассматриваются основные принципы построения классических мультисервисных сетей: ISDN, Frame Relay, ATM.

Второй раздел посвящен рассмотрению технологий и принципов построения современных мультисервисных сетей, среди которых выделяются технологии DOCSIS, WiMAX и EPON.

Традиционные мультисервисные сети

Как было отмечено во введении к настоящему изданию, взаимное проникновение сетей различного назначения путем использования единых компонентов и совмещения выполняемых функций уже имеет достаточно богатую историю. Среди традиционных технологий, которые были призваны обеспечить интеграцию разнородного трафика в единых телекоммуникационных инфраструктурах прошлых лет, в первую очередь следует отметить технологии ISDN, Frame Relay и ATM. И хотя сегодня эти технологии можно считать морально устаревшими, большинство основополагающих принципов и технических решений, которые были в них использованы впервые, остаются по-прежнему актуальными.

Цифровые сети ISDN с интеграцией услуг

Технология *ISDN* (Integrated Services Digital Network) появилась в начале 1990 годов и представила первую реализацию идеи интеграции услуг — объединение сетей передачи данных и телефонных сетей. До появления сетей ISDN телефонные сети и сети передачи данных развивались независимо друг от друга, однако использовали единые коммуникации — абонентские линии и магистральные каналы. Помимо указанных выше передачи данных и стандартных телефонных сервисов, технология ISDN обеспечивает и новые виды услуг, такие, например, как высокоскоростная передача файлов и организация видеоконференций.

Инициаторами создания технологии ISDN были крупные телефонные операторы, и это, несомненно, оказало влияние на идеологию построения этой сети. По существу, сеть ISDN представляет собой глобальную сеть, которая для обеспечения передачи данных использует те же идеи, принципы и аппаратные решения, которые положены в основу построения современной телефонной сети:

- предоставление услуги путем организации вызовов;
- выделение гарантированной полосы пропускания для обслуживания каждого вызова.

Сеть ISDN представляет также дальнейшее развитие идеи передачи голосового трафика в цифровой форме, что обеспечивает дополнительное повышение качества телефонной связи.

Типы услуг сети ISDN

Интеграция разнородных трафиков в сети ISDN выполняется по принципу временного разделения или согласно технологии *TDM* (Time Division Multiplexing). Для передачи каждого из видов трафика при этом выделяется фиксированная, согласованная и гарантированная доля полосы пропускания сети ISDN в виде *стандартного (элементарного) канала*. Выделение сетевых ресурсов ISDN выполняется по запросам, поступающим от абонента. Абонент сети ISDN формирует запрос (CALL), в котором он указывает тип запрашиваемой услуги и адрес удаленного абонента. В том случае, если сеть обладает необходимыми ресурсами для организации вызова, то вызывающий абонент получает в свое распоряжение коммутируемый канал, соединяющий его с вызываемым абонентом. Для передачи сигналов, используемых для организации и обслуживания абонентских вызовов в сети ISDN, применяются специальные *каналы внеканальной сигнализации*.

Стандартизирующие документы ISDN определяют набор элементарных каналов, комбинации из которых могут быть использованы для формирования

различных типов абонентских интерфейсов. В табл. 1.1 представлен набор стандартных каналов сети ISDN. Наибольшее распространение получили только каналы типов "D" и "B", которые составляют абонентские интерфейсы первичной и базовой скорости ISDN.

Таблица 1.1. *Стандартные каналы сети ISDN*

Тип	Скорость	Назначение
A	—	Аналоговый телефонный канал 4 кГц
B	64 Кбит/сек	Передача данных или оцифрованного голосового сигнала
C	8 или 16 Кбит/сек	Цифровой канал передачи данных
D	16 или 64 Кбит/сек	Цифровой канал передачи внеканальной сигнализации
E	64 Кбит/сек	Цифровой канал для внутренней сигнализации ISDN
H0	384 Кбит/сек	Цифровой канал передачи данных
H10	1472 Кбит/сек	Цифровой канал передачи данных
H11	1536 Кбит/сек	Цифровой канал передачи данных
H12	1920 Кбит/сек	Цифровой канал передачи данных

Интерфейс базовой скорости ISDN, или иначе интерфейс *BRI* (Basic Rate Interface), предоставляет абоненту сети ISDN услуги в виде двух каналов типа "B" с пропускной способностью 64 Кбит/сек. Оба этих канала могут быть использованы абонентом для обеспечения информационного обмена и для передачи и приема оцифрованного телефонного трафика. Передача сигналов внеканальной сигнализации в данном случае выполняется по независимому каналу типа "D", который имеет пропускную способность 16 Кбит/сек. Сформированный таким образом интерфейс базовой скорости ISDN обычно обозначается "2B+D" и может быть использован для организации одного или двух цифровых телефонных каналов или для передачи данных со скоростью до 128 Кбит/сек.

Интерфейс первичной скорости ISDN, или иначе интерфейс *PRI* (Primary Rate Interface), имеет различную структуру в разных регионах мира. В Европе PRI предоставляет абоненту услуги сети ISDN в виде 30 каналов "B"-типа и одного канала "D"-типа (30B+D). В Северной Америке и Японии интерфейс PRI предоставляет пользователю сеть ISDN в виде 23 каналов "B"-типа и одного канала "D"-типа (23B+D). Передача сигналов внеканальной сигнализации в интерфейсе первичной скорости выполняется по независимому каналу типа "D", который имеет пропускную способность 64 Кбит/сек. Элементарные каналы PRI также могут быть использованы как для передачи данных, так и передачи оцифрованного телефонного трафика.

Принципы построения и компоненты сетей ISDN

Сеть ISDN образуют функциональные компоненты, связанные друг с другом стандартизированными интерфейсами для передачи управляющей информации и абонентского трафика. Основными компонентами сетей ISDN являются:

- абонентские терминалы;
- терминальные адаптеры, или иначе *TA* (Terminal Adapters);
- сетевые терминальные устройства, или иначе *NT* (Network Termination Devices);
- линейные терминальные устройства, или иначе *LT* (Line-Termination Equipment).

Абонентские терминалы ISDN обеспечивают доступ пользователя к услугам сети. В сети ISDN могут быть использованы два типа абонентских терминалов:

- специализированные ISDN терминалы — *TE1*;
- неспециализированные ISDN терминалы — *TE2*.

Специализированные ISDN терминалы TE1 обеспечивают представление данных пользователю и непосредственное подключение пользователя к интегрированной сети. Неспециализированные ISDN терминалы TE2 представляют собой терминалы в обычном понимании этого термина и не обеспечивают непосредственного подключения пользователя к сети ISDN.

Схема подключения различных абонентских терминалов к сети ISDN приведена на рис. 1.1. Для подключения к сети неспециализированных терминалов используются терминальные адаптеры ISDN, обозначенные буквами "TA" на приведенном рисунке. Символ "R" используется для общего обозначения интерфейсов, которые соединяют неспециализированные терминалы ISDN и терминальные адаптеры.

Сетевой терминал NT2 обеспечивает взаимодействие абонентских терминалов с сетью ISDN. Основной функцией NT2 является управление доступом абонентских терминалов к каналам передачи данных сети ISDN. Задачей этого сетевого терминала также является организация и обслуживание вызовов, поступающих из сети и от абонентских терминалов. Для обозначения магистрали подключения абонентских терминалов ISDN к сетевому терминалу NT2 используется литера "S".

Магистраль подключения абонентов ISDN

Основные технические требования и характеристики магистрали S ISDN BRI представлены в рекомендации *ITU-T I.430 (11/95)* "BASIC USER-NETWORK INTERFACE — LAYER 1 SPECIFICATION".

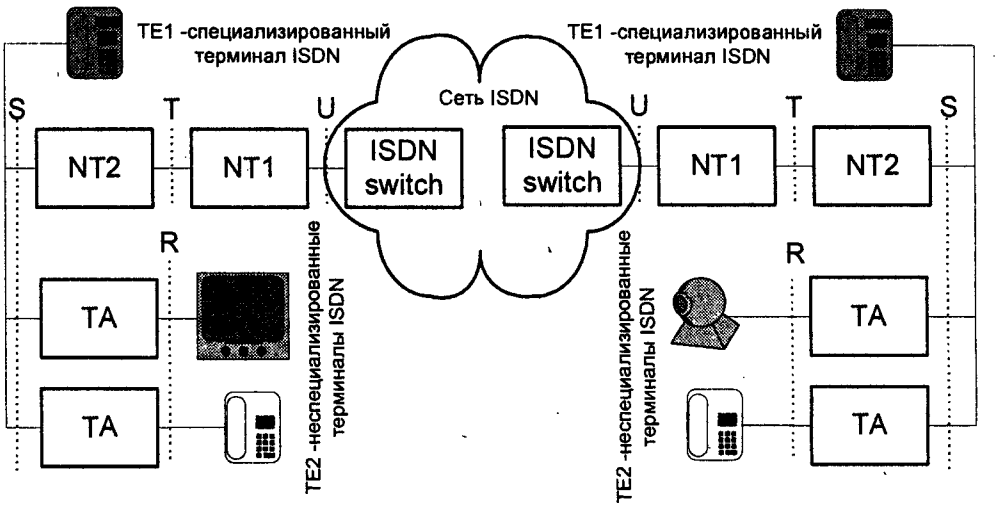


Рис. 1.1. Схема подключения абонентских терминелов к сети ISDN

В соответствии с этим документом подключение абонентских терминалов к NT2 может быть выполнено как по схеме "точка-точка", так и по многоточечной схеме. В зависимости от выбранного варианта подключения, максимальное расстояние от сетевого терминала до абонентского терминала может изменяться. Абсолютно максимальное значение расстояния составляет 1 000 м и соответствует подключению к сетевому терминалу одного терминала TE1.

Примечание

Фактором, ограничивающим максимальную длину магистрали S, является затухание сигнала в кабеле. По нормативам I.430 максимальное значение этого параметра не должно превышать значения 6 дБ.

Для подключения к магистрали S используется 8-контактный соединитель RJ-45. Общее количество проводов в магистрали может доходить до 4-х пар, из них собственно для передачи данных по магистрали S используется две пары — по одной для приема и передачи данных. Еще две пары при необходимости могут быть использованы для того, чтобы передать терминалам питающее напряжение. Информационный обмен через магистраль S осуществляется фиксированными информационными блоками, каждый из которых состоит из 48 бит и передается с частотой 4 кГц. В состав этих блоков входят 4 байта данных, которые передаются по каналам "B"-типа интерфейса BRI, и четыре бита внеканальной сигнализации, передаваемые по каналу "D". Остальные биты блока являются служебными и используются для управления доступом терминального оборудования к шине S.

Абонентский терминал может инициировать процесс информационного обмена только путем посылки информационного сообщения через канал сигнализации "D". Поскольку к магистрали S может быть одновременно подключено несколько устройств TE, теоретически возможно возникновение коллизий, которые появляются в тот момент, когда два или несколько терминалов пытаются передавать сообщение одновременно. Для того чтобы терминалы смогли обнаружить возникновение такой коллизии, сетевой терминал возвращает полученные им по каналу "D" биты в специальных эхо-разрядах E формируемого им информационного блока. Передающий терминал контролирует соответствие принятых эхо-битов и переданных им битов канала "D" и, следовательно, может обнаружить возникновение коллизии.

Взаимодействие абонентов с сетью ISDN

Сетевой терминал NT1 используется для организации взаимодействия абонентских терминалов с сетью ISDN. Точке сопряжения NT1 и NT2 стандартами ISDN присвоено буквенное обозначение "T" (см. рис. 1.1). Основной функцией NT1 является преобразование интерфейсов для подключения удаленного абонентского офиса к ближайшему коммутатору сети ISDN. Точке сопряжения NT1 с коммутатором стандартами ISDN присвоено буквенное обозначение "U".

Информационное взаимодействие в точке сопряжения U выполняется по схеме "точка-точка" и осуществляется по двухпроводной линии в режиме полного дуплекса. При этом для обеспечения требуемой дальности передачи используется линейное кодирование данных по алгоритму 2B1Q. Увеличение дальности распространения сигнала при использовании этого алгоритма достигается за счет уменьшения частоты сигнала, который передается по линии. Для передачи сигнала 2B+D, информационная скорость которого составляет 160 Кбит/сек, используется амплитудно-импульсно-модулированный сигнал 80 кГц.

Большая номенклатура стандартных функциональных блоков и точек сопряжения вызвана различиями в технической политике между европейскими странами и США. В Европе сеть ISDN предоставляется пользователю в точке сопряжения S и, следовательно, аппаратура сетевых терминалов должна быть размещена у провайдера. В Америке услуги сети ISDN предоставляются пользователю в точке сопряжения U, это означает, что сетевые терминалы должны быть размещены на оборудовании абонента. На практике указанные выше компоненты сети ISDN практически никогда не выполняются в виде отдельных блоков. Как правило, сетевые терминалы изготавливаются в виде единого устройства, которое называется *блоком абонентского доступа ISDN.*

Управление процессами передачи данных по каналам типа "B" сети ISDN осуществляется путем обмена управляющими командами, которые переда-

ются по каналам "D". Для передачи управляющей информации на канальном уровне модели информационного взаимодействия OSI ISO 7498 используется специально разработанный для использования в сетях ISDN протокол *LAPD* (*Link* Access Procedure D-channel). Спецификация этого протокола определена в рекомендации *ITU-T Q.921 (09/97)* — "ISDN USER-NETWORK INTERFACE — DATA LINK LAYER SPECIFICATION".

Примечание

Краткая информация о модели информационного взаимодействия открытых систем OSI ISO 7498 приведена в *главе 6* настоящего издания.

В соответствии с требованиями данной рекомендации управляющая информация по каналу "D" передается в виде кадров переменной длины. Кадр протокола LAPD содержит 5 полей: FLAG, ADRESS, CONROL, DATA, FCS.

Поле FLAG занимает в кадре первый и последний байт и используется для обрамления кадра. С помощью данной последовательности приемник распознает начало и конец блока данных канального уровня.

В поле ADRESS может быть также помещен физический адрес терминала, или иначе *TEI* (Terminal Endpoint Identifier) — 7 бит. Наличие этого адреса в пакете LAPD позволяет выполнять процедуры информационного взаимодействия с одним из группы абонентских терминалов, подключенных к магистрали S. Динамически выделяемые адреса находятся в диапазоне от 64 до 126. Адреса с 0 по 63 закрепляются за терминалами статически, адрес 127 используется для широковещательных пакетов, которые адресованы всем абонентским терминалам.

Тип информации, которая размещена в поле CONROL, зависит от типа кадра LAPD. Следует заметить, что кадры бывают трех типов:

- *Информационные кадры* — (Information Frames) I-кадры — предназначены для непосредственной передачи управляющих сообщений сетевого уровня ISDN. В поле CONTROL — номер передаваемого кадра и номер кадра, ожидаемого к приему;
- *Управляющие кадры* — (Supervisory Frames) S-кадры — предназначены для управления процессом передачи I-кадров и для разрешения проблем, которые связаны с потерями кадров в процессе передачи. В поле CONTROL содержится номер кадра, ожидаемого к приему;
- *Ненумерованные кадры* — (Unnumbered Frames) U-кадры — предназначены для управления логическим каналом. В поле CONTROL содержится управляющая и диагностическая информация.

Блоки данных сетевого уровня ISDN предназначены для непосредственной передачи сигнальной информации в виде сообщений, которые используются

для управления абонентскими запросами. Структура блоков данных сетевого уровня, алгоритмы установления, обслуживания и разрыва соединений приведены в рекомендации *ITU-T Q.931 (05/98)* — "ISDN USER-NETWORK INTERFACE LAYER 3 SPECIFICATION FOR BASIC CALL CONTROL".

В пакете ISDN размещается управляющая информация, которая содержит:

- основные параметры создаваемого по данному запросу соединения (тип соединения, скорость передачи данных, адреса вызываемого и вызывающего абонентов);
- тип выполняемой процедуры (создание соединения, завершение соединения);
- состояние обслуживаемого запроса.

Для организации запроса TE формирует сообщение SETUP сетевого уровня — "Установление соединения". Сообщение SETUP передается в направлении ближайшего к данному терминалу коммутатора ISDN. Во время предварительной проверки данного сообщения коммутатор определяет наличие ресурсов для организации запроса. В частности, проверяется наличие свободного канала "B" в направлении инициатора обмена, а также доступность вызываемого абонента — определяется теоретическая возможность дозвониться до указанного абонента. В том случае, если все необходимые условия для организации запроса соблюдены, коммутатор посылает в направлении инициирующего терминала сообщение CALL PROCEEDING. Данное сообщение подтверждает возможность установления соединения и закрепляет за инициируемым запросом один из каналов "B".

Вызываемый абонент подтверждает получение запроса передачей сообщения ALERTING — "Приведение в готовность". Затем вызываемый абонент определяет возможность ответа на данный запрос. В том случае, если данный входящий запрос может быть разрешен, то вызываемый терминал пользователя формирует сообщение CONNECT — "Соединение установлено". Это сообщение передается коммутаторами по сети в направлении терминала — инициатора соединения. При получении этого сообщения вызывающий терминал формирует сообщение о подтверждении установления соединения CONNECT ACKNOWLEDGE и начинает процесс информационного обмена с использованием соответствующих каналов "B".

Завершение запроса может быть произведено по инициативе любого из компонентов, которые принимали участие в его организации. Для завершения запроса терминал или коммутатор направляет ближайшему компоненту сообщение о разрывании соединения — DISCONNECT. В ответ на данное сообщение ближайший компонент ISDN формирует ответное сообщение о завершении запроса — RELEASE. Данное сообщение сигнализирует о возможности

освобождения ресурсов, которые были использованы при организации запроса — в первую очередь это информационные каналы "B"-типа. Для подтверждения освобождения компонентов, которые были использованы при организации запроса, используется сообщение RELEASE COMPLETE — "Освобождение завершено".

Технология Frame Relay

Технология, которая впоследствии получила название "Коммутация кадров", или иначе *FR* (Frame Relay), первоначально была разработана в 1980-х для использования в сетях ISDN, но после гораздо более активно использовалась как альтернатива выделенным линиям при построении сетей доступа в Интернете. Развитием спецификации Frame Relay занимается неформальная и некоммерческая организация *Frame Relay Forum — FRF*.

Технология FR обеспечивает информационное взаимодействие на физическом и канальном уровне OSI ISO 7498 и позволяет реализовать динамическое разделение ресурсов канала между абонентскими приложениями.

Технология FR имела ряд преимуществ по сравнению с технологиями X.25 и ISDN, которые использовались в то время для обеспечения доступа к распределенным вычислительным ресурсам. Характерными особенностями сетей доступа, построенных с использованием FR, являются:

- использование виртуальных каналов для изоляции трафика абонентских приложений;
- высокая степень готовности сети передачи данных;
- малая величина вносимой задержки;
- низкая стоимость и высокая эффективность использования канала;
- возможность масштабирования построенных сетей доступа.

Особенности построения сетей Frame Relay

Технология FR регламентирует организацию информационного взаимодействия только на канальном уровне OSI ISO 7498. Основными компонентами сети являются коммутаторы FR, иначе *FR switch*, и устройства подключения абонентов — *FRAD* (Frame Relay Access Device). Передача данных в сети, построенной с использованием технологии Frame Relay, выполняется по виртуальным каналам, иначе *PVC* (Permanent Virtual Circuits), которые представляют собой логическое соединение, существующее между двумя устройствами FRAD в сети FR.

Для идентификации виртуальных каналов в сети Frame Relay используется аппарат идентификаторов логических каналов, или иначе *DLCI* (Data-Link

Connection Identifier). Значение DLCI однозначно определяет номер виртуального канала для устройства Frame Relay и номер виртуального порта для абонентского приложения.

На рис. 1.2 приведена схема организации виртуальных каналов для обеспечения информационного обмена между головным и периферийными офисами некоторой организации.

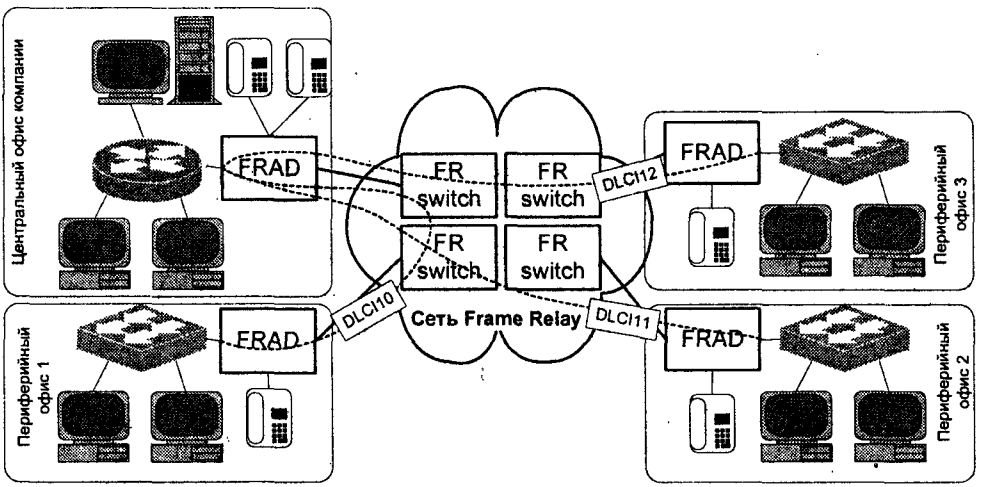


Рис. 1.2. Использование виртувльных каналов FR для обеспечения информационного обмена между головным и периферийными офисами некоторой организации

В данном случае виртуальный канал с идентификатором DLCI 10 используется для передачи данных из первого периферийного офиса в центральный офис организации. Виртуальные каналы с идентификаторами DLCI 11 и 12 используются для аналогичной цели в периферийных офисах 2 и 3 соответственно.

Примечание

Идентификатор DLCI обычно имеет только локальное значение. Он должен быть уникальным только в пределах одного интерфейса FRAD.

Прямые каналы для передачи данных между периферийными офисами в этой схеме отсутствуют, поэтому информационный обмен между ними возможен только через маршрутизатор центрального офиса. Специальные порты FRAD могут быть использованы для организации служебной телефонной связи между офисами. В этом случае должны быть организованы дополнительные виртуальные каналы, соединяющие телефонных абонентов.

Таким образом, в сети, основанной на технологии FR, для каждого информационного соединения между абонентами должен быть построен логический

канал, проходящий через один или несколько коммутаторов. Эти виртуальные каналы, как правило, являются постоянными и образуют логическую топологию сети. Для изменения этой топологии требуется внесение соответствующих коррекций в настройки коммутаторов, через которые проходят модифицируемые виртуальные соединения.

Структура кадра Frame Relay

Передача данных по виртуальному каналу выполняется стандартными блоками переменной длины, которые называются *кадрами Frame Relay*. Кадр Frame Relay содержит минимально необходимое количество служебных полей, что и определяет высокую эффективность использования данной технологии для передачи данных. В состав кадра Frame Relay входят:

- *стартовый флаг* — выполняет функцию обрамления кадра — 1 байт;
- *заголовок кадра* — здесь размещается информация, которая используется для управления виртуальными соединениями и процессами передачи данных в сети Frame Relay — 2 байта;
- *полезная нагрузка* (Information field) — предназначено для переноса блоков данных протоколов верхних уровней — имеет переменную длину;
- *контрольная сумма кадра* (FCS) — содержит 16-разрядную контрольную сумму всех полей кадра Frame Relay — 2 байта;
- *завершающий флаг* — выполняет функцию обрамления кадра — 1 байт.

Примечание

Кадр Frame Relay во многом напоминает кадр ISDN, что не случайно, поскольку обе технологии в большей или меньшей степени используют принципы информационного обмена, определенные в спецификации ISO High-Level Data Link Control — HDLC.

Структура заголовка кадра Frame Relay представлена в табл. 1.2.

***Таблица 1.2.** Структура заголовка кадра Frame Relay*

Номер поля	Содержание поля	Номер байта/ полубайта	Номер бита
1	DLCI — Идентификатор виртуального канала (ст. часть)	0	7—2
2	C/R — Признак ответного сообщения	0	1
3	EA — Признак расширения заголовка (=1)	0	0
4	DLCI — Идентификатор виртуального канала (мл. часть)	1	7—4
5	FECN — Признак перегрузки (по ходу потока)	1	3

Таблица 1.2 (окончание)

Номер поля	Содержание поля	Номер байта/ полубайта	Номер бита
6	BECN — Признак перегрузки (против хода потока)	1	2
7	DE — Указание о возможности удаления кадра	1	1
8	EA — Признак расширения заголовка (=0)	1	0

Содержимое поля DLCI у каждого полученного кадра коммутатор FR анализирует для того, чтобы по таблице существующих соединений определить номер интерфейса, через который его нужно отправить. По этой же таблице коммутатор определяет новое значение поля, которое будет использоваться для определения номера интерфейса на следующем коммутаторе.

Бит признака ответного сообщения является атавизмом HDLC и не имеет функциональной нагрузки в технологии.

Бит EA используется в качестве признака, который определяет размер заголовка кадра. Заголовок кадра Frame Relay имеет переменную длину и может содержать 2—4 байта. В поле EA последнего байта заголовка должен быть помещен 0.

Биты FECN и BECN обеспечивают функционирование процедуры явного указания перегрузки — Explicit Congestion Notification. При возникновении перегрузки на коммутаторе Frame Relay бит FECN устанавливается равным 1 в кадрах, которые следуют по направлению перегружающего потока. Бит BECN устанавливается равным 1 в кадрах, которые следуют навстречу перегружающему потоку. Эти признаки должны быть использованы протоколами сетевого и последующих уровней для регулирования скорости информационного обмена.

Примечание

Технология Frame Relay принципиально не имеет собственных механизмов управления темпом информационного обмена. Эта особенность объясняется тем, что FR была предназначена для обеспечения доступа в сеть IP, где для решения этой задачи, при необходимости, должен был использоваться протокол TCP.

Бит DE (Discard Eligibility) используется для обеспечения функционирования второго механизма управления потоком данных в сетях Frame Relay. Этот признак выставляется равным 1 в тех кадрах, которые передаются с нарушением установленного уровня качества обслуживания (см. *следующий раздел*).

Параметры качества обслуживания Frame Relay

В качестве параметров качества обслуживания абонентов сети, построенной на технологии Frame Relay, используются:

- значение согласованной информационной скорости, или иначе *CIR* (Committed Information Rate);
- гарантированный объем передаваемых данных (Committed Burst Size — Bc);
- не гарантированный объем передаваемых данных (Excess Burst Size — Be);
- интервал неравномерности трафика — Tc.

Согласованное значение информационной скорости — CIR — является одним из основных параметров, который определяет стоимость услуги для абонента FR. Значение CIR определяется отдельно для каждого PVC(DLCI)-абонента. В данном случае согласованная информационная скорость — это максимальная скорость, с которой пользователь может обеспечивать информационный обмен по отдельному виртуальному каналу.

Сумма значений CIR всех PVC, которые определены для физического канала, не должна превышать (0,75—0,8) доли его пропускной способности.

Значения гарантированного объема передаваемых данных определяет максимальный объем данных пользователя, который может быть передан без потерь за период Tc.

Значение Be определяет величину предельного увеличения трафика пользователя для конкретного виртуального канала PVC. В "Be" кадрах, принятых за период Tc свыше положенных "Bc", коммутатор устанавливает признак DE = 1. Это означает, что эти кадры будут первыми удалены из очереди на обработку при превышении порогового значения ее длины. Все остальные кадры, которые будут приняты на коммутатор до завершения периода Tc, подлежат уничтожению.

Следует отметить, что в технологии Frame Relay отсутствуют действенные методы планирования и регулирования абонентского трафика, поэтому установленные соглашения о качестве обслуживания могут быть выполнены только методом "Best Efforts". По этой же причине абоненту достаточно сложно проконтролировать уровень качества предоставляемой услуги.

Спецификация LMI

Широкое использование технологии Frame Relay в качестве универсальной транспортной среды вызвало необходимость разработки дополнительных спецификаций, которые обеспечивали более гибкое управление ресурсами PVC и SVC в сети Frame Relay. Одной из первых таких спецификаций была

спецификация LMI. Спецификация интерфейса локального управления, или иначе *LMI* (Local Management Interface), была разработана в 1990 году инициативной группой, в которую вошли компании Cisco Systems, StrataCom, Northen Telecom и DEC. Появление интерфейса локального управления позволило обеспечить передачу по сети, построенной с использованием технологии Frame Relay, сообщений, управляющих структурой виртуальных каналов. Создание спецификации LMI позволило использовать следующие виды сервиса:

- применение значений DLCI для глобальной адресации в сети Frame Relay;
- механизм автоматического определения текущего статуса PVC;
- внедрение режима группового обмена;
- применение процедур обратного разрешения (определение номера DLCI по соответствующему адресу IP).

Для передачи управляющих сообщений в первоначальном варианте спецификации LMI предлагалось использовать DLCI #1023. Мониторинг состояния PVC в данном случае осуществлялся с использованием принципа запрос-ответ (Status inquiry и Status report соответственно). Впоследствии организации ANSI и ITU-T разработали свои версии спецификации LMI:

- ITU-T Q.933bis "ABSTRACT TEST SUITE — SIGNALING SPECIFICATION FOR FRAME MODE BASIC CALL CONTROL CONFORMANCE TESTING FOR PERMANENT VIRTUAL CONNECTIONS (PVCs)";
- ANSI "SUPPLEMENT T1.617A-1994" (annex D).

Указанные выше спецификации разрабатывались с использованием материалов, которые были подготовлены специалистами FRF. Благодаря этому указанные спецификации отличаются незначительно и допускают совместную реализацию, хотя и не являются полностью совместимыми. От первоначального варианта (Cisco) интерфейса локального управления обе эти спецификации отличаются тем, что обеспечивают взаимодействие однотипного оборудования при управлении параметрами PVC по интерфейсу "Сеть-Сеть" (Network to Network Interface — *NNI*). Другим отличием является использование DLCI#0 (а не 1023) для передачи управляющих сообщений.

Технология ATM и ее использование в мультисервисных сетях

Технология ATM представляет собой дальнейшее развитие принципов, которые были положены в основу технологий ISDN и Frame Relay. Как уже было отмечено, технологии ISDN и Frame Relay не могли обеспечить возможность построения достаточно качественной и гибкой цифровой сети с интегрированными услугами. Технология ISDN обеспечивала гарантированное качест-

во обслуживания, однако не обладала необходимой гибкостью и не позволяла абоненту использовать высокие (более 2 Мбит/сек) скорости передачи данных. Технология Frame Relay обеспечивала бóльшие, чем технология N-ISDN скорости передачи данных и достаточную эффективность использования ресурсов физического канала, однако была не способна выделить гарантированную полосу пропускания для передачи оцифрованного голосового трафика. Сети, построенные по технологии ATM, должны были обеспечить возможность передачи разнородного информационного трафика по единому каналу.

Аббревиатура *ATM* означает Asynchronous Transfer Mode (в дословном переводе — технология асинхронной передачи). Термин "асинхронный" в названии технологии указывает на ее отличие от синхронных технологий с фиксированным распределением пропускной способности канала между информационными потоками (TDM, ISDN). ATM называют также технологией коммутации ячеек. Существенное отличие технологии ATM от ISDN и Frame Relay заключается в том, что блок данных канального уровня ATM имеет фиксированную длину — 53 байта. Фиксированная длина ячейки ATM обеспечивает гарантированное постоянное время ее обработки на коммутирующем оборудовании, и следовательно — возможность обеспечения гарантированного качества обслуживания информационных потоков пользователя. Эта особенность также делает возможным построение аппаратных коммутаторов ATM, что в свою очередь приводит к резкому уменьшению времени коммутации ячейки и к увеличению пропускной способности системы в целом.

Компоненты сетей ATM

Главными компонентами сетей, которые построены на технологии ATM, являются ATM-коммутаторы (ATM Switches), которые взаимодействуют между собой по межсетевым интерфейсам — *NNI* (Network to Network Interface), и оборудование пользователя — *CPE* (Customer Premises Equipment), которое взаимодействует с коммутатором ATM по абонентскому интерфейсу — *UNI* (User — to — Network Interface). ATM-коммутаторы представляют собой быстродействующие специализированные вычислительные устройства, которые аппаратно реализуют функцию коммутации ячеек ATM между своими портами.

Устройства CPE обеспечивают адаптацию информационных потоков пользователя для передачи с использованием технологии ATM. Эти устройства могут иметь самую разнообразную реализацию — в зависимости от типа конкретного информационного потока. Это могут быть коммутаторы локальных вычислительных сетей, маршрутизаторы, рабочие станции. Функциональное назначение CPE в сетях ATM соответствует устройству FRAD в сети Frame Relay.

Так же, как и Frame Relay, технология ATM является ориентированной на соединение — это означает, что процесс передачи данных состоит как минимум из двух этапов: создания соединения и собственно передаче данных. Для передачи данных в сети ATM организуется виртуальное соединение — *VC* (Virtual Circuit).

В пределах интерфейса виртуальное соединение ATM определяется уникальным сочетанием идентификатора виртуального пути — *VPI* (Virtual Path Identifier) и идентификатора виртуального канала — *VCI* (Virtual Circuit Identifier).

Определения

Виртуальный канал ATM представляет собой фрагмент логического соединения, по которому производится передача данных одного пользовательского процесса.

Виртуальный путь ATM представляет собой группу виртуальных каналов, которые в пределах данного интерфейса имеют одинаковое направление передачи данных.

На рис. 1.3 приведена схема коммутации ячеек на коммутаторе ATM.

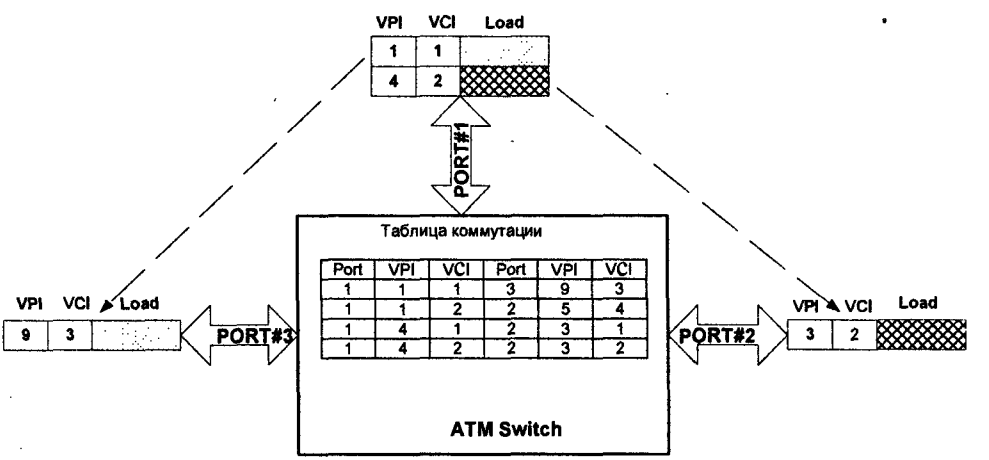


Рис. 1.3. Схема коммутации ячеек на ATM-коммутаторе

ATM-коммутатор (ATM Switch) анализирует значения идентификаторов виртуального пути (VPI) и виртуального канала (VCI) у ячеек, поступающих на его входной порт, и направляет эти ячейки на один из выходных портов. Для определения номера выходного порта коммутатор использует динамически создаваемую таблицу коммутации. На схеме, которая приведена на рис. 1.3,

коммутатор ATM выполняет обработку двух ячеек, которые поступают на его порт № 1. В соответствии с содержимым таблицы коммутации, первая из принятых ячеек будет передана через порт № 3, и для нее будут установлены новые значения VPI = 9 и VCI = 3.

Примечание

В том случае, если один абонент сети ATM получает трафик нескольких приложений, значение VPI может быть ассоциировано с сетевым адресом абонента, а VCI — с номером приложения. При этом коммутация ячеек на промежуточных коммутаторах сети ATM будет выполняться только по идентификатору виртуального пути — VPI.

Формат ячейки ATM

Ячейка ATM имеет длину 53 байта и состоит из двух частей:

- *заголовок ячейки* — 5 байтов;
- *поле полезной нагрузки ячейки* — 48 байтов.

Заголовок может иметь различный формат в зависимости от типа интерфейса, через который передается ячейка. Незначительные изменения заголовка могут иметь ячейки ATM для различных аппаратных реализаций. Обязательными полями заголовка ячейки являются:

- VIRTUAL PATH IDENTIFIER (VPI);
- VIRTUAL CIRCUIT IDENTIFIER (VCI);
- PAYLOAD TYPE (PT);
- CONGESTION LOSS PRIORITY (CLP);
- HEADER ERROR CONTROL (HEC).

Идентификаторы VPI и VCI используются для обозначения виртуальных соединений ATM. Обычно для записи идентификатора виртуального пути используется 8 бит заголовка ячейки ATM. Для записи идентификатора виртуального канала обычно используется 16 бит заголовка ячейки ATM.

Поле PAYLOAD TYPE занимает 3 бита в заголовке ячейки ATM. В этом поле располагается информация, которая определяет тип информации, передаваемой в поле полезной нагрузки ячейки ATM, а также содержит управляющие биты. Первый бит поля PAYLOAD TYPE содержит собственно признак типа ячейки — управляющий или информационный. Во втором бите поля PAYLOAD TYPE ячейки информационного типа содержится признак возникновения перегрузки в сети. В третьем бите содержится признак незавершенности, который устанавливается в том случае, если содержимое поля по-

лезной нагрузки является продолжением информационного сегмента, размещенного в предыдущей ячейке.

Бит CLP в ячейке ATM имеет такое же значение, как бит DE в кадре Frame Relay. Ячейки ATM, у которых этот бит CLP установлен в 1, при возникновении перегрузки на коммутаторе должны быть уничтожены в первую очередь.

Поле HEC занимает один байт в заголовке ячейки ATM. В поле HEC ячейки ATM размещается проверочная контрольная сумма 4-х предыдущих байтов заголовка.

Интеграция трафика в сети ATM

Спецификация ATM forum 4.0, в зависимости от требований к скорости передачи, определяет пять основных классов передаваемых данных (трафика).

- *Постоянная информационная скорость* — *CBR* (Constant Bit Rate);
- *Переменная информационная скорость с лимитированным временем доставки* — *Rt-VBR* (Real Time Variable Bit Rate);
- *Переменная информационная скорость с нелимитированным временем доставки* — *Nrt-VBR* (Non — Real Time Variable Bit Rate);
- *Допустимая информационная скорость* — *ABR* (Available Bit Rate);
- *Неопределенная информационная скорость* — *UBR* (Unspecified Bit Rate).

Для каждого из классов передаваемых данных определен перечень параметров, которые регламентируют его обработку и доставку по сети ATM. Для трафика CBR, например, это могут быть значения (CIR, Bc, Be и Tc). Построение виртуального соединения для передачи этого вида трафика по сети ATM может быть выполнено только при условии обеспечения требуемых значений качества обслуживания. Это значение обеспечивается благодаря применению соответствующих протоколов и механизмов на каждом из уровней информационного взаимодействия ATM.

На физическом уровне OSI ISO 7498 в сети ATM осуществляется управление передачей и приемом по физической среде. На этом уровне также определяются способы задания границ и правила упаковки ячеек ATM в кадры физического уровня. Физический уровень ATM функционально делится на два подуровня:

- *Уровень физической среды* (Physical Medium Sub-Layer);
- *Уровень преобразования* (Transmission Convergence Sub-Layer).

На уровне физической среды определяются способы кодирования данных, процедуры обеспечения синхронизации передачи и приема данных. Протоколы, которые используются на данном уровне, полностью определяются ти-

пом среды передачи данных. Физический уровень преобразования ATM обеспечивает выполнение следующих функций:

- Формирование границ ячейки ATM на физическом уровне

  Для того чтобы приемник мог определить начало передачи ячейки в битовом потоке, сформированном передатчиком, в этот поток включаются специальные сигнальные последовательности.

- Помещение блоков данных в кадр физического уровня и выполнение обратной операции

  Для передачи ячеек ATM по физическому каналу они помещаются в кадры физического уровня. Физический уровень преобразования ATM обеспечивает формирование кадра физического уровня и управление его структурой.

- Формирование и проверка контрольной суммы заголовка

  Совпадение вычисленного значения контрольной суммы принятого заголовка ячейки ATM с переданным значением свидетельствует о правильном функционировании физического звена передачи данных.

- Согласование информационных скоростей

  При передаче некоторых типов трафика (например, CBR) с использованием технологии ATM необходима синхронизация источника данных и формирователя ячеек ATM. В том случае, если скорость, с которой передаются ячейки, превышает скорость, с которой данные поступают на передачу, возможно возникновение ситуации, когда в ячейку будет нечего поместить. В этом случае формируются пустые ячейки, которые будут уничтожены на приемной стороне.

Информационное взаимодействие на канальном уровне OSI ISO 7498 в сети ATM осуществляется на двух подуровнях:

- канальном уровне ATM;
- уровне адаптации ATM.

На канальном уровне ATM определяются процедуры и выполняются основные функции по управлению трафиком:

- создание виртуальных соединений;
- управление виртуальными соединениями;
- обеспечение необходимого уровня обслуживания.

Для выполнения этих функций используется информация, которая помещена в заголовке ячейки ATM.

Назначение уровня адаптации состоит в определении процедур, в соответствии с которыми выполняется преобразование блоков данных верхних уров-

ней в поток ячеек ATM. Уровень адаптации обеспечивает интерфейс для взаимодействия с протоколами сетевого уровня OSI ISO 7498.

Для того чтобы преобразование в ячейки оптимальным образом соответствовало типу трафика пользователя, применяется несколько стандартных уровней адаптации ATM:

- *уровень 1* — AAL1 (ATM Adaptation Layer1);
- *уровень 3/4* — AAL3/4 (ATM Adaptation Layer3/4);
- *уровень 5* — AAL5 (ATM Adaptation Layer5).

Уровень адаптации AAL1 предназначен для обеспечения передачи по сетям ATM трафика типа CBR (оцифрованный голос, видеоконференции). Использование этого уровня адаптации предполагает взаимную синхронизацию источника данных и адаптера ATM. Блоки данных, поступившие на вход адаптера, помещаются в поле полезной нагрузки очередной ячейки ATM в том порядке, в котором они были приняты.

Уровень адаптации AAL3/4 предназначен для обеспечения передачи по сетям ATM блоков данных *SMDS* (Switched Multi megabit Data Service).

Уровень адаптации AAL5 наиболее часто используется для передачи по сетям ATM трафика локальных вычислительных сетей и имеет специальное название — *SEAL* (Simple and Efficient Adaptation Layer). Процесс формирования ячеек ATM состоит из трех этапов. На первом этапе к входному кадру добавляется 32-разрядная контрольная сумма и заголовок. На втором этапе полученный блок данных разбивается на фрагменты по 48 байтов. В отличие от AAL3/4 никаких дополнительных информационных полей к фрагменту в данном случае не добавляется. На последнем этапе фрагменты помещаются в поля полезной нагрузки ячеек ATM.

Современные принципы создания МСС

Классические мультисервисные технологии, краткое описание которых приведено в первом разделе, внедрялись тяжело и долго. В меньшей степени сказанное относится к технологии Frame Relay, которая и не является мультисервисной технологией в обычном понимании. Это объясняется тем, что цикл разработки сложных технологий исторически не соответствовал темпам роста потребностей рынка телекоммуникаций. Поэтому получалось так, что замечательные технологии ISDN и ATM выходили на рынок уже морально устаревшими, а предлагаемые решения оказывались слишком дорогими. В этой ситуации повышенный интерес привлекают разнообразные неклассические технологии создания мультисервисных сетей доступа. Применение таких

технологий, как правило, позволяет создать мультисервисную сеть путем добавления дополнительных услуг к уже имеющимся в сети.

Гибридные сети широкополосного доступа

Появление и развитие гибридных сетей широкополосного доступа представляет собой типичный пример эволюционного развития технологий построения сетей доступа от узкоспециальных услуг к полнофункциональным услугам. Основной особенностью широкополосных сетей кабельного телевидения является их изначальное ориентирование на предоставление вещательных услуг. В спектре современных услуг классические теле- и радиовещание постепенно сдают свои позиции, поэтому инфраструктуры, которые применяются для их предоставления, могут быть достаточно успешно использованы для организации новых сервисов (доступ в сеть Интернет, цифровое видео).

Передача данных по сетям HFC

Первоначально сети широкополосного доступа применялись для трансляции программам кабельного телевидения. В качестве среды передачи данных в этих сетях использовался медный коаксиальный кабель, а телевизионный сигнал передавался по нему в аналоговом виде и в стандартном эфирном формате. Вещание кабельного телевидения в России, как правило, выполняется в диапазоне, который начинается с частот 2-го метрового диапазона (МВ или VHF-H): 134/174—230 МГц (1,72/2,24—1,3 м) и завершается частотами дециметрового диапазона — (ДМВ): 470—790 МГц (64—38 см). Трансляция сигнала одного телевизионного канала занимает полосу частот 8 МГц, поэтому оператор кабельного телевидения может организовать одновременную трансляцию от 20 до 80 телевизионных программ. Поскольку при распространении телевизионного сигнала на частотах свыше 300 МГц увеличивается его затухание, вносимое коаксиальным кабелем, то для увеличения дальности распространения этого сигнала в сетях кабельного телевидения использовались аналоговые усилители-регенераторы. В дальнейшем, с увеличением количества абонентов, для построения магистральных сегментов своих сетей операторы кабельного телевидения стали использовать волоконно-оптический кабель. При этом оптическая магистраль, как правило, использовалась для подключения к общей сети одной или нескольких связанных между собой коаксиальных ветвей. Преобразование сигнала, передаваемого из волоконно-оптического сегмента в коаксиальный сегмент, выполнялось стандартными конвертерами. Такие гибридные *волоконно-оптические/коаксиальные сети*, или иначе *сети HFC* (Hybrid-Fiber/Coax), оказались способны передавать телевизионный сигнал на расстояние до нескольких сотен километров.

В дальнейшем, по мере развития рынка и появления новых услуг и вследствие роста конкуренции со стороны провайдеров спутникового телевидения, операторы кабельного телевидения были вынуждены искать пути повышения качества предоставляемых услуг, а также возможности для организации новых сервисов для своих клиентов. В качестве таких новых услуг для абонентов сетей кабельного телевидения были представлены высокоскоростная передача данных и доступ в сеть Интернет. На рис. 1.4 представлена схема использования сети HCF для организации высокоскоростной передачи данных и доступа в сеть Интернет. Основными компонентами этой схемы являются:

- кабельные модемы — *CM* (Cable Modem);
- транслирующая станция кабельных модемов — *CMTS* (Cable Modem Termination System).

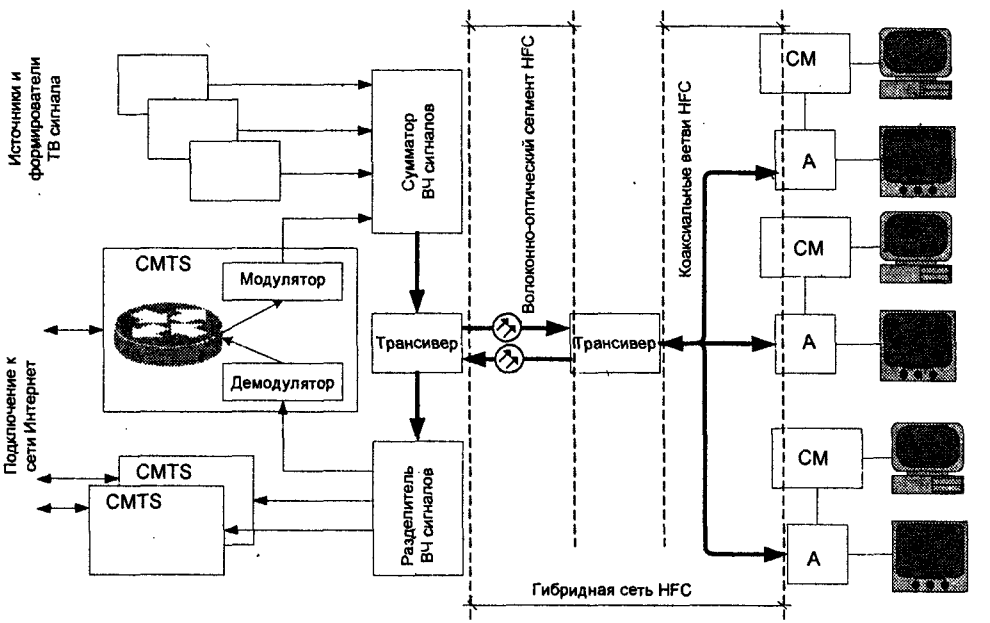


Рис. 1.4. Использование сети HFC для высокоскоростной передачи данных и доступа в сеть Интернет

Кабельные модемы в этой схеме используются для передачи и приема данных по специально выделенным частотным каналам сети кабельного телевидения, свободным от трансляции телевизионных программ. Стандартный кабельный модем снабжен двумя интерфейсами: один используется для подключения к сети кабельного телевидения, другой — для подключения к рабочей станции или к сегменту локальной сети абонента. Пассивные ответвители, помеченные буквой "A" на рис. 1.4, обеспечивают абоненту возмож-

ность одновременно просматривать телевизионные программы и использовать услугу высокоскоростного доступа в сеть Интернет.

Транслирующие станции кабельных модемов — CMTS обеспечивают:

- передачу данных в направлении абонента *(DOWNSTREAM)* в частотном формате сетей кабельного телевидения;
- прием передаваемых абонентом данных *(UPSTREAM)*;
- кодирование передаваемых данных;
- управление подключением абонентов — установление подлинности, подсчет принятого трафика.

Дополнительные проблемы оператору кабельного телевидения, решившему предоставлять услугу передачи данных, создает необходимость организации обратного канала. Поскольку сети кабельного ТВ изначально были однонаправленными и передавали сигнал только от оператора к абоненту, промежуточные усилители и формирователи, которые использовались на коаксиальном участке HFC, просто не были способны обеспечить передачу обратного сигнала. В тех случаях, когда передача обратного сигнала по сети HFC не могла быть обеспечена, оператор кабельного телевидения мог использовать гибридную схему, в которой для передачи *UPSTREAM*-сигнала использовался отдельный канал, например, модемное соединение по коммутируемой линии.

Спецификации DOCSIS

На начальном этапе для обеспечения передачи данных по сетям кабельного телевидения многие операторы использовали фирменные технологии, что существенно сдерживало развитие этого сектора услуг. Появление универсальной спецификации *DOCSIS* (Data-Over-Cable Service Interface Specifications) и последующее утверждение основных технических решений DOCSIS в рекомендациях ITU-T не только обеспечили требуемый уровень конкурентоспособности для услуги передачи данных, предоставляемой операторами кабельного телевидения, но и заложили основу для построения будущих интерактивных мультисервисных сетей HFC.

Основные технические характеристики, регламентирующие передачу данных в системах DOCSIS, изложены в спецификациях, подготовленных некоммерческими организациями CableLabs и CableNET. С момента начала разработок (1995) эти организации подготовили четыре версии спецификации DOCSIS, часть из которых была закреплена в рекомендациях ITU-T:

- DOCSIS v1.0 — ITU-T J.112 (03/98) "TRANSMISSION SYSTEMS FOR INTERACTIVE CABLE TELEVISION SERVICES";
- DOCSIS v1.1 — ITU-T J.112 (03/01) "TRANSMISSION SYSTEMS FOR INTERACTIVE CABLE TELEVISION SERVICES";

- DOCSIS v2.0 — ITU-T J.122 (12/02) "SECOND-GENERATION TRANSMISSION SYSTEMS FOR INTERACTIVE CABLE TELEVISION SERVICES — IP CABLE MODEMS";
- DOCSIS v3.0.

Передача данных по коаксиальному кабелю в прямом направлении (от CMTS к CM) выполняется на фиксированных каналах из частотного диапазона от 108 до 862 МГц (в Европе). Для модуляции передаваемого в прямом направлении сигнала применяются алгоритмы линейного кодирования *QAM-64* (размер символа 5 бит) и *QAM-256* (размер символа 7 бит), что позволяет при использовании одного телевизионного канала обеспечить информационную скорость до 55 Мбит/сек.

Для передачи данных в обратном направлении (от CM к CMTS) используется отдельный частотный диапазон (от 5 до 65 МГц), что позволяет вести информационный обмен между CM и CMTS в режиме полного дуплекса. Последние версии спецификации DOCSIS рекомендуют использовать для модуляции сигнала, передаваемого в обратном направлении, алгоритм линейного кодирования QAM-128 (размер символа 6 бит), при этом данные в обратном направлении могут передаваться со скоростью до 30 Мбит/сек.

Примечание

Увеличение пропускной способности обратного канала в спецификациях DOCSIS v1.1 и v2.0 было вызвано необходимостью обеспечить симметричный информационный обмен при использовании сетей кабельного телевидения для объединения локальных сетей удаленных офисов.

В табл. 1.3 приведен перечень основных документов, регламентирующих построение и организацию информационного взаимодействия в сетях КТВ, построенных с использованием технологии DOCSIS v1.1 и v2.0.

***Таблица 1.3.** Основные документы DOCSIS v1.0,v1.1 и v2.0*

DOCSIS 1.0	DOCSIS 1.1	DOCSIS 2.0	Назначение
SP-RFI	SP-RFI v1.1	SP-RFI v2.0	Описание высокочастотного интерфейса CM — Radio Frequency Interface Specification
SP-OSSI	SP-OSSI v1.1	SP-OSSI v2.0	Описание интерфейса управления компонентами сети — Operations Support System Interface Specification
SP-BPI	SP-BPI+	SP-BPI+	Описание способов управления доступом к ресурсам сети — Baseline Privacy Interface Specification
SP-CMCI			Описание интерфейса подключения к оборудованию абонента — Cable Modem to Customer Premises Equipment Interface Specification

Таблица 1.3 (окончание)

DOCSIS 1.0	DOCSIS 1.1	DOCSIS 2.0	Назначение
SP-CMTS-NSI			Описание интерфейса CMTS — Cable Modem Termination System Network Side Interface Specification

В табл. 1.4 приведен перечень основных документов, регламентирующих построение и организацию информационного взаимодействия в сетях, построенных с использованием технологии DOCSIS v3.0.

Таблица 1.4. Основные документы DOCSIS v3.0

Обозначение	Назначение
CM-SP-PHYv3.0	Описание высокочастотного интерфейса CM — Physical Layer Specification
CM-SP-MULPIv3.0	Описание принципа распределения ресурсов каналоа между приложениями — Media Access Control and Upper Layer Protocols Interface Specification
CM-SP-OSSIv3.0	Описание интерфейса упраалеиия компонентами сети — Operations Support System Interface Specification
CM-SP-SECv3.0	Описание способоа управления доступом к ресурсам сети Security Specification

В соответствии с требованиями спецификации DOCSIS сразу после включения кабельного модема он автоматически выполняет процедуру согласования параметров прямого и обратного канала с CMTS, состоящую из следующих этапов:

- поиска активного прямого (DOWNSTREAM) канала и установки режима синхронизации с CMTS — (Scanning and synchronization to downstream);
- приема от CMTS характеристик обратного канала — (Obtain upstream parameters);
- согласования параметров служебных и информационных потоков — (Ranging and automatic adjustments);
- определения класса устройства — (Device Class Identification);
- установки IP-соединения с CMTS — (Establish IP connectivity);
- установки календаря и системных часов на CM — (Establish time of day);
- приема актуальных параметров информационного обмена — (Transfer operational parameters);
- регистрации кабельного модема на CMTS — (Registration);

- установки параметров защиты информационного обмена — (Baseline Privacy Initialization).

На этапе поиска активного канала СМ выполняет сканирование частотного спектра, выделенного под прием прямого канала, для того чтобы обнаружить передачу от CMTS. Поиск передающей станции модем выполняет с учетом специфики кабельного вещания в данном регионе — с шагом на 6 или 8 МГц в Северной Америке и Европе соответственно. Обнаруженный прямой канал передачи от CMTS считается разрешенным к использованию в том случае, если все процедуры синхронизации принимаемых данных на кабельном модеме были успешно завершены. В противном случае модем выполняет поиск следующего прямого канала от CMTS.

После установки синхронизации принимаемых данных кабельный модем должен получить от CMTS параметры разрешенного к использованию обратного канала. Для передачи этих параметров CMTS периодически формирует сообщения с описанием характеристик этого канала — *UCD* (Upstream Channel Descriptor Message). В том случае, если кабельный модем не получит это сообщение в течение установленного временного интервала, СМ должен повторить этап поиска прямого канала.

Основное назначение действий, выполняемых на этапе согласования параметров служебных и информационных потоков, состоит в распределении между этими потоками пропускной способности прямого и обратного каналов. Это распределение выполняется с учетом необходимости обеспечения удаленного управления модемом от CMTS и индивидуальных требований конкретного абонентского приложения.

Для определения параметров IP-соединения на кабельном модеме используется стандартный механизм конфигурирования удаленного узла — протокол *DHCP* (Dynamic Host Configuration Protocol) — IETF RFC 2131.

Установка на кабельном модеме текущих значений календаря и системного времени также выполняется при помощи стандартного протокола сети Интернет — *NTP* (Network Time Protocol) — IETF RFC 868.

На следующем этапе кабельный модем должен принять от CMTS файл, который содержит рекомендованные к использованию значения параметров служебных и информационных потоков. Эти значения могут не совпадать с теми, которые были определены на предыдущих этапах и используются модемом в настоящее время. В таких случаях модем не должен передавать на CMTS согласующее сообщение, и процедура согласования должна быть продолжена.

На последующих этапах модем выполняет действия, которые обеспечивают его идентификацию на CMTS и, при необходимости, информационную защиту передаваемых через него данных.

Универсальный шлюз DOCSIS

Следующим логичным шагом создателей спецификации DOCSIS явилась разработка концепции универсального шлюза — *DSG* (DOCSIS Set-top Gateway), который обеспечивал предоставление абоненту кабельной сети не только доступа в сеть Интернет, но и множества новых дополнительных услуг. На рис. 1.5 приведены варианты схем подключения абонентов к сети кабельного телевидения (КТВ) после внедрения спецификации DOCSIS.

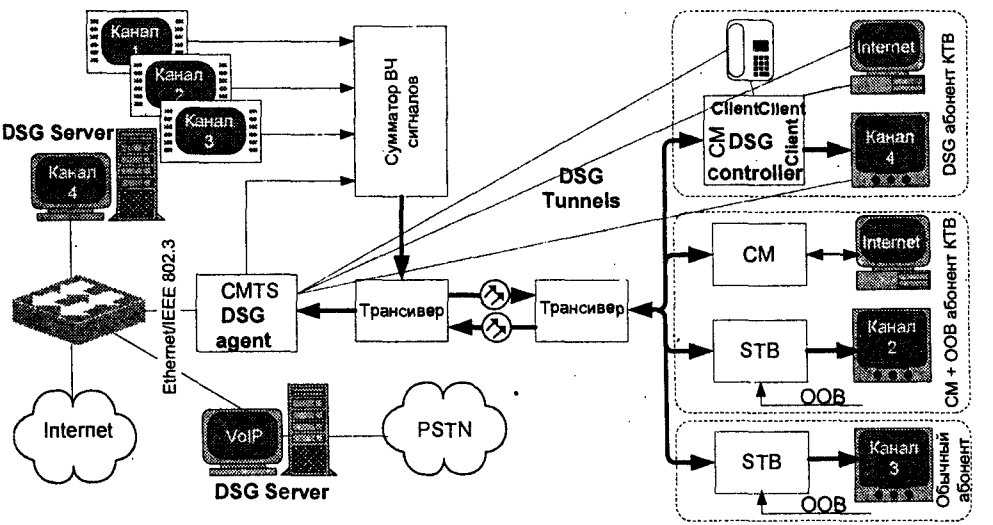


Рис. 1.5. Схемы подключения абонентов к сети кабельного телевидения

Для подключения стандартного телевизионного приемника к сети КТВ обычно используется специальная приставка — *STB* (Set-Top-Box). Приставка обеспечивает двунаправленный информационный обмен сообщениями с узлом предоставления услуг КТВ по выделенному частотному каналу — *OOB* (Out-Of-Band) для выполнения следующих функций:

- управления декодированием телевизионного сигнала, защищенного от несанкционированного доступа;
- приема информации о программах кабельного телевидения — *EPG* (Electronic Program Guide);
- приема и передачи сообщений о чрезвычайных ситуациях — *EAS* (Emergency Alert System).

Для изготовления этих приставок применялись, как правило, нестандартные фирменные технологии производителей оборудования, что существенно по-

вышало стоимость реализации технических решений, усложняло эксплуатацию оборудования и делало практически невозможным дальнейшее развитие сети.

Внедрение спецификации DSG в сеть кабельного телевидения (КТВ) позволяет успешно решить все проблемы, связанные с использованием нестандартного оборудования, и обеспечивает реализацию надежного служебного обмена между оборудованием абонента и серверами приложений оператора КТВ на основе интернет-технологий.

Принципы построения сети КТВ с использованием решений DSG описаны в спецификации интерфейса CM-SP-DSG — ("DOCSIS Set-top Gateway (DSG) Interface Specification"). В соответствии с требованиями этой спецификации, основными компонентами DSG-сети КТВ являются:

- *DSG Server* — представляет собой сервер абонентского приложения или любое другое сетевое устройство, предназначенное для передачи трафика клиенту через туннельное соединение (DSG Tunnel);
- *DSG Client* — принимает трафик, направляемый ему сервером. В состав DSG-шлюза может входить несколько клиентов;
- *DSG Agent* — реализует протокол DSG на промежуточном узле — CMTS. Агент обеспечивает построение DSG-туннеля и передачу по нему трафика в направлении клиента;
- *DSG Client Controller* — часть абонентской приставки, которая обрабатывает управляющие сообщения протокола DSG;
- *DSG Tunnel* — поток пакетов, передаваемых от CMTS в направлении DSG-клиента. В зависимости от используемого режима, туннели могут передавать данные по схемам "один — одному" (режим IP UNICAST) или "один — группе" (режим IP MULTICAST).

Примечание

Более подробно о режимах адресации, используемых в сети Интернет, рассказывается в *главе 6* настоящего издания.

На схеме, представленной на рис. 1.5, функции "DSG Server" выполняют серверы абонентских приложений — шлюз VoIP и IP-ретранслятор телевизионных программ канала 1. Транслирующая станция кабельных модемов CMTS выполняет функции посредника "DSG Agent" и формирует туннели для передачи трафика абонентских приложений по сети кабельного телевидения. Размещаемый у абонента КТВ универсальный шлюз DSG представляет собой коммуникационное устройство, основной частью которого является кабельный модем DOCSIS. Различные абонентские терминалы, подключаемые к этому устройству: телевизионный приемник, телефон, персональный компь-

ютер, позволяют абоненту сети КТВ принимать трафик различных служб от серверов кабельного оператора.

Таким образом, использование рекомендаций DSG при построении сети КТВ по технологии DOCSIS обеспечивает возможность создания гибридной мультисервисной сети. При этом перевод абонентов КТВ на новую схему предоставления услуг может быть выполнен постепенно, по мере приобретения ими соответствующего оборудования.

Следует, однако, отметить, что сосуществование различных схем предоставления услуг в единой сети HFC существенно повышает требования к частотным характеристикам линий на оконечном — коаксиальном участке, поскольку для передачи трафика по новой схеме в этом случае должны быть использованы более высокочастотные каналы. Это может существенно замедлить процесс внедрения новых услуг в многоэтажных зданиях с разветвленной и изношенной кабельной инфраструктурой.

Сети беспроводного доступа

Долгое время технологии беспроводного доступа использовались преимущественно для подключения мобильных абонентов к ресурсам локальной вычислительной сети (ЛВС) или сетей общего пользования. Первые технологии беспроводной передачи данных, получившие неофициальное наименование *Wi-Fi* (Wireless Fidelity), обеспечивали передачу данных на скорости несколько десятков мегабит в секунду на расстояния до 100 м. Новый этап в развитии беспроводных технологий передачи данных совпал с периодом резкого повышения спроса на мультисервисные услуги. Мобильность и быстрая окупаемость увеличивают конкурентоспособность беспроводных решений при построении мультисервисных сетей и делают их, несомненно, очень привлекательными для операторов связи.

Спецификации IEEE 802.11 (Wi-Fi)

Система мобильного доступа обычно имеет в своем составе одну или несколько *точек доступа — AP* (Access Point), к которым по радиоканалу подключались *мобильные станции — MS* (Mobile Station). Все точки доступа имели прямое подключение у локальной сети и при необходимости обеспечивали роуминг для подвижных абонентов. Если мобильная станция находилась в зоне действия хотя бы одной точки доступа, то эта станция могла обмениваться данными с любым из абонентов ЛВС.

Основные принципы построения подобных систем изложены в спецификациях комитета IEEE 802.11 Part 11: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". В табл. 1.5 приведены основ-

ные характеристики наиболее популярных технологий беспроводного доступа, разработанных комитетом IEEE 802.11.

Таблица 1.5. Популярные технологии беспроводного доступа IEEE 802.11

Обозначение спецификации	Диапазон рабочих частот (ГГц)	Предельное значение информационной скорости (Мбит/сек)	Схема модуляции сигнала
IEEE 802.11g	2,3—2,7	54	OFDM
IEEE 802.11b	2,3—2,55	11	DSSS
IEEE 802.11 a	5,1—6,1	54	OFDM

Формирование частотного спектра передаваемого сигнала согласно стандарта IEEE 802.11 осуществляется при помощи двух различных схем модуляции DSSS и OFDM.

Модуляционная *схема прямого расширения спектра — DSSS* (Direct Sequence Spread Spectrum) использовалась только в ранних версиях спецификаций IEEE 802.11. В современных технологиях беспроводного доступа для формирования частотного спектра передаваемого сигнала применяется *схема ортогонального частотного мультиплексирования — OFDM* (Orthogonal Frequency Division Multiplexing), при этом для передачи трафика одного абонентского канала используется частотный диапазон шириной 20 МГц. Использование OFDM обеспечивает уменьшение взаимного влияния сигналов, передаваемых по разным каналам, и позволяет существенно уменьшить затухание сигнала в радиоканале. Значения информационных скоростей, приведенные в третьем столбце таблицы, могут быть достигнуты при наличии только одного абонента у точки доступа.

Применение технологий IEEE 802.11 в среднем обеспечивает распространение сигнала в помещении на дальность порядка 100 м, при этом ЭИИМ (эффективная изотропно-излучаемая мощность) АР не превышает 100 мВт. Использование направленных антенн и антенных усилителей высокочастотного сигнала позволяют существенно увеличить дальность распространения сигнала — зону покрытия точки доступа. Это, в частности, делает возможным применение технологий IEEE 802.11 для создания радиомостов между сегментами ЛВС. Следует, однако, отметить, что такие мосты не всегда могут обеспечить ту скорость, которая требуется для информационного обмена между сегментами современных ЛВС. Недостаточная пропускная способность и отсутствие гарантий обслуживания делает практически невозможным построение мультисервисных сетей на основе технологии IEEE 802.11.

Спецификации IEEE 802.16 WiMAX

Многие технические решения, апробированные в технологиях IEEE 802.11, были положены в основу нового технологического комплекса организации беспроводной связи, который получил неофициальное наименование *WiMAX* (Worldwide Interoperability for Microwave Access). Базовая спецификация, подготовленная комитетом IEEE 802.16, определяет общие принципы построения мобильных и стационарных систем беспроводного доступа ("Air Interface for Fixed and Mobile Broadband Wireless Access Systems"). В соответствии с положениями этой спецификации система беспроводного доступа включает в себя *базовую станцию — BS* (Base Station), к которой по радиоканалам подключается одна или несколько *абонентских станций — SS* (Subscriber Station). На рис. 1.6 приведена схема использования беспроводных технологий для обеспечения служебной и коммерческой связи.

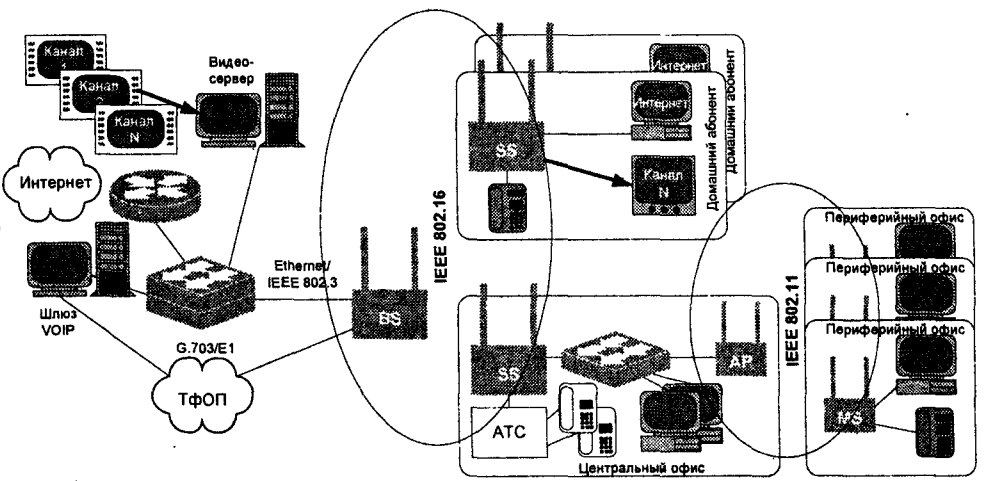


Рис. 1.6. Применение беспроводных технологий для организации служебной и коммерческой связи

На приведенной схеме технология IEEE 802.16 применяется для организации доступа к услугам сервис-провайдера. Беспроводные каналы в данном случае используются как для обеспечения доступа в сети общего пользования (Интернет и ТфОП), так и для получения услуг от сервис-провайдера. В рамках общего стандарта IEEE 802.16 были разработаны пять вариантов спецификации беспроводного интерфейса, в которых применяются различные принципы формирования радиочастотного канала. В табл. 1.6 приведен перечень спецификаций радиочастотного интерфейса стандарта IEEE 802.16.

В спецификациях WirelessMAN-SC и WirelessMAN-SCA для построения радиочастотного канала передачи данных используется одночастотный метод —

SC (Single-Carrier). В спецификациях WirelessMAN-OFDM и WirelessMAN-OFDMA предусматривается использование технологии ортогонального частотного мультиплексирования OFDM для создания высокочастотных каналов передачи данных. Ширина полосы пропускания, занимаемая одним абонентским каналом в общем спектре передаваемого сигнала в соответствии с требованиями стандарта IEEE 802.16, может меняться в диапазоне от 2,0 до 20 МГц, что существенно повышает эффективность использования частотного ресурса. Применение дополнительных алгоритмов линейного кодирования QAM-16 и QAM-64 позволяет при этом обеспечить передачу данных на скорости свыше 100 Мбит/сек на расстояние более 1 000 м. Технологии WirelessMAN-OFDMA и WirelessMAN-SCA предназначены для организации систем множественного доступа. Режим двунаправленного (full-duplex) обмена между базовой станцией и абонентскими станциями обеспечивается благодаря применению методов временного разделения — *TDD* (Time Division Duplex) или частотного разделения — *FDD* (Frequency Division Duplex).

Таблица 1.6. *Спецификации радиочастотного интерфейса IEEE 802.16*

Обозначение спецификации	Диапазон рабочих частот	Обеспечение full-duplex
WirelessMAN-SC	10—66 ГГц	TDD / FDD
WirelessMAN-SCA	Ниже 11 ГГц (лицензируемый диапазон)	TDD / FDD
WirelessMAN-OFDM	Ниже 11 ГГц (лицензируемый диапазон)	TDD / FDD
WirelessMAN-OFDMA	Ниже 11 ГГц (лицензируемый диапазон)	TDD / FDD
WirelessHUMAN	2400—2483,5 МГц и 5725—5875 МГц	TDD

Интеграция разнородного трафика в сетях WiMAX

Большая дистанция уверенного приема сигнала и широкая полоса пропускания канала, безусловно, делают весьма привлекательным использование систем беспроводного доступа WirelessMAN-OFDMA для построения городских мультисервисных сетей.

Основные принципы организации мультисервисных систем множественного доступа и многие технические решения IEEE 802.16 во многом совпадают с теми, которые используются в технологическом комплексе DOCSIS. Это совпадение не является случайным, поскольку обе технологии предназначены для передачи сигналов по средам с множественным доступом абонентов. В гибридных сетях DOCSIS такой средой является коаксиальный сегмент HFC, в беспроводных сетях аналогичные функции выполняет выделенный радиочастотный диапазон. В обоих случаях выделение частотного ресурса

для создания канала передачи данных выполняется центральным узлом (CMTS или BS) по запросу абонентской станции (CM или SS).

Для выделения этого ресурса центральная станция учитывает специфику обслуживания конкретной абонентской станции и тип запрашиваемой услуги. При организации канала для доступа в Интернет, например, пропускная способность канала, направленного от базовой станции к абонентской станции, обычно в несколько раз превышает ширину обратного канала. Для обслуживания телефонного вызова, однако, должны использоваться симметричные каналы с гарантированной пропускной способностью. Для обеспечения возможности управления качеством обслуживания в сетях, построенных с использованием технологий IEEE 802.16, трафик, передаваемый по радиоканалам, делится на классы, для каждого из которых устанавливаются стандартные критерии качества обслуживания.

В табл. 1.7 приведены характеристики различных типов трафика, определенные в спецификациях IEEE 802.16:

- обслуживание с гарантированной пропускной способностью — тип трафика *UGS* (Unsolicited Grant Service);
- обслуживание с гарантированным временем отклика — тип трафика *rtPS* (real-time Polling Service);
- обслуживание с негарантированным временем отклика — тип трафика *nrtPS* (non-real-time Polling Service);
- обслуживание без гарантий — тип трафика *BE* (Best Effort).

Таблица 1.7. *Характеристики типов трафика IEEE 802.16*

Тип трафика	Абонентское приложение	Обеспечение качества обслуживания и full-duplex
UGS	Услуги, предоставляемые в реальном масштабе времени. Фиксированный размер передаваемого блока. (Оцифрованный телефонный трафик)	Базовая станция (BS) назначает приложению фиксировввнные интервалы для передачи данных фиксированным периодом
RtPS	Услуги, предоставляемые в реальном масштабе времени. Переменный размер передаваемого блокв. (Оцифрованный видеотрвфик)	Базовая станция (BS) назначает приложению запрвшиваемые интервалы для передачи данных с фиксированным периодом
NrtPS	Передвчв файлов	Бвзоввя станция (BS) выделяет ресурс по запросу для передвчи двнных
BE	Передвчв сообщений e-Mвil, отображение документов WWW	Нв общих основвниях

Обеспечение требуемого уровня качества обслуживания начинается с запроса нового сервиса от абонентской станции и состоит из следующих этапов:

- поиска канала BS и организации соединения;
- согласования ключевых параметров и определения класса устройства;
- определения параметров и установке IP-соединения с BS;
- получения конфигурационного файла по протоколу TFTP;
- регистрации абонентского приложения на базовой станции.

Таким образом, при создании абонентского канала IEEE 802.16 одновременно решаются основные задачи, необходимые для успешного функционирования мультисервисной сети — управление доступом абонентов и обеспечение качества их обслуживания. Безопасность информационного обмена гарантируется применением дополнительного шифрования всех передаваемых блоков данных с использованием специального *протокола управления ключами — PKM* (Key Management Protocol).

К основным достоинствам, которые присущи беспроводным технологиям, следует отнести возможность быстрого развертывания, мобильность, относительно невысокую стоимость построения и эксплуатации.

Основные недостатки технологий беспроводного доступа определяются особенностями используемой среды передачи данных, разделяемой между многими абонентами. К таким недостаткам, в первую очередь, относятся резкое уменьшение скорости доступа при увеличении количества абонентов или при воздействии радиочастотных помех (IEEE 802.11) а также необходимость приобретения разрешительных документов на право использования частотного диапазона (IEEE 802.11 — WirelessMAN-SCA, WirelessMAN-OFDM, WirelessMAN-OFDMA).

Мультисервисные ЛВС на основе Ethernet-технологий

Долгое время Ethernet не рассматривался в качестве технологии передачи мультисервисного трафика. Это объяснялось разными причинами, но все они являлись следствием того бесспорного факта, что технология Ethernet изначально не имела ни одного из обязательных признаков мультисервисных технологий, поскольку была разработана для обеспечения конкурентного доступа абонентов к разделяемой среде передачи данных. Например, спецификация 10Base2 Ethernet обеспечивала передачу данных со скоростью до 10 Мбит/сек в полудуплексном режиме и имела непрогнозируемое (из-за возникновения коллизий при передаче) время доставки блока данных. В первоначальном варианте кадра Ethernet отсутствовало поле для указания необходимого уровня обслуживания, поскольку инструментов для реализации этого

требования в первых версиях Ethernet просто не было и не могло быть. Однако, по мере развития и роста популярности, Ethernet постепенно приобрел все недостающие признаки мультисервисной технологии. Вследствие перехода от разделяемой к выделенной среде передачи данных — (сначала витая пара, а потом волоконно-оптический кабель) в сетях Ethernet появился полнодуплексный режим, скорость передачи данных при этом увеличилась в 1 000 раз. Постоянно растущие темпы производства компонентов сетей Ethernet вызвали резкое снижение их стоимости, что повысило привлекательность этих компонентов для потребителя. Все это в совокупности делает Ethernet одной из наиболее перспективных технологий доставки мультисервисного трафика.

Применение волоконно-оптических линий связи в сетях доступа

Внедрение *волоконно-оптических линий связи* (ВОЛС) в технологии передачи данных произошло достаточно давно, и поэтому подавляющее большинство современных магистральных каналов являются волоконно-оптическими. Характерными особенностями передачи данных по ВОЛС являются:

- *широкая полоса пропускания сигнала* — по волоконно-оптическому кабелю данные могут передаваться в диапазоне частот от единиц герц до тысяч мегагерц;
- *нечувствительность к электромагнитным помехам* — сигнал, передаваемый по волоконно-оптическому кабелю, сам не создает электромагнитных помех и не подвержен их воздействию;
- *малый уровень ослабления сигнала* — потери, вносимые при распространении сигнала по волоконно-оптическому кабелю, соизмеримы с теми, которые сигнал испытывает при эфирном распространении.

Таким образом, волоконно-оптический кабель является практически идеальной средой передачи данных, поэтому необходимость его использования при построении перспективных мультисервисных сетей доступа не может быть поставлена под сомнение.

Вместе с тем очевидно, что применение классических технологий построения оптических магистралей для создания сетей доступа невозможно, поскольку это неминуемо приведет к неприемлемому повышению цены технического решения. С другой стороны, способность оптического кабеля передавать высокочастотный сигнал на десятки километров без использования регенераторов позволяет строить оптические сети, не содержащие активных (потребляющих электрическую энергию) компонентов. Сети абонентского доступа в этом случае могут быть построены по одной из двух возможных схем:

- *схеме пассивных оптических сетей* — *PON* (Passive Optical Networks);
- *схеме сквозных каналов от точки до точки* — *PTP* (Point to Point).

Сети доступа, построенные по схеме PTP, предполагают наличие прямого волоконно-оптического соединения от оптического терминала центрального офиса — *OLT* (Optical Line Terminal) до каждого абонентского терминала — *ONU* (Optical Network Unit). Сети, построенные по этой схеме, принято называть *полностью-оптическими сетями Ethernet — AOEN* (All-Optical Ethernet Networks). Применение схемы PTP теоретически позволяет предоставить абоненту полосу пропускания до нескольких гигагерц, однако при этом существенно возрастает стоимость построения и обслуживания кабельной инфраструктуры и увеличивается период окупаемости капитальных вложений.

Сети доступа PON строятся с применением пассивных оптических разделителей (optical splitter) мощности сигнала, передаваемого по волоконно-оптическому кабелю. Такие оптические разделители позволяют использовать одно магистральное волокно для передачи сигнала по нескольким направлениям, что существенно снижает стоимость построения сети и позволяет реализовать групповые режимы информационного обмена (вещание по схеме "один — группе").

Пассивные оптические сети — PON

Внедрение пассивных участков ВОЛС при построении сетей доступа может быть выполнено по следующим технологическим схемам:

- *Волокно до абонента* — схема *FTTH* (Fiber-To-The-Home);
- *Волокно до здания* — схема *FTTB* (Fiber-To-The-Building);
- *Волокно до шкафа* — схема *FTTC* (Fiber-To-The-Curb);
- *Волокно до узла* — схема *FTTN* (Fiber-To-The-Node).

Схема FTTH предполагает применение только волоконно-оптических каналов и может быть реализована с использованием принципов PON (Passive Optical Networks). В последнем случае пассивные разделители-сплиттеры монтируются на промежуточном узле таким образом, что к каждому магистральному волокну подключается до 32 абонентских волокон. Использование этой схемы обеспечивает информационный обмен со скоростью 80—100 Мбит/сек на расстоянии до нескольких километров.

Основной особенностью схемы FTTB является то, что волоконно-оптический кабель в этом случае используется только на магистральном участке, а подключение абонентов выполняется при помощи соединений по выделенным медным линиям. Передача сигнала на магистральном участке волоконно-оптического кабеля в данном случае выполняется по схеме PTP — для каждого здания при этом используется выделенная линия.

Схемы FTTC и FTTN могут быть использованы для подключения разрозненных абонентов на расстоянии до центрального офиса или точки предоставле-

ния услуги. Схема FTTN обеспечивает подключение большего числа абонентов, поскольку предполагает установку удаленного терминала на промежуточном узле. В обоих случаях для передачи сигнала на магистральном участке используется схема PTP, а подключение абонентов выполняется по существующей медной кабельной инфраструктуре.

В настоящее время для передачи данных по пассивным оптическим сетям могут быть использованы различные технологии. Первоначально разработка технологий абонентского доступа с использованием пассивных ВОЛС проводилась в рамках проекта полнофункциональных сетей доступа — *FSAN* (Full Service Access Network). В качестве базовой технологии при построении такой сети предполагалось использовать ATM, поэтому первая спецификация этой технологии получила неформальное обозначение — *APON* (ATM PON). В дальнейшем эта технология неоднократно дорабатывалась, в нее добавилась поддержка новых услуг и, в уже измененном виде, она была закреплена в рекомендации ITU-T G.983 "BROADBAND OPTICAL ACCESS SYSTEMS BASED ON PASSIVE OPTICAL NETWORKS (PON)". Определенная таким образом технология пассивных широкополосных сетей — *A/BPON* (ATM/Broadband Passive Optical Networks) могла быть использована для построения мультисервисных сетей доступа, обеспечивающих передачу данных со скоростью до 622 Мбит/сек на расстояние до 20 км по одному оптическому волокну. Однако вскоре широкое внедрение в локальных сетях технологии IEEE 802.3 1000BaseX привело к необходимости кардинального преобразования спецификации. В окончательном варианте, который был закреплен в рекомендации ITU-T G.984 "GIGABIT-CAPABLE PASSIVE OPTICAL NETWORKS (GPON)", пассивные оптические сети поддерживают подключение сегментов высокоскоростных ЛВС и обеспечивают передачу данных со скоростью 2500 Мбит/сек на расстояние до 20 км. Основные технические характеристики технологий BPON (Broadband Passive Optical Networks) и GPON (Gigabit-capable Passive Optical Networks) приведены в табл. 1.8.

Таблица 1.8. *Технические характеристики BPON и GPON*

Характеристика	BPON	GPON
Определение спецификации	ITU-T G.983	ITU-T G.984
Максимальная скорость прямого (UPSTREAM) потока	622 Мбит/сек	2500 Мбит/сек
Максимальная скорость обратного (DOWNSTREAM) потока	155 Мбит/сек	2500 Мбит/сек
Длина волны передатчика прямого потока (аналоговое видео)	1550 нм	1550 нм
Длина волны передатчика дополнительного прямого потока (передача данных)	1490 нм	1490 нм

Таблица 1.8 (окончание)

Характеристика	BPON	GPON
Длина волны передатчика обратного потока	1310 нм	1310 нм
Максимальное число подключаемых абонентов	32	64
Поддерживаемые интерфейсы	ATM	ATM, IEEE 802.3

Спецификация EPON

Разработка спецификации Ethernet по пассивной оптической сети — *EPON* (Ethernet over Passive Optical Networks) проводилась в рамках проекта *EFM* (Ethernet In The First Mile). Необходимость разработки отдельной спецификации для передачи кадров Ethernet по пассивным оптическим сетям объяснялась высокой стоимостью и недостаточной эффективностью использования пропускной способности канала у существующих ATM-PON-технологий. Основными задачами, которые решали разработчики спецификации EPON, были:

- обеспечение симметричного полнодуплексного обмена по одному волокну оптического кабеля;
- разрешение коллизий при обращении к обратному каналу;
- интеграция трафика TDM (Time Division Multiplexing) в поток кадров Ethernet.

Первые две из поставленных задач не являются специфическими для EPON и поэтому решаются стандартным для технологий xPON образом — путем применения частотного разделения трафика, передаваемого в прямом и обратном каналах, и использования режима запросов при обращении к обратному каналу.

Примечание

Примерно такие же методы используются для аналогичных целей в технологиях DOCSIS и WiMAX.

Специфические особенности организации информационного обмена в сети Ethernet, построенной с использованием пассивных оптических компонентов, отражены в действующей редакции стандарта IEEE 802.3 "LAN/MAN CSMA/CD Access Method" — Раздел 64 — "Multipoint MAC Control". В этой спецификации определяется понятие многоточечного соединения Ethernet — *P2MP* (Point-To-Multipoint) и формулируются основные принципы реализации протокола управления многоточечным соединением Ethernet — протокола *MPCP* (Multipoint Control Protocol).

Протокол MPCP определяет дополнительные процедуры управления доступом к многоточечной среде передачи данных, с тем чтобы обеспечить:

- эмуляцию обычного прямого соединения Ethernet — *P2PE* (Point-to-Point Emulation) для каждого из абонентов, подключенных к сети с использованием технологии EPON;
- управление полосой пропускания обратного канала по запросам абонентов EPON.

Специфика пассивной среды EPON заключается в том, что только один абонентский блок ONU (Optical Network Unit) может передавать данные, поскольку все ONU могут использовать только один обратный канал до оптического терминала ONT(Optical Network Terminal). Разделение ресурсов обратного канала между ONU выполняется ONT по запросам от оконечных устройств по принципу разделения времени — *TDM* (Time Division Multiplexing). Для реализации этого разделения между ONT и каждым ONU устанавливается взаимная синхронизация, которая обеспечивает динамическое измерение задержки распространения сигнала с точностью 16 нс.

Протокол MPCP обеспечивает выполнение следующих функций:

- поиск и регистрация ONU *(Discovery Processing)*;
- запрос полосы пропускания обратного канала *(Report Processing)*;
- выделение полосы пропускания обратного канала *(Gate Processing)*.

Поиск и регистрация используются для подключения к сети EPON нового абонентского устройства ONU. Для выполнения этой функции OLT (Optical Line Terminal) формирует в обратном канале специальные запросные интервалы, свободные от передачи данных. В течение этого интервала вновь включенное устройство может направить OLT асинхронное сообщение "Запрос регистрации" — REGISTER_REQ. В том случае если несколько абонентов одновременно сформируют запрос регистрации, то на обратном канале произойдет коллизия, и все переданные запросы будут потеряны. Для предотвращения возникновения повторных коллизий каждый из OLT, который зафиксировал потерю запроса, может повторить его передачу только по истечении случайно выбранного интервала времени.

Для запроса полосы пропускания обратного канала каждое абонентское устройство ONU периодически направляет OLT сообщения REPORT, в которых содержится информация о состоянии процессов, ожидающих отправки данных. Такие сообщения должны быть сформированы даже в том случае, если очередь на отправку из данного ONU не содержит ни одного процесса.

Выделение полосы пропускания обратного канала осуществляется при помощи сообщений GATE, которые формируются OLT для управления передающими устройствами ONU. Ресурс обратного канала выделяется абонентскому

устройству в виде пакета параметров, определяющих передачу данных одним абонентским приложением. Этот пакет, для обозначения которого в спецификации IEEE 802.3 используется слово "grant", содержит, в частности, моменты времени, в которые должен быть включен и выключен передающий лазер на ONU.

Значения основных технических характеристик технологии EPON — длина волны излучателей прямого и обратного потока, наличие и размер окна в обратном потоке для трансляции аналогового телевидения — полностью соответствуют значениям, установленным для существующих технологий PON. Это обеспечивает возможность применения однотипного оборудования и облегчает процесс модернизации.

В табл. 1.9 приведены эксплуатационные параметры сетей, построенных с использованием технологий EPON класса A и B. Класс сети PON в данном случае определяется величиной бюджета оптической линии.

***Таблица 1.9.** Эксплуатационные параметры EPON*

Характеристика	Класс A	Класс B
Максимальная скорость прямого (UPSTREAM) потока (Мбит/сек)	1000	1000
Максимальная скорость обратного (DOWNSTREAM) потока (Мбит/сек)	1000	1000
Бюджет оптической линии — прямой/обратный поток (дБ)	21/23	26/26
Количестао аетаей PON	16	32
Максимальная дистанция OLT — ONU (км)	10	20

На рис. 1.7 приведена схема построения мультисервисной сети абонентского доступа с использованием спецификации EPON. В данном случае для подключения шести абонентов используются два уровня делителей мощности оптического сигнала 1/4.

На приведенной схеме домашние абоненты получают по сети EPON услуги доступа в сеть Интернет, IP-телефонии и аналоговое видео. Абоненты центрального офиса используют EPON для информационного обмена с периферийными офисами и для выхода в телефонную сеть общего назначения — *PSTN* (Public Switching Telephone Network).

Таким образом, применение спецификации EPON позволяет создавать относительно недорогие мультисервисные сети на основе технологии Ethernet. Применение пассивной оптической среды в данном случае позволяет получить дополнительные преимущества, поскольку схема передачи трафика P2MP идеально согласуется с концепцией группового (Multicast) обмена в

сетях Ethernet/Интернет. Все это позволяет технологии EPON сочетать в себе главные достоинства как сети, основанной на разделяемой среде передачи данных, так и сети, построенной на выделенной среде передачи данных.

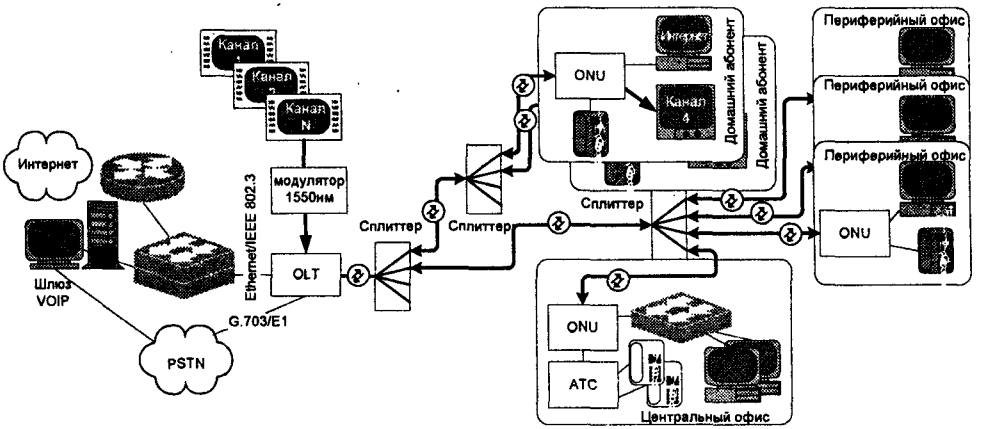
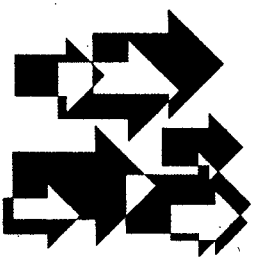


Рис. 1.7. Схема мультисерайсной сети абонентского доступа на основе спецификации EPON

ГЛАВА 2



Голосовые приложения мультисервисных сетей

Звук и голосовой сигнал до последнего времени являлись основными, а в некоторых случаях — единственными способами информационного обмена в человеческом обществе. Несмотря на то, что появление телевидения и глобальных сетей существенно изменили эту ситуацию, влияние телефонной и оперативной голосовой связи на все сферы деятельности человека ничуть не уменьшилось. Наоборот, именно развитие телекоммуникационных технологий, появление новых путей и способов передачи данных позволяет улучшать качество, реализовывать новые функции телефонной связи, что делает ее одним из основных компонентов современных мультисервисных сетей.

В первом разделе данной главы рассматриваются основные принципы и способы преобразования голосового сигнала, которые выполняются для передачи телефонного трафика по сети с коммутацией пакетов.

Второй раздел посвящен рассмотрению принципов и способов построения современных сетей пакетной телефонии. В этом разделе рассматриваются основные компоненты, которые используются для построения таких систем, и наиболее популярные их приложения.

Способы преобразования голосового сигнала

Построение современных мультисервисных сетей началось именно с решения задачи интеграции телефонного трафика и трафика сети передачи данных. Для того чтобы успешно интегрировать голосовой сигнал в мультисервисную сеть, телефонный трафик должен пройти несколько стадий последовательного преобразования:

- квантование;
- кодирование;

- сжатие;
- упаковка в пакеты.

Сложность этих преобразований заключается в том, что на каждом из перечисленных этапов должны быть учтены не только результаты всех предыдущих этапов, но и характерные особенности исходного речевого сигнала.

Принципы построения кодирующих устройств

Голос является по своей сути непрерывно изменяющимся во времени аналоговым сигналом. Ограниченность частотного диапазона этого сигнала определяется, с одной стороны, ограниченными возможностями органов речи, а с другой — органов слуха человека. Вместе с тем голос и речь каждого человека имеют индивидуальные особенности, которые не должны изменяться в процессе преобразования сигнала. Задачей современных алгоритмов кодирования является изменение формы представления телефонного сигнала таким образом, чтобы обеспечить его передачу по сети с коммутацией пакета без ущерба для качества.

Особенности голосового сигнала

Несмотря на то, что диапазон воспринимаемых человеком звуковых частот находится в интервале между десятками герц и десятками килогерц, в нормальной человеческой речи обычно не встречаются частоты, выходящие за пределы диапазона 300—3400 Гц. Каналы, обеспечивающие передачу аналогового сигнала этого диапазона, назывались каналами тональной частоты и использовались в системах аналоговой телефонии для организации международных и междугородних телефонных разговоров. Возникающее при передаче на большое расстояние ослабление голосового сигнала в этом канале компенсировалось при помощи аналоговых усилителей. При этом на каждом каскаде усиления одновременно усиливался и шум, действующий на сигнал, и, соответственно, необратимо ухудшалась различимость голосового сигнала на фоне шума канала, определяемая *соотношением сигнал/шум — SNR* (Signal/Noise Ratio).

Основная проблема, возникающая при передаче голосового сигнала в аналоговом виде, заключается в невозможности разделения шума и полезного сигнала в канале, поскольку обе этих составляющих являются одинаково непредсказуемыми для приемника сигнала. Единственным способом, который гарантированно позволяет скомпенсировать воздействие шума, является нормирование — ограничение количества возможных состояний передаваемого сигнала. В случае если расстояние между разрешенными уровнями нормированного сигнала превышает уровень шума в канале, то этот сигнал может быть полностью восстановлен.

Первые цифровые сети были разработаны для того, чтобы обеспечить передачу телефонного трафика по высокоскоростным цифровым магистральным каналам. Преимущества передачи голосового трафика в цифровом виде очевидны: обеспечивается большая достоверность передачи информации, цифровое оборудование является более дешевым и простым в эксплуатации. Кроме того, передача информации в цифровом виде свободна от многих недостатков, которые свойственны аналоговым системам передачи, и, в частности, от основного — ослабления сигнала в канале с многочисленными переприемами. Чем больше аналоговых компонентов входит в канал, тем хуже будет соотношение сигнал/шум у получателя информации. Для цифровых каналов это правило не действует, оцифрованный сигнал одинаково хорошо распространяется на любые, сколь угодно большие расстояния.

На рис. 2.1 приведены функциональные схемы передачи голосового сигнала по аналоговому и цифровому каналам. Схема, представленная на рис. 2.1, *а*, показывает последовательность преобразования голосового сигнала при его передаче по аналоговым каналам с использованием аппаратуры частотного уплотнения. Шум, действующий на сигнал, в этом случае не может быть скомпенсирован и присутствует в принятом сигнале. На схеме, представленной на рис. 2.1, *б*, показаны этапы преобразования голосового сигнала для его отправки по цифровым каналам передачи данных с использованием принципов *импульсно-кодовой модуляции* — *ИКМ*, или иначе *PCM* (Pulse Code Modulation).

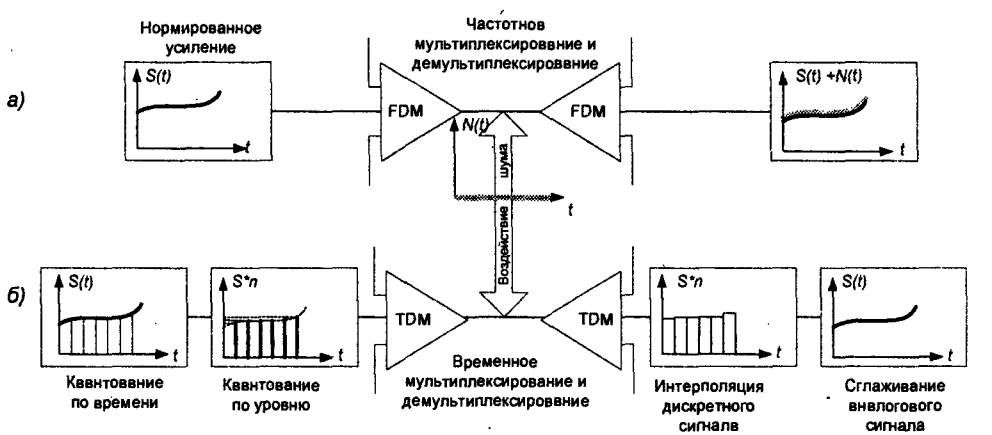


Рис. 2.1. Схемы передачи голосового сигнала по аналоговому и цифровому каналам

На первом этапе преобразования аналогового сигнала выполняется его квантование по времени. Шаг временного квантования в этом случае может быть определен по теореме Котельникова—Шеннона.

Теорема Котельникова—Шеннона

Сигнал, описываемый непрерывной функцией времени $S(t)$ и имеющий ограниченный спектр, полностью определяется своими значениями, выбранными через интервалы времени $T = 1/(2\Omega)$, где Ω — ширина спектра сигнала.

Следовательно, для корректного восстановления обычного голосового сигнала вполне достаточно использовать мгновенные значения аналогового сигнала, снимаемые с частотой более 6 кГц.

На втором этапе выполняется нормирование зафиксированных мгновенных значений аналогового сигнала (квантование) по амплитуде и формирование передаваемого кода. Затем сформированные коды суммируются по принципу разделения времени и передаются в магистральном канале вместе с кодами других голосовых потоков. Аналоговый шум, который и в этом случае воздействует на передаваемый сигнал, не вызовет искажений передаваемых по каналу кодов в том случае, если величина шага квантования превышает амплитуду шума. Поэтому на принимающей стороне после демультиплексирования и нормализации исходный код принимается без искажений. На следующем этапе выполняется интерполяция этого кода — преобразование его в последовательность прямоугольных импульсов, амплитуда которых соответствует значению принятого в данном периоде кода, а длительность соответствует шагу временного квантования. На последнем этапе эта последовательность сглаживается низкочастотным фильтром, который преобразует сигнал со ступенчатой амплитудой в непрерывный сигнал. Таким образом, после выполнения всех преобразований на приемной стороне появляется переданный сигнал, очищенный от аналогового шума линии.

Компенсация шума квантования

Для передачи голоса в цифровом потоке аналоговый голосовой сигнал преобразуется в информационный код методом импульсно-кодовой модуляции. Основное назначение кодирования заключается в преобразовании аналогового сигнала в форму, которая обеспечивает безошибочную передачу сигнала по цифровым сетям и последующее восстановление его первоначального аналогового вида у получателя. Для того чтобы обеспечить адекватное восстановление аналогового сигнала, он преобразуется в последовательность кодовых импульсов, которые следуют с периодом 8 кГц. Мгновенному значению амплитуды аналогового входного сигнала ставится в соответствие одна из 256 возможных кодировок. Таким образом, оцифрованный голосовой сигнал передается в виде 8-разрядного кода с частотой повторения 8 кГц.

Однако при выполнении аналого-цифровых преобразований передаваемый *сигнал* подвергается воздействию специфического для аналого-цифровых преобразователей (АЦП) фактора — шума квантования.

Определение

Шум квантования представляет собой изменяющуюся во времени разность между исходным аналоговым сигналом и его квантованной по амплитуде копией, которая передается по цифровому каналу.

Поскольку максимальное значение уровня шума квантования равно половине шага квантования аналогового сигнала по амплитуде, наибольшее воздействие он оказывает на голосовые сигналы с небольшим уровнем сигнала и маленьким диапазоном изменения. Именно такие сигналы, однако, соответствуют согласным буквам и имеют большое значение для адекватной передачи голосового сигнала. С целью уменьшения воздействия шума квантования на низкоуровневые голосовые сигналы, преобразование амплитуды в код выполняется по нелинейному логарифмическому закону. При этом одинаковые изменения низкоуровневых и высокоуровневых сигналов приводят к большим и меньшим, соответственно, изменениям результирующего кода. Применение этого правила уменьшает общий динамический диапазон изменения сигнала, что, в свою очередь, позволяет сжать размер передаваемого кода с 13 до 8 разрядов. На рис. 2.2 приведена схема нелинейного преобразования для компенсации воздействия шума квантования на голосовой сигнал, передаваемый по цифровым линиям связи.

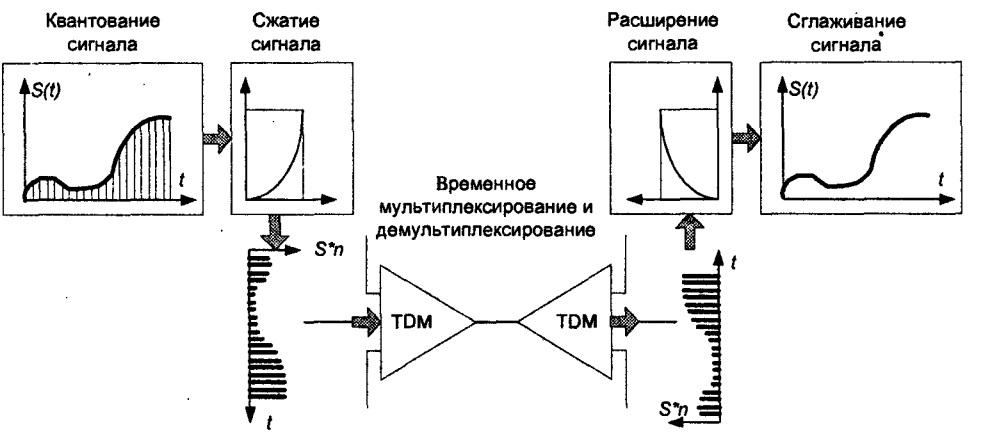


Рис. 2.2. Схема компенсации воздействия на голосовой сигнал шума квантования

Для восстановления исходного динамического диапазона аналогового сигнала на принимающей стороне перед цифроаналоговым преобразованием выполняется расширение кода по обратному — экспоненциальному закону.

Примечание

Описанное преобразование выполняется по различным правилам в европейской и североамериканской системах цифровой телефонии. Принятая в Европе

схема преобразования голосового сигнала (A-Law) обеспечивает больший диапазон изменения, но меньшую защиту от шума квантования голосового сигнала, чем принятая в Северной Америке схема (μ-Law).

Для практической реализации сжатия и расширения голосового сигнала, как правило, применяются упрощенные схемы, в которых логарифмическая и экспоненциальная зависимости аппроксимируются отрезками прямых линий — хордами (chords). При этом в сжатом коде только пять двоичных разрядов определяют уровень и полярность передаваемого сигнала, а остальные 3 бита указывают номер используемой хорды.

Типы и характеристики кодирующих систем

Прямое и обратное преобразование голосового сигнала в цифровую форму обычно выполняется унифицированными программными или аппаратными модулями, которые принято называть *кодеками* (codec — coder-decoder) или *вокодерами* (vocoder — voice-coder). Бурное развитие и широкое распространение этих систем объясняется тем, что передача голосового сигнала в цифровом виде имеет неоспоримые преимущества для построения распределенных телефонных систем:

- повышается качество принимаемого сигнала;
- обеспечивается возможность восстановления передаваемого сигнала.

Однако следует учитывать, что пропускная способность, необходимая для передачи оцифрованного голосового сигнала, как правило, в несколько раз превышает ширину полосы пропускания аналогового канала, который использовался для передачи голоса в аналоговых системах. Повысить эффективность использования пропускной способности канала передачи данных можно путем применения усовершенствованных алгоритмов преобразования голосового сигнала, однако при этом качество восстановленного голосового сигнала может ухудшиться.

В современных системах, в зависимости от требований к значению максимальной скорости цифрового потока и качеству восстановленного голосового сигнала, для цифрового преобразования голосового сигнала может быть использовано несколько алгоритмов. Некоторые типы кодеков за счет применения современных алгоритмов обработки сигналов позволяют более чем в 10 раз уменьшить информационную скорость, необходимую для передачи оцифрованного голосового сигнала. При выполнении подобных преобразований активно используются такие характеристики голосового сигнала, как непрерывность и ограниченность частотного спектра.

Голосовые кодеки PCM (G.711 и G.726)

В рекомендации ITU-T G.711 "PULSE CODE MODULATION (PCM) OF VOICE FREQUENCIES" приведены принципы реализации и требования к

основным характеристикам кодирующего и декодирующего устройств, использующих алгоритм классической импульсно-кодовой модуляции для преобразования аналогового сигнала. Диапазон изменения оцифрованного сигнала составляет 8 бит, преобразование производится с тактовой частотой 8 кГц. Таким образом, скорость потока данных на выходе кодирующего устройства составляет 64 Кбит/с (8 бит × 8 кГц). Для снижения влияния шума квантования на сигналы с небольшой амплитудой при кодировании используется нелинейное преобразование входного аналогового сигнала по схемам A-law или μ-law.

Благодаря простоте реализации кодек G.711 широко распространен в системах традиционной телефонии с коммутацией каналов. Однако кодеки, построенные в соответствии с требованиями рекомендации G.711, достаточно редко применяются в современных системах интегрированной передачи данных из-за высоких требований, предъявляемых к пропускной способности используемого канала. Применение кодирующих схем, отвечающих требованиям рекомендации G.711, можно считать обоснованным лишь в тех случаях, когда требуется обеспечить максимальное качество кодирования речевой информации при небольшом числе одновременных разговоров.

В рекомендации ITU-T G.726 "40, 32, 24, 16 KBIT/S ADAPTIVE DIFFERENTIAL PULSE CODE MODULATION (ADPCM)" приведены принципы реализации и требования к основным характеристикам кодирующего и декодирующего устройств, использующих для преобразования голосовой информации технологию *адаптивной дифференциальной импульсно-кодовой модуляции (АДИКМ)*. Отличие этой технологии от классической ИКМ заключается в том, что при использовании схемы АДИКМ в канал передается не абсолютное значение амплитуды аналогового сигнала, а приращение этого значения по отношению к значению, измеренному на предыдущем шаге. За счет сокращения размерности передаваемых данных, применение этой технологии может обеспечить формирование цифрового потока с интенсивностью 32, 24 и 16 Кбит/сек. Кодирующие схемы, построенные в соответствии с требованиями рекомендации ITU-T G.726, могут применяться совместно со схемами G.711 для повышения эффективности использования сетевых ресурсов.

Голосовые кодеки CELP (G.723.1, G.728 и G.729)

В рекомендации ITU-T G.723.1 "DUAL RATE SPEECH CODER FOR MULTIMEDIA COMMUNICATIONS TRANSMITTING AT 5.3 AND 6.3 KBIT/S" приведены принципы реализации и требования к основным характеристикам кодирующего и декодирующего устройств, использующих для преобразования голосовой информации технологию *многоимпульсного многоуровневого квантования* — *MP-MLQ* (Multy-Pulse — Multy Level Quantization). Кодирующие устройства G.723.1 выполняют преобразование аналогового сигнала

в поток данных со скоростью 64 Кбит/сек по стандартному алгоритму импульсно-кодовой модуляции, а затем при помощи многополосного цифрового фильтра выделяют в сформированном сигнале частотные фонемы и формируют значение результирующего выходного кода, определяемое текущим состоянием фонем во входном аналоговом сигнале. Использование подобного алгоритма кодирования позволяет снизить скорость передачи кодированного голосового сигнала информации до 5,3 или 6,3 Кбит/сек без ощутимого ухудшения качества речи.

Кодирующие схемы ITU-T G.723.1 обеспечивают возможность применения двух вариантов кодирования. Первый вариант предполагает использование кодирующего алгоритма MP-MLQ и обеспечивает формирование цифрового потока с интенсивностью не более 6,3 Кбит/сек — 24 байта с периодом 30 мсек. Второй вариант предполагает использование кодирующего алгоритма *линейной экстраполяции с кодовым инициированием — CELP* (Code Excited Linear Prediction) и обеспечивает формирование цифрового потока с интенсивностью не более 5,3 Кбит/сек — 20 байтов с периодом 30 мсек. Алгоритм MP-MLQ предназначен для использования в сетях с пакетной передачей голоса и обеспечивает лучшее качество кодирования по сравнению с вариантом CELP. Однако этот алгоритм относительно менее приспособлен к использованию в сетях со смешанным типом трафика (голос/данные).

В рекомендации ITU-T G.728 "CODING OF SPEECH AT 16 KBIT/S USING LOW-DELAY CODE EXCITED LINEAR PREDICTION" приведены принципы реализации устройств, использующих для преобразования голосовой информации технологию *линейной экстраполяции с кодовым инициированием и малыми задержками — LD-CELP* (Low-Delay Code Excited Linear Prediction). Метод основан на предсказании аналогового сигнала в сочетании с элементами кодирования формы сигнала. При использовании этого алгоритма процесс аналого-цифрового преобразования выполняется в несколько этапов. После выполнения операции кодирования аналогового сигнала производится его декодирование, восстановление аналогового сигнала и сравнение восстановленного сигнала с входным сигналом. Для обеспечения наибольшего соответствия производятся изменения параметров кодирующей схемы, после чего выполняется повторное аналого-цифровое преобразование. При достижении оптимального результата кодирующее устройство формирует очередное значение выходного кода. Использование кодирующих устройств, построенных в соответствии с требованиями рекомендации G.728, обеспечивает формирование цифрового потока с интенсивностью 16 Кбит/сек.

В рекомендациях ITU-T G.729 "CODING OF SPEECH AT 8 KBIT/S USING CONJUGATE-STRUCTURE ALGEBRAIC-CODE-EXCITED LINEAR PREDICTION (CS-ACELP)" приведены принципы реализации и требования к основным характеристикам кодирующего и декодирующего устройств, исполь-

зующих для преобразования голосовой информации технологию *алгебраической экстраполяции с кодовым инициированием* — *CS-ACELP* (Conjugate Structure — Algebraic Code Excited Linear Prediction).

Рекомендация G.729 Annex B предполагает использование дополнительной функции — *определение активности голосового канала* — *VAD* (Voice Activity Detector). Применение этой функции обеспечивает существенное повышение эффективности использования канала передачи данных, поскольку в данном случае аналого-цифровому преобразованию предшествует амплитудное нормирование входного сигнала. В том случае, если амплитуда этого сигнала не превышает порогового значения, аналого-цифровое преобразование данного сигнала не производится. При использовании этой процедуры паузы на приемной стороне заполняются комфортным шумом, который формирует специальный генератор.

Использование кодирующих устройств, построенных в соответствии с требованиями рекомендации G.729, может обеспечить формирование цифрового потока с интенсивностью 8 Кбит/сек — 10 байтов с периодом 10 мсек или 6,4 Кбит/сек — 8 байтов с периодом 10 мсек.

В табл. 2.1 приведены обобщенные характеристики голосовых кодеков. В предпоследней графе этой таблицы приведены значения информационной скорости, которая используется для передачи голосового сигнала, преобразованного соответствующим алгоритмом.

***Таблица 2.1.** Характеристики голосовых кодеков*

Название кодека	Тип алгоритма	Информационная скорость (Кбит/сек)	Период преобразования (мс)
G.711	Импульсно-кодоввя модуляция — (PCM)	64	0,125
G.726	Адаптивная дифференциальная импульсно-кодовая модуляция — (ADPCM)	40, 32, 24, 16	0,125
G.723.1	Многоимпульсное многоуровневое квантование (MP-MLQ) или линейная экстраполяция с кодовым инициированием (CELP)	5.3, 6.3	30
G.728	Линейная экстраполяция с кодовым инициированием и малыми задержками (LD-CELP)	16	0,625
G.729	Алгебраическая экстраполяция с кодовым инициированием (CS-ACELP)	8	10

В подавляющем большинстве случаев, использование кодека для преобразования голосового сигнала приводит к формированию цифрового потока, со-

стоящего из группы бит (от 2 до 8), которые передаются с периодом 125 мксек. В остальных случаях используются существенно более длинные последовательности, которые состоят из нескольких байтов и передаются с периодом от 10 до 30 мсек.

Передача голоса по пакетным сетям

Изначально преобразование голоса в цифровую форму выполнялось для последующей передачи по системам цифровой телефонии сетей ISDN. В этой сети, основанной на принципе коммутации каналов, для организации телефонного вызова между абонентами создавалось временное соединение с установленными характеристиками, которое и обеспечивало двунаправленный информационный обмен. Как уже было отмечено, подобные схемы обеспечивают максимально возможный уровень качества обслуживания, но их основным недостатком является низкая эффективность использования пропускной способности канала передачи данных, что в конечном счете определяет относительно высокую стоимость услуги классической цифровой телефонии. Дело в том, что в процессе нормального телефонного разговора активным является только один собеседник, таким образом, в течение примерно половины времени разговора выделенный канал не используется для организации обмена. В то же время широкое распространение сетей с коммутацией пакетов — Ethernet и Интернет, появление высокоскоростных каналов и эффективных алгоритмов кодирования голосового сигнала делает весьма желательным и возможным передачу голосового сигнала в сетях, построенных по этим принципам.

Преимущества пакетной телефонии

В основе технологии коммутации пакетов лежит принцип разбиения информационного потока на автономные блоки — пакеты, каждый из которых содержит фрагмент передаваемого потока и управляющую информацию, необходимую для доставки этого фрагмента абоненту.

Примечание

Более подробно основные принципы коммутации пакетов рассматриваются в *главе 6* настоящего издания.

Применение технологий коммутации пакетов способно обеспечить максимальную эффективность использования пропускной способности канала передачи данных. Именно по этой причине такие технологии коммутации пакетов, как Ethernet и Интернет, которые широко используются для построения сетей передачи данных, являются привлекательными для создателей перспективных телефонных систем.

Основными преимуществами трансляции голосового потока по сетям передачи данных с коммутацией пакетов являются:

- существенное уменьшение стоимости предоставления услуги — поскольку в этом случае отпадает необходимость организации дополнительных каналов и их обслуживании;
- возможность построения единой сети для предоставления комплекса интегрированных услуг;
- возможность широкого применения дешевых интеллектуальных терминалов и предоставления новых видов услуг;
- обеспечение единства администрирования.

Эти и другие побудительные причины привели к появлению комплекса спецификаций, регламентирующих передачу мультимедийного трафика по сетям с коммутацией пакетов. Поскольку на начальном этапе разработки и внедрения этих спецификаций наиболее быстрыми темпами развивались именно системы передачи телефонного трафика по сети Интернет, за этими спецификациями закрепилось неофициальные наименования "IP-телефония" или "Голос по IP" — *VoIP* (Voice over IP).

Особенности пакетного преобразования голоса

Само по себе применение технологий пакетной передачи голосового сигнала не всегда может обеспечить желаемую эффективность использования пропускной способности канала передачи данных. Например, при передаче трафика VoIP через сеть Ethernet каждый блок передаваемых голосовых данных будет снабжен блоком, состоящим, как минимум, из 38 байтов управляющих данных. Поскольку, в общем случае, эффективность использования канала определяется соотношением размеров блоков полезной и управляющей информации в передаваемом пакете, для ее повышения целесообразно увеличивать информационное наполнение каждого передаваемого пакета. При передаче голосового сигнала, однако, повышение эффективности использования канала приводит к появлению алгоритмической задержки, вызванной необходимостью накопления данных перед их отправкой в пакете. В табл. 2.2 приведены характеристики кодеков, наиболее часто используемых в сетях VoIP.

Как видно из таблицы, применение эффективных кодеков приводит к увеличению задержки передачи сигнала в канале. Сама по себе задержка в несколько десятков миллисекунд не оказывает влияния на процесс телефонного разговора. Допустимыми, в частности, признаны значения задержки, не превышающие 150 мсек. Однако следует учитывать, что в процессе передачи пакета по сети задержка будет только увеличиваться. Наиболее неприятным

последствием увеличения задержки распространения оцифрованного голосового сигнала является усиление влияния эхо-сигнала на качество телефонного разговора.

Таблица 2.2. *Характеристики кодеков, применяемых в системах VoIP*

Обозначение кодека	Размер нагрузки (байт)	Информационная скорость (Кбит/с)	Алгоритмическая задержка (мс)	Скорость передачи данных в канале (Кбит/с)[1]	
				Ethernet[2]	IP[3]
G.711	160	64	20	80	64.8
G.723.1 (6.3)	24	6.3	37.5	17.1	6.9
G.723.1 (5.3)	20	5.3	37.5	16	5.9
G.726-32	160	32	20	42.7	32.8
G.726-24	160	24	20	34.7	24.8
G.726-16	160	16	20	26.7	16.8
G.729 (8)	20	8	25	18.7	8.8
G.729 (6.4)	16	6.4	25	17.1	7.2

Примечания:

[1] По материалам Packetizer, Inc. (http://www.bandcalc.com/).

[2] С учетом заголовка протокола IP.

[3] При передаче через последовательный (не CSMA/CD) канал.

Эхо-сигнал возникает из-за паразитного взаимного просачивания звуковых сигналов, поступающих на дифференциальную систему, осуществляющую прием-передачу данных по двухпроводному абонентскому каналу. Сформированные таким образом паразитные эхо-сигналы проходят обработку в системе преобразования и поступают обратно к говорящему абоненту, что может привести к существенному ухудшению разборчивости принимаемой речи. Особенно сильное влияние на качество принимаемого сигнала оказывается в том случае, если задержка распространения звукового сигнала от источника к приемнику и обратно превышает 50 мсек. Телефонный сигнал с двухпроводной линии поступает на дифференциальную систему, которая разделяет приемную и передающую часть канала. Далее принимаемый сигнал вместе с "просочившейся" частью передаваемого сигнала поступает на вход аналого-цифрового преобразователя. Сформированный этим преобразователем цифровой код поступает на блок компенсации эхо-сигнала. В устройстве эхо-компенсации из принимаемого сигнала передачи вычитается ослабленный и задержанный передаваемый сигнал. Эхо-компенсатор представляет собой

адаптивный фильтр, длина памяти (порядок) которого и механизм адаптации определяются требованиями рекомендации G.165 (ITU-T).

Требования голосовых приложений к параметрам МСС

Для нормального распространения голосового сигнала по сети с коммутацией пакетов, в зависимости от типа используемого кодека, должна быть обеспечена полоса пропускания от 8 до 80 Кбит/сек, при этом задержка распространения голосового сигнала по сети с коммутацией пакетов не должна превышать 30—50 мсек. Следует признать, что в современных сетях, построенных с использованием каналов 100 и 1000 Мбит/сек, оба этих требования достаточно легко реализуются. Необходимо, однако, учесть, что для передачи телефонного трафика важны не столько параметры используемого канала, сколько его стабильность, достижение которой в сетях с коммутацией пакетов невозможно без применения специальных механизмов обеспечения качества обслуживания. Плохое качество или отсутствие в нужный момент телефонной связи может нанести непоправимый ущерб не только экономике предприятия, но и здоровью его сотрудников. Поэтому при построении сетей пакетной телефонии основное внимание должно быть обращено на способы повышения надежности и резервирования оборудования и каналов передачи данных.

Архитектура и компоненты систем VoIP

Вне всякого сомнения, системы пакетной телефонии ожидает большое будущее, и вполне возможно, что они через некоторое время полностью вытеснят классические телефонные системы. Однако совершенно очевидно, что для выполнения обновления потребуется немалый интервал времени, в течение которого системы классической и пакетной телефонии должны будут сосуществовать. Следовательно, из разнообразных систем организации пакетной телефонии больше перспектив имеет та, которая, с одной стороны, обеспечивает эффективное взаимодействие с системами аналоговой телефонии, а с другой — позволяет осуществить постепенную и безболезненную миграцию в единую сеть пакетной телефонии. Этот раздел посвящен рассмотрению компонентов и способов построения различных систем пакетной телефонии и вопросов ее интеграции с традиционными телефонными системами.

Системы традиционной и пакетной телефонии

Обязательным требованием к системе пакетной телефонии, естественно, является полная поддержка всего комплекса услуг традиционной телефонии с наименьшими затратами и достаточным качеством. Среди этих услуг, кото-

рые должны обеспечивать системы пакетной телефонии, в первую очередь следует выделить:

- *Организацию междугородних и международных телефонных переговоров*

  Высокая стоимость этой услуги, предоставляемой в современных телефонных сетях, объясняется необходимостью резервирования пропускной способности 64 Кбит/сек на всем протяжении вызова. Разнообразные системы пакетной телефонии позволяют в 3—5 раз сократить стоимость телефонного разговора только за счет уменьшения объемов передаваемых данных.

- *Организацию и проведение телефонных конференций*

  Внедрение систем пакетной телефонии значительно увеличивает функциональные возможности терминального оборудования. Вследствие этого, участники телефонной конференции, организованной в системе пакетной телефонии, могут получить в свое распоряжение дополнительные функции, например, возможность параллельного обмена текстовыми сообщениями.

- *Создание и обслуживание центров автоматизированной обработки телефонных вызовов*

  Применение пакетной телефонии существенно упрощает и снижает стоимость построения центров обработки телефонных вызовов.

Традиционные и гибридные телефонные системы

Системы традиционной телефонии имеют ярко выраженный централизованный характер. Все программное и аппаратное обеспечение, которое используется для обработки и обслуживания телефонных вызовов, размещается в узлах телефонной сети — *автоматических телефонных станциях* (АТС). Телефонные станции, в свою очередь, соединяются между собой цифровыми каналами плезиахронных — *PDH* (Plesiachronous Digital Hierarchy) или синхронных цифровых сетей — *SDH* (Synchronous Digital Hierarchy), образуя *телефонную сеть общего пользования* — ТфОП, или иначе *PSTN* (Public Switching Telephone Network). Основными задачами, которые должна выполнять любая АТС, являются:

- управление телефонным вызовом;
- коммутация телефонного вызова.

Первая задача включает в себя определение возможности построения соединения, создание, обслуживание, разрыв телефонного вызова и формирование сигнальных сообщений на каждом из вышеописанных этапов. При этом сообщения должны быть сформированы в соответствии с правилами той сигнальной системы, которая используется на каждом из внешних подключений

АТС. В классических телефонных системах могут быть использованы разнообразные системы сигнализации, но в современных телефонных системах для передачи сигнальных сообщений обычно используются "D"-каналы цифровых потоков PRI. Сигнальные сообщения содержат телефонные номера вызываемого и вызывающего абонентов в формате E.164 и позволяют телефонным станциям управлять состоянием телефонного вызова — передавать соответствующие сигналы промежуточным станциям, а также вызываемому и вызывающему абонентам. Создание телефонного вызова обеспечивает двунаправленную передачу разговорного трафика между двумя или несколькими абонентами телефонной сети. Для этой цели в системах цифровой телефонии применяются "B"-каналы магистральных интерфейсов PDH/SDH на промежуточных АТС и абонентские линии на оконечных телефонных станциях. Выделение, коммутация, освобождение этих каналов и линий выполняется в зависимости от текущего состояния телефонного вызова.

Таким образом, в процессе телефонного разговора между АТС осуществляется взаимодействие на уровне управления телефонным вызовом (определяется трасса и условия прохождения вызова по телефонной сети PSTN) и на уровне коммутации телефонного вызова (определяются направления и типы каналов, применяемых на каждой АТС для организации данного вызова).

На рис. 2.3, *а* приведена схема взаимодействия основных компонентов, обеспечивающих выполнение функций стандартной телефонии.

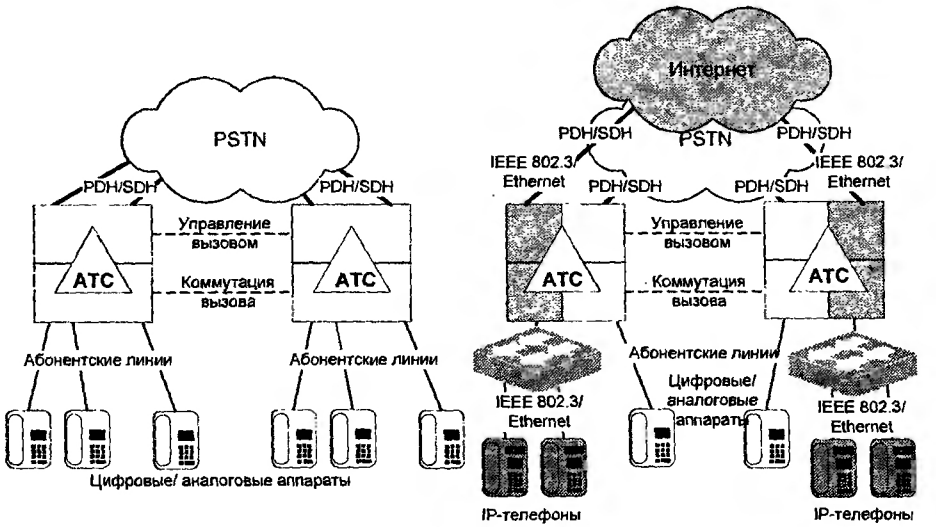


Рис. 2.3. Схемы взаимодействия основных компонентов стандартной и пакетной телефонии

Терминалы телефонной сети — цифровые или аналоговые телефонные аппараты представляют собой простейшие устройства, содержащие минимальное количество органов управления и индикации. В дополнение к функциям обычных телефонных аппаратов цифровые телефоны позволяют абоненту использовать дополнительные услуги сети ISDN. Подключение терминалов к АТС выполняется через двух- или четырехпроводные абонентские линии, при этом телефонный аппарат может находиться от АТС на расстоянии до нескольких километров. Несомненным достоинством терминалов классической телефонной сети является невысокая стоимость их приобретения и эксплуатации (в первую очередь это касается аналоговых аппаратов), что повышает привлекательность и конкурентоспособность предоставляемых через них услуг. Однако очевидно, что такой простой и узкоспециализированный терминал не может быть использован для эффективного управления услугами и, тем более, для получения новых услуг.

Одним из возможных направлений внедрения систем пакетной телефонии является применение в узлах коммутации гибридных устройств, которые сочетают в себе функции коммутатора традиционной и пакетной телефонии. Это может быть, например, обычная цифровая автоматическая телефонная станция (АТС) с установленными модулями пакетной телефонии. Достоинством такой системы является то, что она полностью сохраняет прежние возможности, а новые функции к ней добавляются и наращиваются по мере необходимости.

На рис. 2.3, *б* приведена схема взаимодействия основных компонентов гибридной телефонной системы, обеспечивающей одновременное выполнение функций стандартной и пакетной телефонии. В данном случае предполагается, что в традиционную АТС установлены модули расширения, которые позволяют организовывать телефонные соединения через сеть с коммутацией пакетов — Интернет. Для взаимодействия через сеть Интернет могут быть использованы как обычные для телефонных сетей интерфейсы первичной скорости — Primary Rate Interface — *PRI/E1*, так и традиционные для сетей передачи данных интерфейсы IEEE 802.3/Ethernet. Для подключения к телефонной сети в данном случае могут быть использованы как классические цифровые и аналоговые телефонные аппараты, так и специализированные IP-телефонные аппараты.

В отличие от классических аналоговых и цифровых телефонных аппаратов *IP-телефоны* представляют собой полнофункциональный узел доступа в телефонную сеть с коммутацией пакетов. Для этих терминалов АТС выполняет функции шлюза, обеспечивая возможность организации двусторонних телефонных вызовов между традиционной телефонной сетью и сетью IP-телефонии. Следует отметить, что телефонные вызовы через телефонную сеть общего пользования и сеть Интернет могут быть организованы в равной мере

как со стандартных, так и с IP-телефонов. Очевидным недостатком схемы внедрения пакетной телефонии, представленной на рис. 2.3, *б*, является необходимость больших единовременных вложений капитала, поскольку модули современных АТС, как правило, имеют очень высокую стоимость. Кроме того, внедрение новых модулей может потребовать обновление базового программного обеспечения АТС, что также вызовет дополнительные материальные затраты. Таким образом, следует признать, что построение гибридных систем путем единовременного внедрения функций пакетной телефонии в существующие системы классической телефонии приведет к значительным материальным затратам и не способно обеспечить быстрый возврат вложенных в него средств.

Распределенные системы пакетной телефонии

От большинства недостатков классических и гибридных телефонных систем свободны системы пакетной телефонии с децентрализованной или распределенной архитектурой. В этих системах значительная часть действий, необходимых для создания и обслуживания телефонного соединения, возлагается на интеллектуальное терминальное устройство. Модернизация телефонной системы в этом случае производится путем постепенного переноса части функций центрального коммутатора на периферийные терминалы. Достоинством такого способа модернизации является то, что он может производиться любыми темпами и принципиально не способен снизить уровень готовности основной системы, поскольку новые функции в этом случае обеспечиваются дополнительными устройствами.

В системах пакетной телефонии, имеющих распределенную архитектуру, функции таких терминалов могут выполнять следующие устройства:

- IP-телефоны;
- VoIP-шлюзы;
- серверы медиаприложений.

Существенно сократить затраты на внедрение пакетной телефонии можно путем создания дополнительного коммутирующего узла, который выполняет функции шлюза IP-телефонии. Такой шлюз обеспечивает решение задач управления телефонным вызовом и коммутации вызовов и является, таким образом, параллельной полнофункциональной телефонной станцией с небольшим числом абонентов. На рис. 2.4 представлена схема взаимодействия компонентов распределенной системы пакетной телефонии. Базовым узлом этой схемы является устройство, выполняющее функции *привратника* (gatekeeper). Привратник формирует и обслуживает таблицу адресов абонентов пакетной телефонии и помогает шлюзу определять направление передачи по сети Интернет обслуживаемого телефонного вызова. Одно устройство,

сервер доступа, например, может совмещать в себе функции шлюза и привратника. В некоторых случаях, как шлюз, так и привратник могут находиться за пределами распределенной системы пакетной телефонии, состоящей из одного или нескольких IP-телефонов, подключенных к сети Интернет.

Примечание

Следует отметить, что стоимость IP-телефонов, как правило, в несколько раз превышает цену телефонных аппаратов классической телефонии, что существенно повышает стоимость модернизации сети и уменьшает привлекательность услуги для абонента.

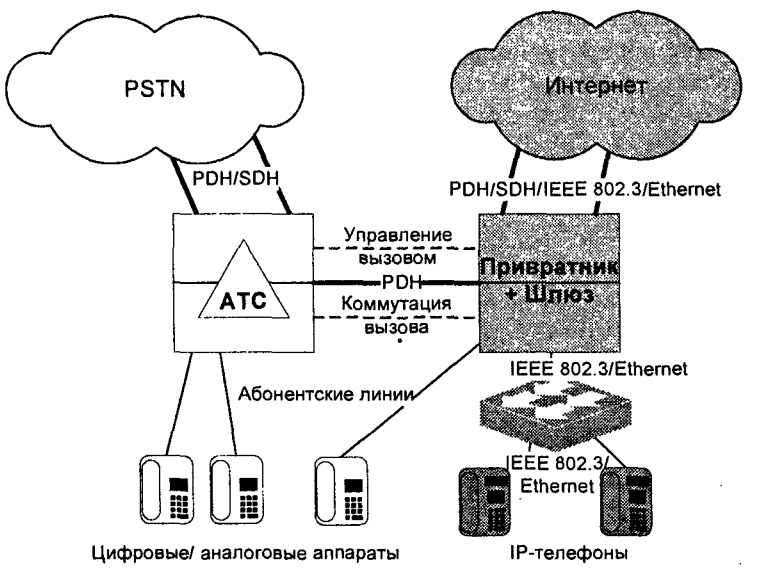


Рис. 2.4. Схема взаимодействия компонентов распределенной систем пакетной телефонии

В свою очередь, некоторые модификации шлюзов позволяют подключать к сети пакетной телефонии аналоговые и цифровые телефонные аппараты, используемые в системах традиционной телефонии. Такой шлюз в совокупности с внешним размещением привратника является наиболее экономичным решением для предоставления интернет-провайдером конкурентоспособной услуги IP-телефонии небольшим организациям и частным лицам.

Достоинством распределенных архитектур является достигаемое в них удобство управления услугами, которое определяется наличием развитых механизмов управления и индикации на многофункциональных терминалах. Основным недостатком такого решения, помимо относительно высокой стоимости оконечного оборудования, является сложность наращивания функций — при изменении способа предоставления старых услуг или введении новых

услуг соответствующие изменения должны быть выполнены на всех шлюзах и интеллектуальных терминалах сети. К недостаткам распределенной схемы организации узлов пакетной телефонии следует отнести зависимость от используемой системы формирования сигнальных сообщений. Наличие в сети пакетной коммутации разнообразных систем формирования сигнальных сообщений вызывает необходимость поддержки на интеллектуальном терминале ВСЕХ возможных вариантов сигнализации.

Иерархические системы пакетной телефонии

Основными недостатками описанных выше решений построения узлов пакетной телефонии являются их недостаточная гибкость и сильная зависимость от типа используемой сигнальной системы. Последний недостаток имеет решающее значение в ситуации, когда в сети пакетной телефонии на равных основаниях используются одновременно несколько различных систем сигнализации, таких, например, как протоколы сигнализации *SIP* (Session Initiation Protocol) или *H.323*.

Альтернативное промежуточное решение, которое соединяет в себе достоинства распределенной и централизованной архитектур пакетной телефонии, представляет иерархическая система пакетной телефонии. В соответствии с концепцией этой системы подключение абонентских терминалов выполняется к физическому шлюзу, который принимает на себя только часть функций, необходимых для предоставления услуги.

В состав иерархических систем пакетной телефонии входят:

- *физические шлюзы* — *MG* (Media Gateways);
- *контроллеры физических шлюзов* — *MGC* (Media Gateway Controllers).

Назначение физических шлюзов иерархических систем пакетной телефонии состоит в том, чтобы обеспечивать переключение подключенных к ним каналов в соответствии с реализуемой схемой обработки вызовов. Переключение каналов на физическом шлюзе выполняется по командам, получаемым от контроллера, который обеспечивает управление телефонными вызовами и контролирует их текущее состояние.

Функции физического шлюза при этом может выполнять сам телефонный терминал — IP-телефон или отдельное устройство, которое обеспечивает сопряжение существующих телефонных аппаратов с сетью пакетной телефонии. На рис. 2.5 представлена схема взаимодействия компонентов иерархической системы пакетной телефонии.

В зависимости от того, какие именно каналы подключены к физическому шлюзу, этот шлюз может выполнять либо простую коммутацию каналов, либо коммутацию с преобразованием типа среды. Так физический шлюз MG_1

(см. рис. 2.5), например, в силу своего положения должен обеспечивать прямое и обратное преобразование голосового потока из аналогового сигнала в последовательность кадров Ethernet. В то же время на шлюз MG_n возлагаются только задачи коммутации аналоговых или цифровых потоков классической телефонии. Физический шлюз также может быть использован для создания многоточечных соединений между абонентами, например, при организации телефонных конференций.

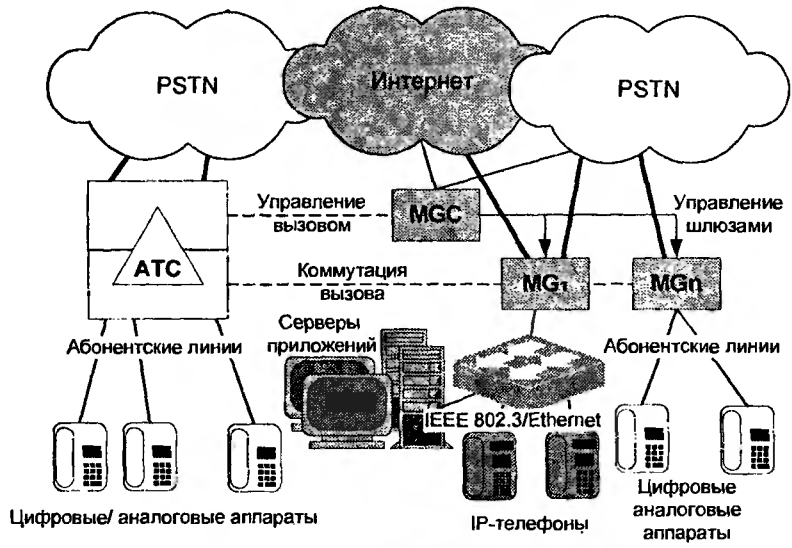


Рис. 2.5. Схема взаимодействия компонентов иерархической системы пакетной телефонии

В иерархических системах контроллеры физических шлюзов (MGC) образуют второй ярус управления телефонной сетью, на котором реализуются основные функции организации и обслуживания телефонного соединения. Устройства, выполняющие функции MGC, контролируют состояние всех активных телефонных вызовов, формируют соответствующие сигнальные сообщения для внешних абонентов, а также сообщения, управляющие подчиненными физическими шлюзами.

Таким образом, в иерархических системах традиционные функции телефонной станции: управление телефонным вызовом и коммутация телефонного вызова оказываются разделенными между контроллером физических шлюзов и собственно физическими шлюзами. Такое разделение позволяет перенести большую часть нагрузки с периферийных узлов на центральные узлы пакетной телефонии, что приводит к существенному упрощению и, следовательно, удешевлению оборудования физических шлюзов.

Компоненты систем пакетной телефонии

В зависимости от назначения конкретной системы пакетной телефонии в ее состав могут входить разнообразные функциональные компоненты. В этом разделе приведены обобщенные характеристики компонентов, которые наиболее часто используются при построении систем пакетной телефонии. Ввиду того, что терминология систем пакетной телефонии находится в стадии становления, одни и те же термины и обозначения могут иметь различное толкование в документации разных производителей телекоммуникационного оборудования. Следует также учитывать, что в современных телефонных системах могут быть использованы многофункциональные устройства, сочетающие в себе функции нескольких стандартных компонентов VoIP.

Универсальные и абонентские шлюзы VoIP

Шлюзы обычно используются в качестве центральных устройств в системах пакетной телефонии, и именно этот компонент, как правило, определяет эксплуатационные характеристики и функциональные возможности этих систем. Основное назначение шлюза состоит в том, чтобы осуществлять взаимодействие объектов, которые используют различные способы информационного обмена. Постоянно растущая потребность в устройствах такого рода в первую очередь объясняется необходимостью обеспечения надежной и экономичной связи в переходный период, при одновременном использовании услуг классической и пакетной телефонии. По своему назначению шлюзы условно можно разделить на две основные категории:

- универсальные шлюзы;
- абонентские (канальные) шлюзы.

Универсальные шлюзы выполняют функции центральных устройств на крупных коммуникационных узлах телефонных систем с распределенной архитектурой. Универсальный шлюз обычно представляет собой сервер доступа, который может обеспечить одновременное управление десятками телефонных соединений. Этот сервер также может выполнять функции пула цифровых модемов и выполнять сценарии интерактивного речевого меню. Универсальные шлюзы, как правило, поддерживают несколько систем формирования сигнальных сообщений, используемых в классической и пакетной телефонии, а также все известные способы пакетного кодирования голосового сигнала. Для подключения универсального шлюза к сети пакетной телефонии могут быть использованы один или несколько интерфейсов PDH/PRI. Подключение универсального шлюза к внешней или внутренней сети пакетной телефонии, как правило, выполняется через интерфейсы IEEE 802.3/Ethernet, однако в некоторых случаях для этой цели могут быть использованы и последовательные интерфейсы PDH или SDH — ATM/FR. Примерами уни-

версальных шлюзов являются серверы доступа компаний Cisco Systems и Lucent.

Абонентские или канальные шлюзы выполняют функцию буферных устройств на средних и малых коммуникационных узлах с иерархической и распределенной архитектурой. Они, как правило, обеспечивают подключение ограниченной группы абонентов классической телефонной сети к телефонной сети с коммутацией пакетов. При этом абонентские шлюзы обычно поддерживают одну из систем формирования сигнальных сообщений, используемых в пакетной телефонии, и некоторые из способов пакетного кодирования голосового сигнала. Для подключения к абонентскому шлюзу абонентов сети пакетной телефонии могут быть использованы один или несколько абонентских — *FXS* (Foreign Exchange Station) или станционных — *FXO* (Foreign Exchange Office) интерфейсов АТС. Подключение универсального шлюза к внешней или внутренней сети пакетной телефонии, как правило, выполняется через интерфейсы IEEE 802.3/ Ethernet 10/100 Base T.

Аппаратные и программные IP-телефоны

Программные и аппаратные IP-телефоны выполняют функции оконечных устройств — терминалов в телефонных сетях с коммутацией пакетов. Используя IP-телефон, пользователь может организовать прямое телефонное соединение с абонентами сети пакетной телефонии, и — через шлюз с абонентами традиционной телефонной сети. Для того чтобы начать использование IP-телефона, пользователь должен установить адресные параметры, определяющие его положение в сети Интернет, а также, при необходимости, — IP-адрес шлюза и параметры используемых кодеков. В дополнение к обычным сервисам аппарата традиционной телефонии IP-телефоны поддерживают множество дополнительных возможностей и функций:

- автоматическую синхронизацию календаря по протоколу NTP;
- использование пароля для ограничения доступа к терминалу;
- удаленный контроль и управление телефонным терминалом по протоколам HTTP, SNMP и Telnet;
- загрузку обновлений программного обеспечения по протоколу FTP.

Аппаратные IP-телефоны представляют собой отдельные устройства, внешнее отличие которых от традиционных телефонных аппаратов заключается в наличии разъема для подключения к сети Ethernet. Некоторые аппаратные IP-телефоны имеют в своем составе встроенный коммутатор, обеспечивающий расширение порта Ethernet 10/100 Base T. При установке такого IP-телефона у абонента, он подключается к тому порту Ethernet, куда была прежде подключена рабочая станция абонента. После этого рабочая станция включается в сеть Ethernet через порт расширения IP-телефона, что позволяет сохранить в

организации общее число портов, используемых для подключения абонентов ЛВС. Электропитание аппаратных IP-телефонов выполняется от внешнего источника или через сетевой кабель Ethernet от коммутатора, который поддерживает электропитание по сети Ethernet — *PoE* (Power over Ethernet).

Программные IP-телефоны представляют собой аппаратно-программный комплекс, основной частью которого является персональный компьютер абонента, функционирующий под управлением сетевой операционной системы. На персональном компьютере программно реализуются основные функции IP-телефона:

- управление телефонным вызовом;
- индикация состояния телефонного вызова;
- прямое и обратное преобразование голосового сигнала в поток пакетов.

Поскольку программный IP-телефон использует тот же интерфейс подключения к локальной сети, что и персональный компьютер, то для подключения этого телефона к локальной сети не требуется внесения никаких изменений. Дополнительным преимуществом программного IP-телефона является возможность применения специализированных приложений в процессе обработки телефонного вызова. Для повышения удобства использования программного IP-телефона пользователь может подключить к компьютеру по интерфейсу USB телефонную трубку или гарнитуру. Основным недостатком программного IP-телефона следует считать невозможность приема телефонных вызовов при выключенном компьютере. Этот недостаток, впрочем, не имеет существенного значения при использовании программных IP-телефонов в составе центра обработки телефонных вызовов, описание которого приведено в следующем разделе настоящей главы.

Приложения пакетной телефонии

Под приложениями пакетной телефонии мы будем называть аппаратно-программные комплексы, при реализации которых были использованы основные принципы преобразования сигнала и методы передачи данных, применяемые в системах пакетной телефонии.

Универсальные карточные системы

Одним из наиболее популярных приложений пакетной телефонии являются универсальные карточные системы (платформы). Универсальные карточные системы предназначены для предоставления абоненту комплекса предварительно оплаченных услуг. Обычно этот комплекс услуг включает в себя:

- доступ в сеть Интернет по коммутируемой линии;
- междугороднюю и международную телефонную связь.

Главное преимущество карточных систем состоит в том, что весь технологический цикл предоставления услуги в них полностью автоматизирован и практически не требует вмешательства обслуживающего персонала. Для предоплаты услуги потенциальные абоненты приобретают на пунктах распространения карточки соответствующего номинала. Каждая карточка имеет индивидуальный номер и секретный код, который известен только ее покупателю. Также карточка содержит номера телефонов, по которым будет оказываться услуга IP-телефонии и модемного пула для доступа в Интернет. На этих телефонах с использованием системы *интерактивных голосовых меню* — *IVR* (Interactive Voice Response) организуется голосовой интерфейс взаимодействия с абонентом. Следуя указаниям голосового меню, абонент легко получает необходимые инструкции для реализации услуги, например, порядок набора международного телефонного кода или некоторую дополнительную информацию, например, величину остатка средств на карточке. Универсальность описываемой системы заключается в том, что одну карточку можно использовать для оплаты всех услуг, поддерживаемых на данной платформе. Как мы видим, карточный способ предоставления услуг одинаково удобен и абоненту и провайдеру, что значительно повышает интерес к нему со стороны традиционных телефонных и интернет-операторов. На рис. 2.6 приведена типичная схема построения универсальной карточной платформы.

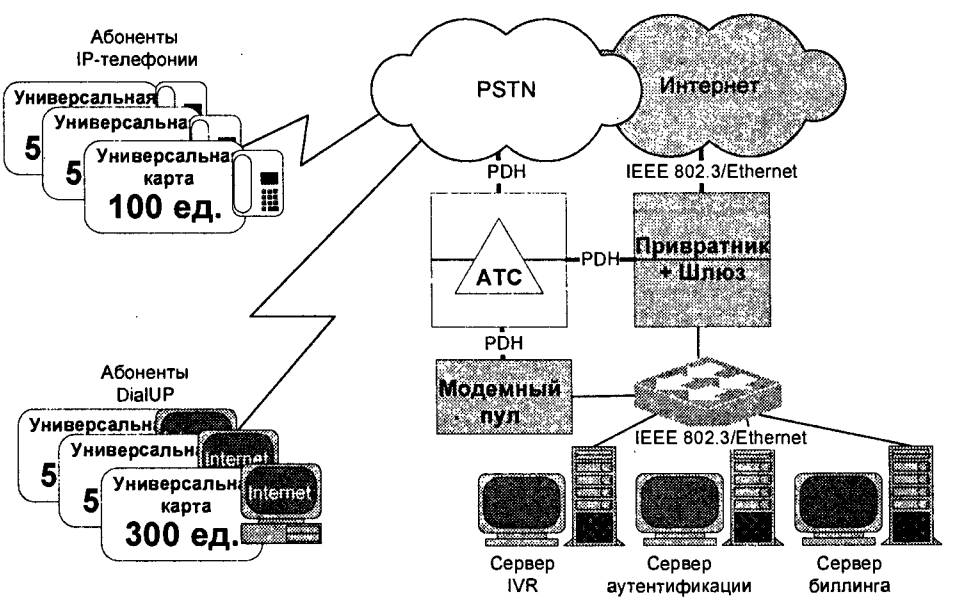


Рис. 2.6. Схема взаимодействия компонентов универсальной карточной платформы

Основными компонентами универсальной карточной системы являются:

- универсальный шлюз VoIP;
- сервер установления подлинности абонентов;
- сервер тарификации абонентов;
- сервер IVR.

Универсальный шлюз является центральным элементом пакетной платформы и предназначен для управления предоставлением всего комплекса услуг. Доступ каждого из карточных абонентов к услуге реализуется на шлюзе в виде независимого процесса по стандартному сценарию, который включает в себя следующие этапы:

- установление состояния счета и подлинности абонента;
- определение возможности предоставления запрашиваемой услуги;
- предоставление услуги;
- тарификация услуги и изменение счета абонента.

Установление подлинности абонента выполняется путем сопоставления секретного кода, введенного абонентом, с тем, который хранится в базе данных на сервере аутентификации. Платежеспособность абонента определяется текущим состоянием счета, хранимого на сервере тарификации. На этом же сервере при помощи специальных программ-обработчиков формируются тарифные планы, а также другие отчетные и финансовые документы. Сервер IVR выполняет синтез и формирование фраз интерактивного голосового меню, которое используется для навигации в системе абонента карточной платформы.

Примечание

Современные телекоммуникационные устройства могут одновременно реализовывать функции нескольких компонентов карточной платформы. Так, например, универсальный шлюз может выполнять также функции сервера интерактивного голосового меню и модемного пула, а функции сервера установления подлинности абонентов и сервера тарификации абонентов может выполнять одно устройство.

Описанная выше схема построения карточной платформы имеет все признаки системы пакетной телефонии с распределенной архитектурой, центральным звеном которой является многофункциональный шлюз. Выбор этой архитектуры, однако, определяется не столько специфическими требованиями карточной системы, сколько возможностями оборудования, которое используется для их реализации и экономическими соображениями. Дело в том, что шлюз, сочетающий в себе функции сервера доступа пакетной телефонии и модемного пула, как правило, стоит дешевле и его проще администрировать,

чем два отдельных устройства. Привлекательными чертами подобной системы являются меньший уровень затрат на эксплуатацию и короткий срок самоокупаемости.

Центры обработки вызовов

Под *центром обработки вызовов*, или иначе *call-центром*, понимают набор программных и аппаратных средств, позволяющий при помощи решений пакетной телефонии автоматизировать процесс приема и обработки телефонных вызовов. Построение такого центра позволяет не только понизить стоимость приема и ускорить обработку телефонных вызовов, но и обеспечить такие дополнительные возможности, как:

- автоматическое распределение телефонных вызовов, поступающих от абонентов;
- представление менеджеру индивидуального профиля абонента;
- документирование диалогов менеджеров с абонентами;
- статистический анализ деятельности менеджеров.

Построение центра обработки телефонных вызовов позволяет существенно повысить эффективность производственной деятельности сотрудников компании и перейти на качественно новый уровень обслуживания клиентов.

Основными компонентами центра обработки телефонных вызовов являются:

- шлюз пакетной телефонии;
- сервер базы данных (БД) абонентов;
- сервер интерактивного голосового меню (сервер IVR);
- сервер документирования активности менеджеров (Record-сервер).

В состав call-центра могут также входить серверы, обеспечивающие поддержку сервисов традиционной телефонии:

- Fax-сервер;
- сервер голосовой почты.

На рис. 2.7 приведена схема построения центра обработки вызовов с использованием концепции иерархических шлюзов.

Центральным звеном системы является контроллер физических шлюзов — MGC, который обеспечивает взаимодействие всех компонентов центра обработки вызовов с абонентами классической телефонной сети и сетью IP-телефонии. Реализованное на контроллере программное обеспечение call-центра позволяет помещать принятые вызовы в очередь и по заданному сценарию распределять вызовы из очереди на того или иного менеджера. Идентификация вызывающего клиента и назначение обслуживающего менеджера произ-

водится по информации АОН (автоматический определитель номера). Использование программных IP-телефонов позволяет менеджеру использовать в процессе обслуживания клиента специальные программные приложения. Назначение физического шлюза MG_1 в данном случае состоит в том, чтобы под управлением контроллера MGC организовывать многоточечные соединения IP-телефонов сотрудников компании с клиентами и серверами голосовых приложений. Задачей физического шлюза MG_2 является обработка под управлением контроллера MGC телефонных вызовов, поступающих из сети PSTN — прием факсимильных сообщений и фиксирование сообщений голосовой почты.

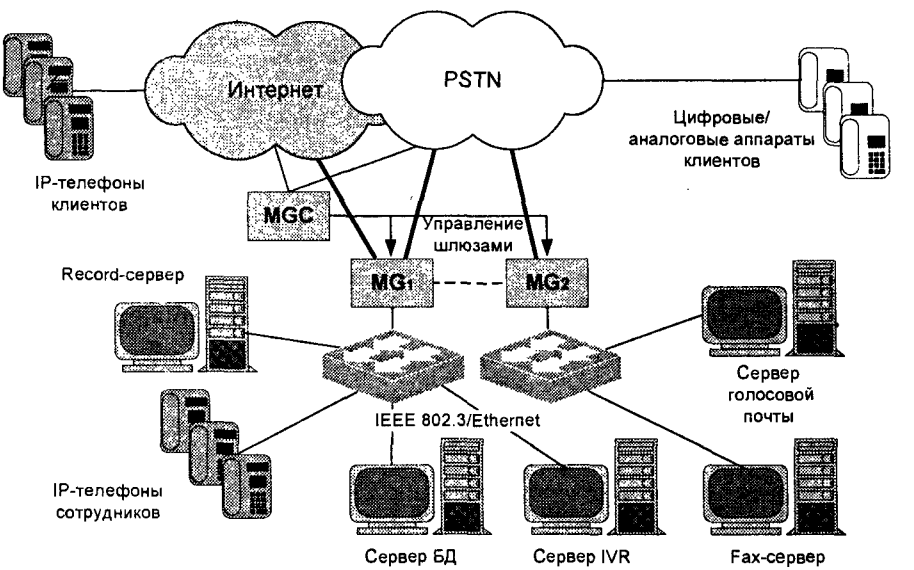
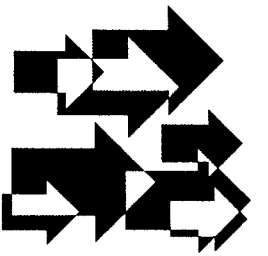


Рис. 2.7. Схема построения центра обработки вызовов с иерархической архитектурой

Иерархический характер архитектуры представленного на рис. 2.7 центра обработки вызовов обеспечивает, наряду с использованием имеющегося оборудования традиционной телефонии, внедрение функций пакетной телефонии и возможность их дальнейшего наращивания при модернизации оборудования call-центра в будущем.

ГЛАВА 3



Коммерческие и технологические видеоприложения мультисервисных сетей

Разнообразные визуальные средства всегда занимали и будут занимать ведущее место среди источников, которые человек использует для получения информации. Развитие современных технологий, в частности построение мультисервисных сетей, приводит к тому, что видеоприложения все более глубоко проникают в различные бытовые сферы и разнообразные области человеческой деятельности. Дальнейшее усовершенствование телевизионных технологий, например, позволяет не только резко улучшить качество изображения, но и кардинально изменить существующую схему телевизионного вещания путем внедрения в нее новых интерактивных услуг. В то же время видеоприложения, наряду с другими информационными технологиями, все более активно используются в сферах управления и производства на современных предприятиях.

В первом разделе данной главы рассматриваются основные принципы формирования видеосигнала телевизионных систем и алгоритмы кодирования. Рассматриваемые в этой главе алгоритмы кодирования используются для трансляции телевизионного сигнала по цифровым сетям передачи данных и обеспечения других форм распространения разнообразных видеообъектов.

Второй раздел посвящен обзору наиболее популярных видеоприложений. В этом разделе также рассматриваются основные принципы и особенности реализации этих приложений в современных мультисервисных сетях.

Способы формирования и кодирования видеосигнала

За более чем шестьдесят лет, которые прошли с момента первой трансляции телевизионного сигнала, телевизионные системы неоднократно подвергались

существенным изменениям. Задачей очередного этапа телевизионной революции является постепенный переход от аналогового к цифровому представлению видеосигнала с одновременным увеличением насыщенности телевизионного изображения. В связи с этим резко повышается значение алгоритмов кодирования, которые способны существенно уменьшить передаваемые объемы при трансляции телевизионных программ по цифровым каналам передачи данных.

Системы аналогового телевидения

Изначально проблема кодирования видеоизображения решалась в системах промышленного телевидения. Размер и характеристики телевизионного изображения определялись, с одной стороны, возможностями используемых технологий воспроизведения изображения, а с другой — особенностями человеческого восприятия этого изображения.

Принципы формирования телевизионного изображения

Изображение на экране телевизионного приемника создавалось при помощи модуляции интенсивности электронного луча, воздействующего на люминесцентное покрытие — *люминофор* приемной трубки — *кинескопа*. При построении телевизионного изображения электронный луч периодически перемещался по всей поверхности экрана кинескопа как по горизонтали, создавая очередную *строку* светящихся или темных точек, так и по вертикали — для создания *кадра телеизображения*, состоящего из нескольких сотен строк. Период послесвечения люминофора был выбран таким образом, чтобы свечение точки изображения заканчивалось к моменту, когда электронный луч кинескопа снова попадет в соответствующий участок экрана. Опытным путем было выяснено, что человеческий глаз перестает воспринимать пульсации яркости объекта, которые происходят с частотой свыше 50 Гц, поэтому в случае, когда смена телевизионных кадров выполняется с этой частотой, человек видит на экране непрерывное черно-белое статическое или подвижное изображение.

Формирование очередного кадра изображения может быть выполнено двумя способами перемещения электронного луча по экрану телевизионного приемника:

- прогрессивным сканированием — P (Progressive);
- чересстрочным сканированием — I (Interlaced).

При использовании прогрессивного способа формирования изображения в каждом кадре должны быть переданы все строки телеизображения. При чересстрочном способе передачи изображения в четных кадрах будут переда-

ваться четные строки исходного кадра (четный полукадр), а в нечетных кадрах будут передаваться нечетные строки. Естественно, изображение, сформированное с использованием чересстрочной развертки, имеет меньшее качество по сравнению с тем, что получается благодаря использованию прогрессивного режима, но зато применение чересстрочной развертки позволяет в два раза уменьшить ширину полосы пропускания, занимаемой телевизионным сигналом.

Сигнал первых промышленных телевизионных систем был аналоговым и представлял собой совокупность напряжений, используемых для модуляции интенсивности светового излучения всех строк передаваемого кадра. Для обеспечения эфирного распространения телевизионного сигнала он подвергался нормированию и модуляции высокочастотным напряжением, частота которого установлена для данного канала в сетке вещания. Сформированный таким образом телевизионный сигнал занимал полосу частот шириной 6—8 МГц и теоретически обеспечивал передачу от 500 до 700 элементов черно-белого изображения в каждой строке.

Системы цветного телевидения

Основной теоретический принцип передачи цветного изображения был разработан в первой половине прошлого века. Он предусматривал разложение исходного цветного изображения на три составляющие основных цветов: красного (Red — R), зеленого (Green — G) и синего (Blue — B), их передачу телевизионному приемнику, где осуществлялось восстановление цветного изображения путем взаимного наложения всех трех составляющих. Таким образом, при переходе от черно-белого телевидения к цветному телевидению разработчикам телевизионных систем пришлось решать две основные задачи:

- разработать способ кодирования цветовых составляющих сигнала, занимающего ту же полосу частот, что и сигнал черно-белого телевидения (8 МГц);
- обеспечить возможность приема сигнала с цветовым кодированием на черно-белые телевизионные приемники.

В разных странах эти задачи решались по-разному, что привело к практически одновременному созданию нескольких стандартов цветного телевизионного вещания:

- NTSC;
- PAL;
- SECAM.

Первый промышленный стандарт цветного телевизионного вещания *NTSC* (National Television System Committee) был разработан в 1953 году Американ-

ским телевизионным комитетом. В целях сокращения полосы пропускания, занимаемой телевизионным сигналом, использовался чересстрочный способ формирования изображения. Этот стандарт получил наименование NTSC и обеспечивал передачу и прием телевизионного изображения со следующими параметрами:

- количество строк в кадре — 525;
- частота смены кадров — 60 Гц;
- способ формирования кадра — чересстрочная развертка;
- скорость передачи сигнала — 29,97 кадров в секунду.

В телевизионном сигнале, закодированном в соответствии с правилами формата NTSC, каждая телевизионная строка содержит составляющую яркости Y и два разностных сигнала цветности I и Q. Переход от базовых осей цветового кодирования U и V к осям — I и Q используется для сужения до 0,5 МГц ширины полосы пропускания используемых для передачи цветовых сигналов.

В начале шестидесятых годов в развитых странах Центральной Европы началась промышленная эксплуатация систем цветного телевизионного вещания, построенных по Европейскому стандарту *PAL* (Phase Alternating Line). Первая Европейская система промышленного телевидения обеспечивала чуть большее разрешение изображения, но меньшую частоту смены кадров, чем NTSC:

- количество строк в кадре — 625;
- частота смены кадров — 50 Гц;
- способ формирования кадра — чересстрочная развертка;
- скорость передачи сигнала — 25 кадров в секунду.

В телевизионном сигнале, закодированном в соответствии с правилами формата PAL, применяется амплитудная модуляция цветоразностных сигналов U и V с фазовым сдвигом гармоники несущего сигнала на 90°. Применение этого метода обеспечивает уменьшение взаимного влияния цветовых сигналов при их передаче в едином канале.

Также в начале шестидесятых годов во Франции завершилась разработка второго варианта европейской спецификации цветного телевизионного вещания, которая получила наименование *SECAM* (Sequential Couleur Avec Memoire). Основные характеристики телевизионного изображения, формируемого в системе SECAM — количество строк в кадре, частота смены кадров, совпадали с аналогичными характеристиками телевизионной системы PAL. Отличие между этими системами заключается только в используемых способах кодирования цветовых сигналов. В телевизионном сигнале, закоди-

рованном в соответствии с правилами формата SECAM, в отличие от PAL, используется частотная модуляция цветоразностных сигналов.

Форматы видеоизображения

В предыдущих разделах было отмечено, что в ранних системах промышленного телевидения видеосигнал был дискретным по вертикали (в пределах кадра), но аналоговым и непрерывным по горизонтали (в пределах строки). Для объективной оценки качества изображения, сформированного таким сигналом, можно было использовать только один параметр — количество строк в кадре. Очевидно, что применение такого критерия не могло обеспечить требуемую точность оценки качества и не давало представления об информационной насыщенности передаваемого изображения.

Для оценки качества любого изображения принято считать, что оно состоит из элементарных графических компонентов — цветовых точек, называемых *пикселами*.

Определение

Пиксел — термин, используемый для обозначения наименьшей единицы графического изображения (picture element), которая может быть отображена на экране приемника видеопотока.

Используя понятие пиксела, можно определить критерий графической плотности изображения в виде соотношения количества точек изображения (пикселов) к площади участка экрана, на которой они отображаются. Понятие пиксел также используется для определения стандартных форматов видеоизображения.

Так, например, видеоизображение общего промежуточного формата — *CIF* (Common Intermediate Format) состоит из 352 пикселов по горизонтали и 240 пикселов по вертикали в системах промышленного телевидения NTSC и 352 и 288 пиксела соответственно в системах промышленного телевидения PAL.

Видеоизображение четвертного промежуточного формата — *QCIF* (Quarter-size Common Intermediate Format) представляет собой четвертую часть от видеоизображения CIF — размеры видеоизображения QCIF по горизонтали и вертикали вдвое меньше соответствующих размеров изображения формата CIF. На рис. 3.1 представлены относительные соотношения размеров некоторых стандартных изображений.

Принято считать, что видеоизображение четырехкратного промежуточного формата — *4CIF* по своим размерам и плотности соответствует изображению, воспроизводимому на экране стандартного телевизионного приемника. В системах различного назначения также могут быть использованы и другие

форматы видеоизображений — от сверхбольших размеров — *16CIF* — до миниатюрных форматов *SQCIF*.

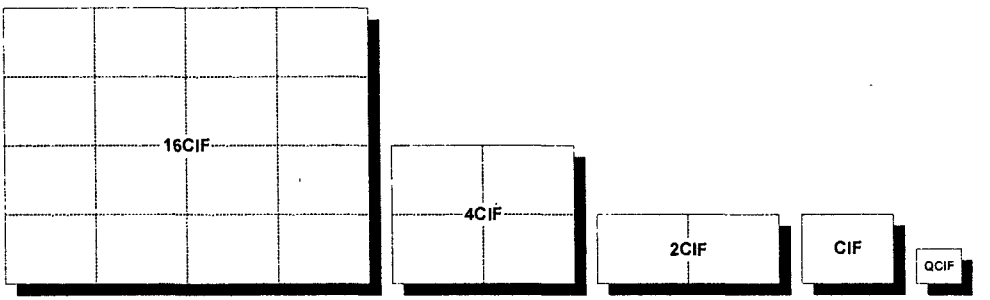


Рис. 3.1. Соотношение размеров видеоизображений стандартных форматов

Применение понятия стандартного формата изображения позволяет также оценить требования к пропускной способности, которая будет использована для трансляции соответствующего видеосигнала по каналу передачи данных. В табл. 3.1 приведены параметры основных форматов стандартных видеоизображений, а также оценки значения скорости информационного потока, который будет использован для их трансляции через канал передачи данных.

Таблица 3.1. *Стандартные форматы видеоизображения*

Название формата	NTSC			PAL/SECAM		
	Размер — Г	Размер — В	Скорость	Размер — Г	Размер — В	Скорость
SQCIF	—	—	—	128	96	2,9
QCIF	176	120	5,1	176	144	6,1
QCIF+	176	220	9,3	176	220	9,3
CIF	352	240	20,3	352	288	24,3
2CIF	704	240	40,6	704	288	48,7
4CIF	704	480	81,1	704	576	97,3
9CIF	1056	720	182,5	1056	864	219,0
16CIF	1408	960	324,4	1408	1152	389,3

В приведенной таблице использованы следующие обозначения:

- "Размер — Г" — количество пикселов в передаваемом изображении по горизонтали;
- "Размер — В" — количество пикселов в передаваемом изображении по вертикали;

- "Скорость" — информационная скорость в Мбит/сек, необходимая для передачи несжатого изображения соответствующего формата.

При расчете приведенного значения скорости частота смены кадров была принята равной 30 Гц, количество градаций яркости передаваемого изображения — 256, т. е. по 8 битов на пиксел.

Приведенные в табл. 3.1 результаты показывают, что информационные скорости, требуемые для передачи оцифрованного видеосигнала, на порядок превышают аналогичные характеристики стандартных приложений, что позволяет сделать однозначный вывод о настоятельной необходимости использования предварительного сжатия видеоизображения для его трансляции по каналам передачи данных.

Типы и характеристики кодирующих систем

Так же, как и в случае с голосовым сигналом, цифровое преобразование видеосигнала призвано решить несколько задач:

- обеспечить возможность передачи видеосигнала по цифровому каналу передачи данных;
- повысить эффективность использования пропускной способности этого канала.

Существенное отличие кодирования изображения от кодирования звука заключается в том, что видеосигнал, как правило, не имеет таких четко выраженных и ограниченных характеристик, как звуковой сигнал. В то же время, очевидно, что видеоизображение является по своей сути очень неоднородным, на любом изображении всегда можно найти достаточно большие неподвижные или одноцветные зоны, что делает, безусловно, возможным выполнение его эффективного сжатия.

Исторически разработку методов и способов кодирования видеоизображений ведут две стандартизирующие организации:

- Международный телекоммуникационный союз *ITU-T* (International Telecommunications Union — Telecommunications) — в рамках направления "Аудиовизуальные и мультимедийные системы" (Audiovisual and multimedia systems — серия рекомендаций группы "H");
- Международная стандартизирующая организация *ISO* (International Organization for Standardization) — в рамках рабочей группы экспертов кодирования подвижных изображений (Moving Picture Expert Group — ISO/IEC JTC1 SC29 WG11 неофициальное наименование — *MPEG*).

Несмотря на то, что работы по созданию алгоритмов и способов построения систем кодирования видеоизображений в этих организациях проводятся не-

зависимо, подготовленные ими спецификации основаны на единых принципах и подходах к решению проблемы. Это делает возможным принятие ряда стандартизирующих документов под единой редакцией, как это, например, произошло с H.262 и MPEG-2. Единство подходов также позволяет использовать унифицированные программные и аппаратные модули для построения многофункциональных систем сжатия видеоизображений.

Кодирование видеопотоков с использованием рекомендации H.261

В рекомендации *ITU-T H.261* "VIDEO CODEC FOR AUDIOVISUAL SERVICES AT P X 64 KBIT/S" содержатся основные принципы построения, требования и характеристики систем сжатия потоков, создаваемых аудиовизуальными приложениями. Поскольку системы кодирования и сжатия звука и видеоизображения H.261 предназначались для обеспечения возможности предоставления аудиовизуальных услуг в сетях ISDN, предполагалось, что сжатые потоки, формируемые кодеком, должны иметь информационные скорости в пределах от 40 до 2 Мбит/сек. По этой же причине шаг изменения информационных скоростей был установлен равным 64 Кбит/сек.

Суть метода сжатия изображения, использованного в H.261, заключается в выполнении гибридного прогнозирования передаваемого видеоизображения с целью определения и компенсации имеющейся в нем временной избыточности.

В рекомендации H.261 описаны алгоритмы преобразования видеоизображения форматов CIF и QCIF.

Примечание

Предполагается, что цветоразностные составляющие телевизионного изображения имеют в четыре раза меньшую плотность.

Для выполнения преобразования видеоизображение формата CIF разбивается на 12 групп блоков — *GOB* (Groups Of Blocks) таким образом, что каждая группа блоков представляет собой фрагмент видеоизображения шириной 176 пикселов и высотой 48 пикселов. На рис. 3.2 представлена структура стандартных компонентов видеоизображения, определенных в рекомендации H.261.

Каждая группа блоков, в свою очередь, делится на 33 макроблока — *MB* (Macro Block). Макроблок представляет собой квадратный фрагмент видеоизображения шириной 16 пикселов и высотой 16 пикселов, и включает в себя четыре элементарных блока изображения размером 8 пикселов по вертикали и горизонтали.

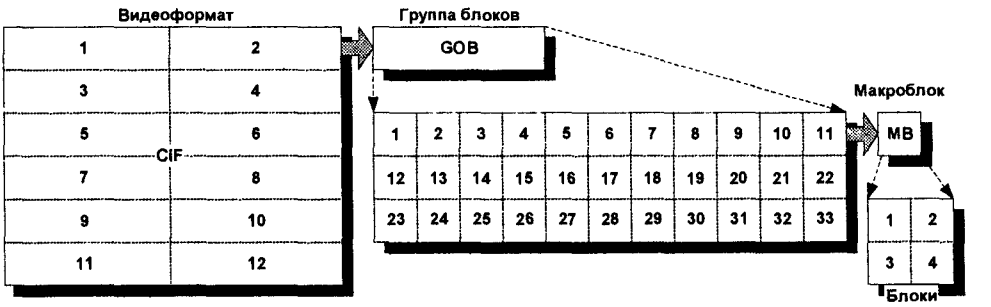


Рис. 3.2. Структура стандартных компонентов видеоизображения, определенных в рекомендации H.261

В соответствии с принципами, сформулированными в рекомендации H.261, элементарный компонент цветного изображения кодируется состоянием трех макроблоков:

- макроблока сигнала яркости Y (четыре элементарных блока);
- макроблока голубого цветоразностного сигнала C_B;
- макроблока красного цветоразностного сигнала C_R.

Таким образом, минимальными компонентами черно-белого и цветного видеоизображения, над которым выполняются базовые преобразования согласно рекомендации H.261, являются блок и макроблок соответственно.

Основу примененного в H.261 метода сжатия видеоизображения составляет обнаружение и кодирование его пространственной и временной неоднородности. Пространственными неоднородностями, например, можно считать ограниченные области внутри кадра, которые отличаются по уровню яркости или цветовому тону от окружающего их фона. Временные неоднородности передаваемого видеоизображения могут быть вызваны изменениями или перемещениями отображаемых на экране объектов. Эти неоднородности фиксируются путем сравнения двух или более последовательно принятых для обработки кадров.

Сжатие и кодирование подвижных изображений обеспечивается путем одновременного выполнения следующих функций:

- обнаружения, прогнозирования и кодирования перемещения компонентов изображения;
- выявления и компенсации пространственной избыточности в передаваемом сигнале;
- компенсации ошибок прогноза перемещения.

Для обнаружения движений и изменений компонентов передаваемого видеоизображения кодирующее и декодирующее устройства H.261 должны сфор-

мировать и хранить текущий образ этого изображения, который выполняет функцию динамического эталона. Формирование такого эталона осуществляется в режиме начального ввода изображения *(Input Picture — INTRA Mode)*.

Выявление и компенсация пространственной избыточности в рекомендации H.261 реализуется путем использования двумерного дискретного косинус-преобразования — *DCT* (Discrete Cosine Transform).

В алгоритмах H.261 предполагается, что кодирование перемещения компонентов изображения и компенсация ошибок прогноза перемещения выполняются в режиме компенсации избыточности передаваемого изображения и ошибок прогнозирования его перемещений *(Prediction Error — INTER Mode)*.

На рис. 3.3 представлена схема сжатия и кодирования видеоизображения по алгоритму, определенному в рекомендации H.261.

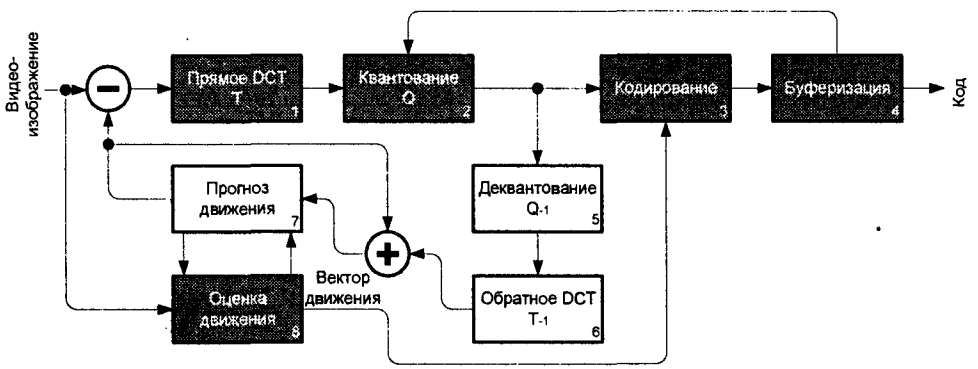


Рис. 3.3. Структурная схема блока кодирования видеоизображения по алгоритму H.261

В режиме INTRA Mode для обработки видеоизображения используются только блоки, отмеченные на рис. 3.3 более темным цветом. В этом режиме функциональные блоки 1 и 2 выполняют двумерную дискретную свертку и последующее квантование входного видеоизображения.

Примечание

Свертка яркостного компонента видеоизображения производится в пределах стандартного блока, а цветоразностных компонентов — в пределах макроблока. Поскольку в стандартном телевизионном видеоизображении на одну цветную точку приходится четыре яркостных — в обоих случаях фрагмент преобразуемого изображения представляет собой квадрат со стороной в 8 пикселов.

Квантование кодов, полученных после выполнения дискретного косинус-преобразования DCT, обеспечивает уменьшение динамического диапазона изменения кодов в 16 раз. Если на вход блока 2 поступают коэффициенты дискретного преобразования, имеющие диапазон изменения от –2048

до 2047, то диапазон изменения выходных кодов составляет от –256 до 255. Блок 3 обеспечивает преобразование поступающих на его входы квантованных значений, в коды переменной длины — *VLC* (Variable-Length Coder). Те значения, которые встречаются часто, кодируются более короткими кодами, а те, которые встречаются редко — более длинными, что позволяет сократить объем передаваемых данных. Аналогичным образом осуществляется кодирование и адреса передаваемого макроблока.

В режиме INTER Mode для обработки видеоизображения используются все функциональные блоки, представленные на рис. 3.3. В этом режиме блок 8 применяется для оценки перемещения компонентов видеоизображения. Основное назначение этого блока состоит в сравнении текущего и прогнозируемого образов изображения и формирования векторов перемещений, которые используются для преобразования передаваемого кода. Независимый вектор перемещения имеет вертикальную и горизонтальную составляющие от –15 до 15 пикселов каждый и может быть сформирован для каждого макроблока видеоизображения. Стартовый образ видеоизображения формируется этим блоком в режиме INTRA Mode и помещается в специальную область запоминающего устройства блока 7, предназначенного для хранения прогнозируемого изображения. Прогнозируемое видеоизображение создается в блоках 5, 6 и 7 путем последовательного выполнения обратных преобразований — расширения и обратной свертки того кода, который был передан в предыдущем цикле. Таким образом, в блоке 7 создается образ видеоизображения, аналогичный тому, что будет восстановлен на приемной стороне. Именно это видеоизображение используется в режиме INTER Mode для сравнения с текущим входным видеоизображением и формирования передаваемого сигнала. Естественно, чем меньше будут отличаться два этих образа, тем меньшим будет объем передаваемого кода.

В режимах INTER Mode и INTRA Mode блок 4 используется для накопления сформированных кодов перед их отправкой через канал передачи данных. В рекомендации H.261 оговаривается максимальный размер кода для допустимых форматов входных видеоизображений:

- не более 64 Кбит — для формата QCIF;
- не более 256 Кбит — для формата CIF.

Блок 4 используется также для формирования управляющих и контрольных сообщений между формирователем и приемником сжатого изображения.

Особенности кодирования согласно рекомендации H.263

Рекомендация ITU-T H.263 "VIDEO CODING FOR LOW BIT RATE COMMUNICATION" представляет собой дальнейшее развитие принципов кодирования подвижных видеоизображений, которые были изложены в рекомен-

дации H.261. Основное отличие рекомендации H.263 от предшествующей состоит в понижении, за счет увеличения плотности кодирования, требований к пропускной способности канала, который используется для передачи видеоизображения. Таким образом, изложенные в рекомендации H.263 алгоритмы и способы кодирования, изначально были ориентированы на использование при построении компактных или мобильных мультимедийных систем. Однако увеличение степени сжатия изображения, достигаемое при использовании кодеков H.263 позволяет применять их также при построении стационарных и крупногабаритных систем. Поэтому в спецификации H.263 определяется три дополнительных, по отношению к рекомендации H.261, форматов видеоизображения. Таким образом, применение кодеков H.263 обеспечивает сжатие и кодирование видеоизображений пяти стандартных форматов:

- SQCIF (176×144);
- QCIF (352×288);
- CIF (704×576);
- 4CIF (1056×864);
- 16CIF (1408×1152).

При построении кодека H.263 были использованы в основном те же принципы и алгоритмы, которые применяются в кодеке H.261 для кодирования подвижных видеоизображений. Улучшение характеристик достигается благодаря следующим модификациям алгоритма кодирования H.263:

- увеличению точности прогноза и компенсации движения компонентов изображения;
- применению синтаксически-ориентированного арифметического кодирования — *SAC* (Syntax-based Arithmetic Coding) вместо стандартного кодирования VLC (Variable-Length Coder);
- использованию режима расширенного двунаправленного прогноза — *Bi-Directional Prediction*.

Двукратное повышение точности прогнозирования перемещения видеоизображения при использовании кодека H.263 обеспечивается благодаря использованию режима интерполяции при расчете значений составляющих вектора перемещения. При использовании кодека H.261 они вычисляются с точностью, которая соответствует расстоянию между соседними пикселами, что, как правило, приводит к значительным ошибкам при прогнозировании медленно движущихся объектов. Применение интерполяции позволяет увеличить точность расчета значений составляющих вектора перемещения и, как следствие, повысить точность прогноза перемещения.

Дополнительное повышение точности прогноза перемещения в кодеке H.263 обеспечивается благодаря применению режима расширенного двунаправленного прогноза. В этом режиме для расчета составляющих вектора перемещения используются два значения:

- вектор прямого прогноза (forward vector);
- вектор обратного прогноза (backward vector).

Оба эти значения используются для независимого вычисления составляющих вектора перемещения. Результирующее значение составляющей вектора перемещения для очередного кадра определяется как среднее арифметическое из двух прогнозируемых значений. Использование режима расширенного двунаправленного прогноза в кодеке H.263 позволяет уменьшить ошибки прогноза положения подвижных фрагментов видеоизображения.

Применение всех описанных выше модификаций кодека H.263 позволяет примерно в два раза уменьшить объем передаваемых данных при сохранении приемлемого качества видеоизображения по отношению к кодеку H.261.

Применение MPEG-1 для кодирования мультимедийных объектов

Спецификация видеокодека ISO/IEC 11172 "INFORMATION TECHNOLOGY -- CODING OF MOVING PICTURES AND ASSOCIATED AUDIO FOR DIGITAL STORAGE MEDIA AT UP TO ABOUT 1,5 MBIT/S", которая получила впоследствии условное наименование *MPEG-1*, была подготовлена рабочей группой ISO/IEC JTC1 SC29 WG11 в 1992 году. В первую очередь данный кодек был предназначен для того, чтобы выполнять сжатие видеофильмов для обеспечения их записи на CD-ROM. Поэтому видеокодек MPEG-1 был призван обеспечить скорость записи не менее 1,5 Мбит/сек, причем общий объем закодированного фильма не должен был превышать 600 Мбайт, а качество восстановленного видеоизображения должно соответствовать качеству воспроизведения с видеокассеты VHS.

Общие принципы и алгоритмы сжатия видеоизображений, которые используются в видеокодеке MPEG-1, практически полностью соответствуют тем, что применяются в кодеке H.261. Спецификация MPEG-1 включает в себя пять разделов:

- общее описание системы;
- описание принципов кодирования видеоизображения;
- описание принципов кодирования звукового сопровождения;
- правила и способы контроля функционирования кодеков;
- текст на языке C программ, моделирующих кодеки.

Применение кодека MPEG-1 обеспечивает возможность манипуляции режимом прогнозирования кадров для управления качеством видеоизображения при сжатии видеофильмов. Как известно, использование стандартных методов кодирования подвижного видеоизображения приводит к появлению в выходном потоке следующих типов кадров:

- Кадров I (Intra pictures) — начальных кадров видеоизображения;
- Кадров P (Predictive pictures) — прогнозируемых кадров видеоизображения;
- Кадров B (Bi-directional predictive pictures) — кадров видеоизображения, прогнозируемых по двум направлениям.

Кадры I-типа формируются в режиме INTRA Mode в результате применения алгоритмов цифровой свертки DCT к входному видеоизображению. Эти кадры в дальнейшем используются в качестве опорных кадров для прогнозирования в режиме INTER Mode. Поэтому кадры I-типа имеют наибольший размер и максимальное качество передачи изображения. Кадры P- и B-типов формируются в режиме INTRA Mode и имеют размеры 0.3 и 0.1 от размера кадра I соответственно.

Стандартное качество передачи видеоизображения обеспечивается при использовании последовательности чередования кадров — *GOP* (Group Of Pictures), которая обозначается "15/3" и имеет следующий вид: "IBBPBBPBBPBBPBB". В этой последовательности на один опорный кадр приходится 14 прогнозируемых кадров, а на каждый простой прогнозируемый кадр приходится два двунаправленных. Эта последовательность, впрочем, может быть нарушена и, если произойдет значительное изменение базового изображения, в этом случае будет передан внеочередной I-кадр.

Очевидно, что лучшее качество передачи у сжатого видеоизображения может быть обеспечено при уменьшении базового соотношения, например, до значения 12/3. Так же очевидно, впрочем, что это изменение неминуемо приведет к увеличению объема передаваемых данных.

Основные принципы кодирования MPEG-2

При разработке спецификации видеокодека MPEG-2 специалисты рабочей группы ISO/IEC JTC1 SC29 WG11 непосредственно сотрудничали со специалистами ITU-T. Это позволило объединенной рабочей группе использовать материалы проекта одноименной рекомендации ITU-T H.262 "INFORMATION TECHNOLOGY — GENERIC CODING OF MOVING PICTURES AND ASSOCIATED AUDIO INFORMATION VIDEO" в качестве основы будущего документа ISO/IEC 13818 "INFORMATION TECHNOLOGY -- GENERIC CODING OF MOVING PICTURES AND ASSOCIATED AUDIO INFORMATION".

В отличие от кодека, определенного в спецификации MPEG-1, описываемый видеокодек был изначально ориентирован на обеспечение сжатия и кодирования при выполнении трансляции многоканальных мультимедийных сигналов по широкополосным каналам передачи данных. Поэтому значительная часть спецификации MPEG-2 посвящена вопросам организации, управления и диагностирования процессов информационного обмена при передаче сжатых мультимедийных потоков. Кроме того, телевизионные кодеки спецификации MPEG-2 выполняют ряд функций, которые являются специфическими именно для систем коммерческого телевизионного вещания, и обеспечивают совместимость с кодеками предыдущей версии MPEG. Снятие ограничений на способ формирования и размер передаваемых видеоизображений позволяет успешно применять кодирование MPEG-2 не только в классических системах промышленного телевидения, но и в перспективных телевизионных системах высокой четкости.

Так же, как и предшествующий документ рабочей группы ISO/IEC JTC1 SC29 WG11, спецификация MPEG-2 включает в себя несколько функциональных разделов:

- общее описание системы;
- описание принципов кодирования видеоизображения;
- описание принципов кодирования звукового сопровождения.

Возможность применения кодека MPEG-2 в телевизионных системах высокой четкости привела к необходимости модификации прежних и введению новых стандартных понятий. Так, в частности, в новой версии кодека определяется понятие "slice" — срез видеоизображения.

Определение

Срезом видеоизображения называется непрерывная последовательность макроблоков, размещенная по горизонтали кодируемого видеоизображения.

Таким образом, исходное видеоизображение может быть представлено кодеком MPEG-2 в виде последовательности, состоящей из нескольких срезов, причем, в зависимости от применяемого режима кодирования, эти срезы могут полностью или только частично покрывать всю площадь кодируемого изображения. В *режиме ограниченной структуры (Restricted Slice Structure)*, в частности, кодирование выполняется для всей площади видеоизображения. В этом режиме способ разбиения видеоизображения соответствует тому, который применялся в предыдущей версии кодека, причем функции блоков GOB в данном случае выполняют срезы. В режиме ограниченной структуры может быть использована возможность варьирования длины каждого из срезов, что позволяет более точно и экономично передать цветовой или яркостной состав кодируемого видеоизображения. Очевидно, что именно этот ре-

жим целесообразно применять для формирования I-кадров. При использовании *режима общей структуры (General Slice Structure)* срезы покрывают только изменяемую часть кодируемого изображения, что позволяет существенно сократить объем передаваемых данных. Режим общей структуры применяется для формирования прогнозируемых кадров P- и B-типа.

В кодеке, обеспечивающем преобразование видеосигнала, формируемого в телевизионных системах с высокой четкостью изображения *(ТВЧ)*, должны быть учтены следующие специфические особенности:

- увеличенный размер изображения (1 000—1 500 пикселов);
- прогрессивный режим развертки;
- повышенная частота смены кадров (60—80 Гц);
- изменение соотношения вертикального и горизонтального размеров видеоизображения;
- повышение цветовой плотности изображения.

Последняя из представленных выше особенностей видеоизображения ТВЧ была учтена при разработке кодека MPEG-2 путем введения дополнительных структур макроблоков, обеспечивающих представление различных цветовых режимов расположения компонентов видеоизображения. Цветовой режим видеоизображения принято описывать тройным соотношением — $NY : NC_V : NC_H$, где:

- NY — число пикселов яркостного компонента в блоке;
- NC_V — число пикселов цветового компонента в блоке по вертикали;
- NC_H — число пикселов цветового компонента в блоке по горизонтали.

Используя эту схему, цветовой режим видеоизображения промышленного телевидения, в котором на четыре яркостных точки приходится всего одна цветовая, можно определить следующим соотношением — 4:2:0.

Примечание

Следует помнить, что понижение цветовой плотности в системах классического цветного телевидения было вызвано огрвничением полосы пропускания канала, который использовался в системах черно-белого телевидения.

На рис. 3.4 представлены структуры макроблоков, используемых для представления видеоизображений в различных цветовых режимах.

Для представления видеоизображения, сформированного классическими телевизионными системами (схема 4:2:0), обычно применяется схема, в которую входят три макроблока (рис. 3.4, *а*). Один из макроблоков определяет четыре блока яркостного компонента видеоизображения, а два других — соответствующие блоки цветоразностных компонентов. Макроблок, структура которого представлена на рис. 3.4, *б*, может быть использован для представ-

ления видеоизображения с повышенной цветовой четкостью. В системах ТВЧ, как правило, используется полный цветовой режим, в котором на каждый пиксел видеоизображения приходится по три цветовых точки. Структура макроблока, который может быть использован для представления такого видеоизображения, представлена на рис. 3.4, *в*.

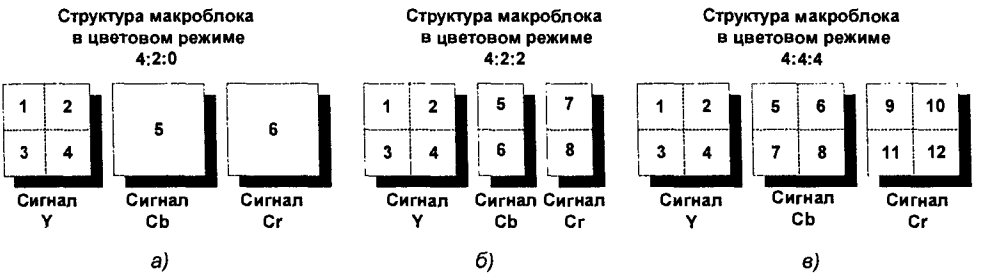


Рис 3.4. Структуры макроблоков, используемых в различных цветовых режимах

Дальнейшее развитие получили в кодеке MPEG-2 принципы и механизмы мультиплексирования и взаимной синхронизации различных информационных потоков в едином канале. Этими потоками могут быть аудио- и видеокомпоненты обычного видеофильма, а также разнообразные сигналы и команды систем, обслуживающих его трансляцию, например, системы шифрования и защиты от несанкционированного копирования. Для обозначения потока, который был получен от одного из таких источников, в кодеке MPEG-2 используется специальный термин — элементарный преобразованный поток *PES* (Packetized Elementary Stream). В зависимости от своего назначения, потоки PES могут быть мультиплексированы в один из двух суммарных выходных потоков кодека MPEG-2:

- *программный поток (Program Stream)*;
- *транспортный поток (Transport Stream)*.

В программном потоке обычно объединяются элементарные потоки, предназначенные для передачи по относительно надежным каналам, которые используют единую синхронизацию. Примерами таких потоков являются видеоизображение и звуковое сопровождение видеофильма, передаваемого по сетям кабельного телевидения. Данные программного потока передаются в блоках переменной длины — от одного до нескольких килобайт.

Транспортный поток, как правило, применяется для объединения и передачи служебных потоков. Характерным примером подобных потоков являются сообщения, используемые в процессе шифрования передаваемого сигнала:

- сообщения управления — *ECM* (Encryption Control Message);
- сообщения обслуживания — *EMM* (Encryption Management Message).

Данные транспортного потока передаются в блоках постоянной длины — 188 байт, что также обеспечивает возможность применения этого канала для передачи сжатых видео- и аудиосигналов по недостаточно надежным каналам.

Спецификация MPEG-4

Работы комитета ISO/IEC JTC1/SC29/WG11 по подготовке спецификации кодека завершились в 1998 году выпуском стандарта ISO/IEC 14496 "INFORMATION TECHNOLOGY -- CODING OF AUDIO-VISUAL OBJECTS". При разработке этого документа специалисты MPEG сделали логичный и важный шаг вперед, связав в единое целое процессы компрессии, анализа и синтеза мультимедийных объектов. В отличие от предшествующих документов, разработанных рабочей группой MPEG и описывающих способы кодирования компонентов мультимедийных потоков, основной акцент в спецификации MPEG-4 сделан на построение единой концепции описания, синтеза и преобразования мультимедийных объектов. В этом документе введен ряд терминов и понятий, используемых для описания мультимедийных объектов и их компонентов.

Определение

Графическая сетка (Mesh) — конструкция, состоящая из связанных элементарных графических элементов, которая используется для описания силуэта или поверхности визуального объекта.

Документ MPEG-4 не только определяет новые методы кодирования мультимедийных объектов, но и устанавливает области применения этих методов, а также способы их взаимодействия с определенными ранее методами кодирования. Таким образом, повышение эффективности кодирования достигается гибким сочетанием кодирования точек и однородных областей изображения с объектно-ориентированным кодированием *(Content-Based Coding)* объектов, которое способно наиболее полно учитывать специфические особенности этого объекта.

Технические решения, предложенные в спецификации MPEG-4, обеспечивают:

- эффективное сжатие мультимедийных объектов;
- эффективное кодирование текстур для их отображения на двумерные и трехмерные графические сетки;
- эффективное сжатие объектов, представленных двумерными графическими сетками;
- эффективное кодирование геометрических потоков, отображающих движение графических сеток;

- произвольный доступ к графическим объектам любого типа;
- расширение возможностей интерактивного взаимодействия с мультимедийными объектами;
- объектно-ориентированное кодирование, временное и пространственное масштабирование мультимедийных объектов;
- компенсацию воздействия ошибок на процесс передачи мультимедийного потока.

Так же, как и предыдущие спецификации, MPEG-4 содержит несколько разделов, в каждом из которых определяются специфические приемы и методы кодирования для мультимедийных объектов каждого из существующих типов. Предложенный в MPEG-4 новый подход к представлению и кодированию видеоизображений основывается на представлении видеоизображения в форме многослойной *сцены (Scene)*. Сцена видеоизображения, в свою очередь, разделяется на *планы визуальных объектов — VOP* (Video Object Plane). Каждому из таких планов соответствует своя система графических координат, в пределах которой осуществляется построение и прогнозирование перемещений размещенных на нем *визуальных объектов — VO* (Video Object). Такой способ представления видеоизображений позволяет существенно повысить эффективность кодирования и трансляции видеоизображений путем использования особенностей отображения специфических визуальных объектов — спрайтов.

Определение

Спрайт (Sprite) — неподвижная фоновая область панорамного видеоизображения.

Классическим спрайтом является полностью или частично неподвижный задний план видеоизображения, например, климатическая карта при представлении прогноза погоды. Статический характер спрайта позволяет однократно выполнить кодирование и поместить его образ в специальный спрайт-буфер приемника, откуда этот спрайт будет отображаться наряду с остальными объектами текущей сцены. Использование спрайтов при кодировании видеоизображений позволяет резко сократить объем передаваемых данных, существенно повышая при этом неравномерность интенсивности формируемого видеопотока.

На рис. 3.5 приведена структурная схема блока кодирования видеоизображения MPEG-4. Основное отличие этой схемы от представленных ранее заключается в использовании нескольких блоков прогноза перемещения и наличии отдельного канала для формирования и кодирования силуэта изображения объекта.

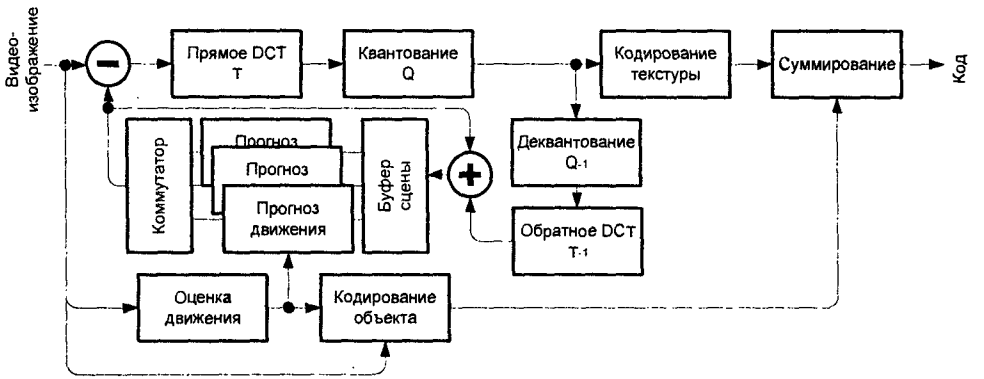


Рис. 3.5. Структурная схема блока кодирования видеоизображения MPEG-4

Описанная ранее концепция построения видеоизображения MPEG-4 позволяет обеспечить новые возможности интерактивного взаимодействия с мультимедийными объектами:

- управление положением зрителя относительно мультимедийной сцены;
  - изменение масштаба изображения;
  - изменение направления и угла обзора сцены;
- изменение состава мультимедийной сцены путем замены или перемещения входящих в нее мультимедийных объектов;
  - удаление или добавление мультимедийных объектов существующей сцены, например, замена сопровождающего звукового сигнала в видеофильме или замена диктора-комментатора;
  - включение или выключение мультимедийных потоков, связанных с объектами, например, отображение на экране вспомогательной текстовой информации о выбранном объекте.

Повышение эффективности кодирования в спецификации MPEG-4 обеспечивается благодаря использованию набора профилей, каждый из которых предназначен для конкретной группы графических и визуальных объектов. Каждому из таких профилей соответствует набор правил и методов кодирования, которые наиболее полно учитывают природу и специфику строения соответствующих образов. Визуальные объекты, определенные в спецификации MPEG-4, можно разделить на две основные категории:

- естественные визуальные объекты (Natural Video Objects);
- гибридные визуальные объекты (Synthetic/Natural Video Objects).

Образы первого из отмеченных типов создаются путем оцифровки визуальных изображений реальных объектов — фотографий, видеофильмов. Гиб-

ридные визуальные объекты имеют искусственную природу, однако могут иметь в своем составе элементы изображений естественных объектов.

В табл. 3.2 представлены краткие характеристики основных профилей, которые используются для кодирования видеоизображений в спецификации MPEG-4.

Таблица 3.2. *Профили, используемые для кодирования видеообъектов MPEG-4*

Название профиля	**Тип видеообъекта**	**Версия MPEG-4**	**Область применения**
Simple Visual Profile	Natural	>1	Мобильные абоненты
Simple Scalable Visual Profile	Natural	>1	Системы с программной реализацией кодеков и поддержкой QoS
Core Visual Profile	Natural	>1	Мультисервисные приложения IP
Main Visual Profile	Natural	>1	Развлекательные программы, DVD-приложения
N-Bit Visual Profile	Natural	>1	Системы оперативного наблюдения
Simple Facial Animation Visual Profile	Synthetic/ Natural	>1	Аудио/видеопрезентации
Scalable Texture Visual Profile	Synthetic/ Natural	>1	Видеоигры
Basic Animated 2-D Texture Visual Profile	Synthetic/ Natural	>1	Мультимедийные приложения
Hybrid Visual Profile	Synthetic/ Natural	>1	Мультимедийные приложения
Advanced Real-Time Simple Profile (ARTS)	Natural	>2	Телеконференции, видеофоны
Core Scalable Profile	Natural	>2	Интернет-приложения, мобильные абоненты, эфирная трансляция
Advanced Coding Efficiency (ACE) Profile	Natural	>2	Мобильные абоненты
Advanced Scaleable Texture Profile	Synthetic/ Natural	>2	WWW-камеры
Advanced Core Profile	Synthetic/ Natural	>2	Видеоигры

Простой визуальный профиль (Simple Visual Profile) предназначен для эффективного помехоустойчивого кодирования объектов с прямоугольными очертаниями. Объекты такого профиля создаются, например, в мобильных системах и не предъявляют высоких требований к ресурсам видеокодека.

Применение *простого расширяемого визуального профиля (Simple Scalable Visual Profile)* обеспечивает кодирование изменяющихся объектов в системах с ограниченными ресурсами, которые поддерживают более одного уровня качества обслуживания.

Базовый визуальный профиль (Core Visual Profile) предназначен для применения в мультимедийных приложениях сети Интернет. Алгоритмы этого профиля поддерживают кодирование изменяющихся объектов, которые имеют произвольный силуэт.

Способы кодирования, используемые для объектов *основного визуального профиля (Main Visual Profile)*, обеспечивают преобразование пересекающихся, полупрозрачных и спрайтовых объектов. Такие объекты характерны для развлекательных телевизионных программ, программ и приложений DVD.

Узкополосный визуальный профиль (N-Bit Visual Profile) предназначен для кодирования объектов, формируемых видеосистемами с пониженной четкостью изображения — от 4 до 12 бит на пиксел. Примером подобных видеосистем являются системы оперативного видеонаблюдения.

Простой профиль лицевой анимации (Simple Facial Animation Visual Profile) обеспечивает простые средства для анимации модели человеческого лица для использования в таких приложениях, как комплексные аудио/видеопрезентации.

Визуальный профиль для расширяемой текстуры (Scalable Texture Visual Profile) позволяет выполнять эффективное кодирование неподвижных объектов, и предназначен для применения в приложениях с несколькими слоями подвижных и неподвижных объектов. Объекты такого рода используются в видеоиграх, а также создаются неподвижными цифровыми камерами, имеющими высокую степень графического разрешения.

Визуальный профиль двумерной текстуры (Basic Animated 2-D Texture Visual Profile) обеспечивает анимацию графических сеток неподвижных изображений и предоставляет средства для анимации упрощенной модели человеческого лица.

Гибридный визуальный профиль (Hybrid Visual Profile) сочетает в себе возможность кодирования частично ограниченных и изменяющихся натуральных объектов с возможностью кодирования частично-синтетических гибридных объектов. Примерами таких объектов являются анимированные неподвижные изображения или упрощенные модели человеческого лица. Этот

профиль предназначен для использования в мультимедийных приложениях, насыщенных разнообразными образами.

Расширенный простой профиль реального времени — ARTS (Advanced Real-Time Simple Profile) обеспечивает эффективное помехоустойчивое кодирование объектов с прямоугольными очертаниями. Характерной чертой кодеков, применяемых для обработки образов этого профиля, является высокая стабильность формирования кодов и малая задержка, вносимая кодеком.

Основное назначение *центрального масштабируемого профиля (Core Scalable Profile)* состоит в поддержке изменения масштаба представления объектов или выделенной зоны интересов с сохранением четкости отображаемого изображения. Предполагается, что объекты данного профиля будут использоваться интернет-приложениями, мобильными абонентами, а также применяться при эфирной трансляции телевизионных программ.

Расширенный профиль повышенной эффективности кодирования — ACE (Advanced Coding Efficiency) применяется для уменьшения требований к каналам используемых для передачи формируемых кодов объектов, которые имеют прямоугольные очертания или произвольный силуэт. Целесообразно применение этого профиля в системах, допускающих некоторое снижение качества представления объекта для повышения эффективности его кодирования.

Расширенный текстурный масштабируемый профиль (Advanced Scaleable Texture Profile) предназначен для кодирования фоновых образов и неподвижных объектов с произвольным силуэтом. Областью применения этого профиля является отображение неподвижных объектов через Интернет, WWW-камеры.

Расширенный базовый профиль (Advanced Core Profile) сочетает в себе возможность кодирования видеообъектов, имеющих произвольный силуэт, с возможностью кодирования неподвижных и фоновых объектов, имеющих произвольные очертания. Этот профиль предназначен для применения в разнообразных потоковых мультимедийных приложениях.

В спецификации MPEG-4 также определяется основанный на языке VRML двоичный формат, который позволяет описывать и синтезировать видеоизображения — *BIFS* (Binary Format for Scenes).

Большое разнообразие определенных в спецификации способов кодирования позволяет эффективно применять кодеки MPEG-4 в мультисервисных системах различного назначения. Выбор соответствующего способа кодирования определяется совокупностью значений следующих характеристик:

- пропускной способностью используемого канала передачи данных;
- параметрами формируемого видеоизображения;
- номенклатурой поддерживаемых функций управления потоком.

Так, например, изображения, формируемые приложениями с невысокой информационной скоростью — *VLBV* (Very Low Bit-rate Video), имеют следующие характеристики: частоту смены кадров не более 15 Гц, размер видеоизображения при этом не превышает стандартного формата CIF. Пропускная способность канала передачи данных, которую могут использовать подобные приложения для передачи видеопотока, обычно лежит в пределах от 5 до 64 Кбит/сек. Для управления видеопотоком в подобных приложениях используется базовый набор функций, который включает в себя произвольный доступ к компонентам потока, прямой и обратный ускоренный поиск. Применение классического алгоритма сжатия, основанного на двумерном DCT-преобразовании с прогнозированием перемещений, для кодирования потоков таких приложений обеспечивает приемлемый уровень качества формируемых видеоизображений и достаточную эффективность использования канала передачи данных.

В высокоскоростных приложениях *(High Bit Rate)* обычно используется такой же набор функций, как и в приложениях VLBV. Отличия между этими приложениями определяются только характеристиками формируемых видеоизображений. Применение алгоритмов сжатия с увеличенной точностью прогноза MPEG-4 позволяет передавать мультимедийные потоки с разрешением и качеством систем ТВЧ по каналам с пропускной способностью от 64 Кбит/сек до 10 Мбит/сек.

Поддержка в кодеке MPEG-4 режимов VLBV и High Bit Rate обеспечивает его обратную совместимость с кодеками предыдущих спецификаций MPEG. Расширенный набор функций управления, так же как и модернизированные методы кодирования, оформлен в MPEG-4 в виде алгоритмических дополнений и функциональных расширений ядра предшествующих спецификаций, что обеспечивает возможность дальнейшего наращивания его функций и возможностей.

Оценки эффективности и качества сжатия видеоизображений

Основным критерием эффективности сжатия видеоизображения является соотношение объемов данных, которые передаются оцифрованным и исходным видеосигналами. Это соотношение называется *степенью сжатия* (Compression Ratio) и изображается в виде частного от деления объема исходного видеоизображения на объем сжатого видеоизображения. В среднем современные алгоритмы кодирования обеспечивают значения от 20 до 80 степени сжатия видеоизображений.

В качестве критерия для оценки качества преобразования и восстановления видеоизображений принято использовать максимальное значение *соотноше-*

ния сигнала и шума — *PSNR* (Peak Signal-to-Noise Ratio). Как и в случае с оцифрованным голосовым сигналом, появление шума вызвано квантованием и кодированием, которые вносят искажения в исходный видеосигнал. Поэтому для вычисления PSNR используется частное от деления максимальной амплитуды оцифрованного видеосигнала на значение среднеквадратичного отклонения исходного и оцифрованного видеосигналов, выраженное в децибелах (dB). Значения PSNR в диапазоне 30—35 dB обычно соответствуют изображению удовлетворительного качества, от 35 до 40 dB — хорошего качества. Кодирование видеоизображения со значением PSNR свыше 45 dB не вносит в него изменений, заметных человеческому глазу.

Следует учитывать, что эффективность сжатия и качество преобразования сильно зависят от характера кодируемого изображения, поэтому для сравнения различных кодирующих схем обычно принято использовать эталонные видеообъекты. Однако даже в этом случае получаемые результаты не могут быть признаны достаточно объективными, поскольку различные реализации одного алгоритма кодирования видеоизображений могут достаточно сильно отличаться друг от друга. В силу этих причин приводимые в табл. 3.3 обобщенные характеристики видеокодеков имеют достаточно условный характер.

Таблица 3.3. *Обобщенные характеристики видеокодеков*

Степень сжатия	Значение соотношения сигнала и шума, иначе PSNR (dB)		
	H.261/MPEG-1	H.263/MPEG-2	MPEG-4
Менее 10	Более 40	Более 50	Более 55
10:1	37—39	41—48	46—50
20:1	36—38	37—45	39—48
50:1	33—37	33—45	36—47
100:1	33—35	32—40	35—45
Более 100	Менее 30	Менее 30	Менее 35

Представленные в приводимой таблице данные позволяют сделать однозначный вывод о том, что по сравнению с предшествующими моделями современные кодеки, как правило, обеспечивают большую степень сжатия изображения при том же качестве передачи видеоизображения.

Идентификация и защита цифровых продуктов MPEG

В отличие от описанных ранее документов MPEG-1, 2 и 4 спецификации MPEG-7 и MPEG-21 не содержат описания алгоритмов синтеза или кодиро-

вания мультимедийных объектов. Оба этих документа, однако, играют важную роль для организации процессов создания и распространения мультимедийных объектов, поскольку они регламентируют такие важные аспекты этих процессов, как организация описания и защиты от несанкционированного использования этих объектов.

Спецификация MPEG-7

Спецификация MPEG-7 ISO/IEC 15938 "INFORMATION TECHNOLOGY – MULTIMEDIA CONTENT DESCRIPTION INTERFACE", в частности, представляет собой стандарт описания мультимедийных объектов. Эта спецификация, безусловно, является важным звеном в цепи стандартов, подготовленных рабочей группой ISO/IEC JTC1/SC29/WG11, поскольку позволяет реализовать эффективную навигацию в среде мультимедийных объектов, без которой процессы производства и распространения этих объектов просто теряют смысл. Наличие корректного и информативного описания не только обеспечивает быстрый поиск мультимедийного объекта, но и расширяет возможности его использования при помощи контекстных ссылок или автоматического формирования профиля интересов абонента.

Описание может являться неотъемлемой частью мультимедийного объекта или храниться отдельно от него. В последнем случае между описанием и объектом должна быть организована двунаправленная информационная связь, например, через сеть Интернет.

Основными компонентами спецификации MPEG-7 являются:

- *набор средств описания* (Description Tools), предназначенный для описания содержания (content) мультимедийных объектов;
- *язык формирования описаний — DDL* (Description Definition Language), который используется для определения правил применения Description Tools;
- *системные средства*, которые обеспечивают взаимную связь и интеграцию описания с мультимедийным объектом во всех режимах его использования.

В состав средств описания входят следующие компоненты:

- *описатели — D* (Descriptors), определяющие синтаксис и семантику каждой из характеристик мультимедийного объекта;
- *схемы описания — DS* (Description Schemes), которые определяют структуру и смысловое содержание связи между характеристиками мультимедийного объекта, которые могут быть, в свою очередь, как описателями, так и схемами описания.

Язык формирования описаний DDL представляет собой модифицированный вариант языка XML. Суть модификаций состоит в адаптации базового языка

к специфике построения описаний мультимедийных объектов. По этим причинам в составе языка DDL можно выделить следующие составляющие компоненты:

- лексические конструкции языка XML;
- конструкции описания данных языка XML;
- специфические расширения MPEG-7.

Системные средства MPEG-7 описания мультимедийных объектов обеспечивают взаимодействие с другими объектами, что в конечном счете и определяет практический эффект внедрения системы описаний.

Спецификация MPEG-21

Спецификация MPEG-21 — ISO/IEC TR 21000 "INFORMATION TECHNOLOGY – MULTIMEDIA FRAMEWORK" регламентирует те аспекты построения инфраструктуры распространения мультимедийных объектов, которые не были раскрыты в спецификациях MPEG-4 и MPEG-7. Спецификация MPEG-21 определяет совокупность технических средств и процедур их применения, которые позволяют контролировать и регулировать все стадии процесса распространения мультимедийных объектов. Такой подход, в частности, позволяет единым образом определить процедуры и способы защиты объектов от несанкционированного изменения, использования и копирования.

В основе инфраструктуры распространения мультимедийных объектов находятся два ключевых понятия:

- понятие "цифровой продукт" Ц-Продукт;
- понятие пользователя в части его отношения к цифровому продукту (Digital Item User).

Примечание

В современных изданиях можно найти различные переводы и трактовки словосочетания "Digital Item" — такие, например, как "цифровой объект", "цифровой элемент". Такие трактовки являются недостаточно конкретными и акцентируют внимание на техническом аспекте понятия "Item", который в данном случае не является первичным. Сочетание "цифровой продукт" более полно раскрывает прагматическую сущность понятия "Digital Item" в контексте рассматриваемого документа, хотя и не обеспечивает достаточный уровень однозначности.

Понятия Digital Item и Digital Item User являются взаимосвязанными, поскольку мультимедийный объект становится цифровым продуктом только по отношению к потенциальному пользователю. В то же время, в контексте спецификации MPEG-21, критерием для разграничения групп пользователей является их отношение к цифровому продукту — Ц-Продукту. Например, можно таким способом определить группу конечных потребителей, которые при-

обретают Ц-Продукт без права его коммерческого использования, или группу провайдеров, которые имеют права на ограниченное количество демонстраций Ц-Продукта по своей сети, и т. д.

Таким образом, основным назначением спецификации MPEG-21 является определение технологий, которые обеспечивают различным группам пользователей возможность формировать и реализовывать свои права по отношению к Ц-Продукту: получать доступ, обменивать, продавать, а также выполнять другие манипуляции с ним.

Для определения содержания цифрового продукта в MPEG-21 применяются две дополнительные спецификации:

- *определение цифрового продукта — DID* (Digital Item Declaration);
- *идентификация цифрового продукта — DII* (Digital Item Identification).

В спецификации DID определяется совокупность универсальных средств, обеспечивающих построение адекватного функционального определения цифрового продукта, например, схемы или модели Ц-Продукта.

Комплекс средств DII применяется для определения способов идентификации Ц-Продукта в части связанных с ним прав собственности. Применение этих средств целесообразно, например, в том случае, когда цифровой продукт состоит из нескольких компонентов, с каждым из которых связаны независимые права интеллектуальной собственности (Intellectual Property — IP). В дальнейшем компоненты DII и DID используются при построении инструментов реализации и защиты прав собственности, связанных с данным цифровым продуктом.

Совокупность прав по отношению к Ц-Продукту определяет допустимые формы и способы употребления этого продукта конкретным пользователем. Сами по себе права также являются продуктом, что дает возможность управлять процессом делегирования прав на коммерческой основе. Именно поэтому значительная часть документа MPEG-21 посвящена определению комплекта инструментов для управления и защиты интеллектуальных и иных прав собственности, связанных с цифровым продуктом.

Для этих целей в спецификации MPEG-21 предлагается использовать:

- стандартные инструменты обслуживания и защиты прав интеллектуальной собственности — *IPMP* (Intellectual Property Management and Protection);
- язык выражения прав собственности — *REL* (Rights Expression Language) и соответствующий ему словарь — *RDD* (Rights Data Dictionary).

Таким образом, спецификации MPEG-7 и MPEG-21 в сочетании с MPEG-4 образуют единый блок документов, определяющих общие принципы созда-

ния, распространения и использования мультимедийных объектов. Тесная взаимная связь предлагаемых в этих документах технических решений позволяет реализовать на их основе эффективную и надежную инфраструктуру, которая способна обеспечить качественное и управляемое распространение разнообразных мультимедийных объектов по сетям передачи данных с коммутацией пакетов (Интернет/Ethernet).

Видеоприложения современных мультисервисных сетей

В силу своей информационной насыщенности и интенсивности создаваемых информационных потоков, видеоприложения, бесспорно, сегодня представляют собой основу современных мультисервисных сетей. Требования именно этих приложений определяют значения основных характеристик современных ЛВС. К наиболее популярным коммерческим видеоприложениям, безусловно, относятся разнообразные формы телевизионного вещания. Среди интенсивно развивающихся в последнее время некоммерческих видеоприложений следует выделить системы проведения видеоконференций и оперативного видеонаблюдения.

Коммерческие видеоприложения

Вследствие высокой популярности, разнообразные телевизионные системы, безусловно, были и остаются основной формой коммерческих видеоприложений.

В отличие от прежних систем промышленного телевидения, которые разрабатывались в расчете на передачу телевизионного сигнала в аналоговом виде по узкополосному радиоканалу, современные телевизионные системы ориентированы в первую очередь на цифровую форму представления видеосигнала. Такое решение позволяет выполнить трансляцию телевизионного сигнала по цифровым сетям передачи данных и позволяет существенно повысить качество передаваемого телевизионного изображения.

В последнее время коммерческое телевидение все больше отходит от классической схемы прямого вещания. Появление и бурное развитие интерактивных телевизионных услуг привело к необходимости создания новых технологий и форм доставки видеотрафика. Существующие и перспективные способы доставки цифрового телевизионного сигнала, далеко не последнюю роль в которых играют технологии Интернета, находятся в стадии становления, что делает особенно важным вопрос выбора правильного направления их дальнейшего развития.

Форматы цифрового телевизионного вещания

Основным стимулом для развития и внедрения цифровых форматов телевизионного вещания являются постоянно растущие требования к качеству представляемого видеоизображения. Применение цифровой формы передачи телевизионного сигнала позволяет одновременно существенно повысить информационную насыщенность этого сигнала и защитить от воздействия помех и искажений при его передаче. Характерными особенностями изображения цифрового телевидения являются:

- увеличение размера изображения с одновременным повышением его цветовой плотности;
- применение прогрессивного режима формирования изображения;
- увеличение частоты смены кадров;
- поддержка панорамного формата видеоизображения.

В зависимости от характеристик формируемого изображения цифровые телевизионные системы могут быть разделены на три основные категории:

- *цифровое телевидение стандартной четкости* — *SDTV* (Standard-Definition Television);
- *цифровое телевидение повышенной четкости* — *HDTV* (High-Definition Television);
- *цифровое телевидение сверхвысокой четкости* — *UHDV* (Ultra High Definition Video).

Основные характеристики цифровых телевизионных систем приведены в табл. 3.4.

Таблица 3.4. *Основные характеристики цифровых телевизионных систем*

Характеристика	SDTV (SD)	HDTV (HD)	UHDV
Форматы видеоизображения	704×480 640×480	1280×720 1920×1080	7680×4320
Режим развертки	Interlaced	Interlaced, Progressive	Progressive
Пропорции видеоизображения	4:3, 16:9[1]	16:9	16:9
Частота повторения кадров (Гц)	25, 30, 60	50, 60	60
Цветовой режим	4:2:0,4:2:2	4:2:2,4:4:4	4:4:4
Протокол сжатия	MPEG-2	MPEG-2, MPEG-4	MPEG-4
Объем передаваемых данных[2] (Мбит/сек)	6—10	25—60	Более 1000

Примечания:

[1] Достигается при помощи изменений соответствующих размеров базового пиксела.

[2] С учетом сжатия передаваемого видеопотока.

Цифровые телевизионные системы стандартной четкости SDTV (SD) разрабатывались с учетом возможности приема формируемого сигнала обычными аналоговыми телевизионными приемниками. Именно поэтому размер, пропорции изображения и частота смены кадров SD соответствуют аналогичным характеристикам аналоговых телевизионных систем. Для преобразования цифрового телевизионного сигнала в аналоговую форму использовались специальные приставки (Set Top Box — STB). Применение цифровых телевизионных систем стандартного разрешения обеспечивает повышение качества доставки сигнала, но не позволяет добиться заметного улучшения качества передаваемого видеоизображения.

Качественное улучшение телевизионного видеоизображения может быть достигнуто только в специально разработанных для этого цифровых телевизионных системах повышенной четкости HDTV (HD). Плотность изображения в таких системах в среднем в четыре раза превышает плотность видеоизображения стандартных аналоговых телевизионных систем. Цифровой телевизионный сигнал этой системы может быть адекватно представлен только на экране специальных телевизионных приемников. Такие приемники, кроме встроенного блока декодирования цифрового сигнала, имеют панорамный экран с пропорциями, которые соответствуют полной зоне обзора — 16 (по горизонтали): 9 (по вертикали). Наряду с использованием прогрессивной развертки Progressive в системах HD поддерживается и чересстрочный режим (Interlaced), который применяется для обеспечения совместимости с предыдущими форматами и приложениями.

Примечание

В современных цифровых телевизионных системах принято использовать сокращенную форму записи формата изображения. Поскольку в этих телевизионных системах применяются только панорамные изображения стандартного формата 16:9, для его определения достаточно указать размер наименьшей стороны. Так, например формат 1920×1080, Interlaced в сокращенном виде будет записан, как "1080i". В некоторых случаях к сокращенной записи формата изображения добавляют значение частоты смены кадров, поэтому "1080p60" означает формат 1920×1080 с прогрессивной разверткой и частотой смены кадров 60 Гц.

Одновременное применение прогрессивной развертки и повышение до 60 Гц частоты повторения кадров в сочетании с панорамным обзором повышает у зрителя телевизионной системы HDTV ощущение полной реальности воспроизводимого на экране изображения.

Плотность изображения в перспективных цифровых телевизионных системах в 16 раз превышает плотность видеоизображения формата 1080, что, безусловно, еще более повышает эффект его восприятия. Однако высокие требования к пропускной способности канала, используемого для передачи видео-

сигнала, существенно ограничивают область возможного применения подобных систем.

Интерактивные видеосервисы VOD

Системы, предназначенные для предоставления услуги "Видео по запросу" — *VOD* (Video On Demand), обеспечивают абоненту возможность заказать доставку или трансляцию выбранного видеофильма или видеопрограммы. Абонент, использующий такую услугу, получает возможность просматривать заказанную видеопрограмму на собственном телевизионном приемнике или персональном компьютере. В процессе просмотра программы абонент может использовать стандартный набор функций управления воспроизведением, например, функции остановки кадра, прямой и обратной перемотки фильма.

Системы VOD могут быть построены на основе двух различных схем доставки заказанных программ абоненту:

- потоковая доставка видеопрограмм;
- доставка видеопрограмм по расписанию.

В первом случае процесс доставки видеопрограммы абоненту выполняется в реальном масштабе времени на фоне ее просмотра. При этом очередные фрагменты просматриваемой программы доставляются абоненту по высокоскоростному каналу прямым потоком или блоками с периодом 10—15 минут. Такой режим доставки обеспечивает возможность просмотра видеофильма практически сразу после оформления заказа и не предъявляет высоких требований к аппаратуре воспроизведения. Системы потоковой доставки, в свою очередь, подразделяются на две категории:

- упрощенные потоковые системы;
- полные потоковые системы — *T-VOD* (True Video-on-Demand).

Системы T-VOD используют прямую потоковую доставку и поэтому способны обеспечить абоненту возможность полного управления режимом просмотра принимаемой видеопрограммы. В отличие от T-VOD, в упрощенных потоковых системах применяется блоковая доставка видеопрограмм, что может существенно ограничить возможности абонента по управлению воспроизведением принимаемой видеопрограммы. Применение обоих вариантов потоковой доставки видеопрограмм в системах VOD целесообразно только при наличии высокоскоростного канала (не менее 6 Мбит/сек) у абонента до провайдера данной услуги.

В системах VOD, которые применяют доставку видеопрограмм по расписанию, абонент во время заказа видеопрограммы должен определить удобный для себя момент начала доставки с учетом расписания трансляции данной программы по сети провайдера. Абонент также должен соответствующим

образом обеспечить возможность записи транслируемой программы на воспроизводящее устройство. Сама доставка видеопрограммы в данном случае может осуществляться по относительно низкоскоростным каналам.

Передача данных в потоковых системах VOD может быть выполнена только в цифровом формате. Эти системы, безусловно, более привлекательны для клиента, но их реализация требует больших ресурсов.

Доставка видеопрограмм по расписанию в соответствующих системах VOD может быть выполнена в аналоговом или цифровом виде, причем форма доставки в данном случае определяется возможностями используемого канала. В системах VOD может также применяться гибридная доставка, когда при помощи специальной приставки передаваемая в цифровом формате видеопрограмма записывается на аналоговый видеомагнитофон.

Способы доставки цифрового телевизионного сигнала

Многочисленные разработки стандартов для передачи сигнала цифровых телевизионных систем были вызваны следующими основными причинами:

- необходимостью использования новых типов среды для передачи телевизионного сигнала;
- повышением требований к пропускной способности канала передачи данных;
- внедрением сервисов интерактивного вещания.

Бурное развитие и возникновение новых телекоммуникационных технологий привело к появлению новых средств и способов распространения телевизионного сигнала. Таким образом, в дополнение к классическим каналам дальнего вещания для передачи сигнала современных телевизионных систем могут быть использованы следующие каналы и среды:

- *коаксиальные кабельные сети* — *CS* (Cable System);
- *спутниковые каналы* — *SS* (Satellite System);
- *сети ближнего вещания* — *TS* (Terrestrial System);
- *сети высокочастотного вещания* — *MS* (Microwave System).

Повышение качества и увеличение плотности изображения современных телевизионных систем неминуемо приводит к резкому увеличению объемов передаваемого сигнала. Даже при условии использования современных алгоритмов сжатия, требования к пропускной способности канала передачи данных в системах HD в 8—10 раз превышают аналогичные параметры классических телевизионных систем.

Резкое увеличение количества телевизионных программ и появление разнообразных информационных и развлекательных ресурсов, таких, например,

как видеоигры или видеобиблиотеки, делает весьма актуальным обеспечение интерактивного взаимодействия абонента с системой предоставления услуги цифрового телевидения.

Для обеспечения доставки сигнала цифрового телевидения различными организациями были подготовлены три спецификации:

- европейская спецификация цифрового вещания — *DVB* (Digital Video Broadcasting);
- американская спецификация цифрового телевидения — *ATSC* (Advanced Television Systems Committee);
- японская спецификация цифрового вещания — *ISDB* (Integrated Services Digital Broadcasting).

Хотя эти спецификации являются полностью несовместимыми, у них можно найти достаточно много общего. Так в представленных спецификациях используются популярные алгоритмы линейного кодирования, такие, например, как *квадратурная амплитудная модуляция — QAM* (Quadrature Amplitude Modulation) или *фазовая манипуляция — PSK* (Phase-Shift Keying). Для каждой из используемых сред передачи во всех спецификациях применяются независимые методы формирования сигнала, которые лучше учитывают специфику организации вещания и распространения сигнала именно в этой среде. Так, например, в системах ближнего цифрового телевещания ATSC применяется восьмиуровневая *однополосная амплитудная модуляция — VSB* (Vestigial Sideband Modulation), которая обеспечивает хорошую помехозащищенность и большую дальность распространения сигнала. Основные характеристики систем цифрового вещания приведены в табл. 3.5. В этой таблице для систем цифрового вещания и типов среды передачи представлены характеристики используемой схемы линейного кодирования в формате A/B/R (алгоритм кодирования/полоса пропускания сигнала/информационная скорость).

Таблица 3.5. *Основные характеристики систем цифрового вещания*

Характеристика (Тип среды)	DVB	ATSC	ISDB
Стандарт	ETSI	ATSC	ARIB
Распространение	Европа	США, Канада, Мексика	. Япония
A/B/R (CS)	(16...256)-QAM	256-QAM / 6.0 / 38.8	—
A/B/R (SS)	QPSK, 8PSK, 16-QAM	—	QPSK / 40 / 35
A/B/R (TS)	(16...64)-QAM	8-VSB / 6.0 / 19.4	64QAM / 5.6 / 19

Все представленные выше спецификации цифрового вещания построены, как правило, по блочной иерархической схеме, что упрощает их реализацию и

модернизацию. В то же время, как уже было отмечено, все они являются взаимно несовместимыми и используют решения, не получившие общее признание или статус официального стандарта, что может существенно сдерживать внедрение этих спецификаций.

Системы IPTV

Комплексами интернет-телевидения — *IPTV* (Internet Protocol Television) — принято называть системы, в которых протоколы сети Интернет используются для трансляции телевизионных программ. Применение технологий Интернета в этих комплексах, однако, не ограничивается только внедрением более перспективных способов доставки телевизионных программ пакетного телевидения. В современном понимании IPTV представляет собой принципиально новую форму коммуникации, которая успешно сочетает в себе информационную полноту и насыщенность сети Интернет с богатыми графическими и акустическими возможностями современных телевизионных систем. Именно по этой причине развитию комплекса технологий IPTV уделяется повышенное внимание. Так, в частности, в рамках сектора ITU, который решает вопросы стандартизации технических решений в сфере телекоммуникаций, разработками базовых документов IPTV занимается специальная рабочая группа — ITU-T FOCUS GROUP ON IPTV.

Базовый комплект документов, подготовленный этой рабочей группой, включает в себя свод положений, определяющий приоритеты и направления развития технологий, объединенных под общим названием "IPTV". В одном из центральных документов этого комплекта содержатся определение и классификация услуг, которые могут быть предоставлены в системах IPTV (FG IPTV-ID-0026 "Classifications of IPTV service and its meaning").

В соответствии с приведенной в данном документе классификацией услуги, предоставляемые в системах IPTV, разделены на три основные группы:

- *базовые (канальные) услуги* (Basic Channel Service);
- *расширенные (избираемые) услуги* (Enhanced Selective Service);
- *интерактивные телематические услуги* (Interactive Data Service).

Базовый комплекс IPTV включает в себя стандартный набор услуг, предоставляемых в сетях кабельного и эфирного телевидения. Реализация этого комплекса обеспечивает возможность трансляции по сетям IP радио и телевизионных программ в сочетании с базовым комплексом услуг сетей передачи данных. При этом предполагается, что услуги базового комплекса не являются взаимосвязанными и могут предоставляться независимо.

Услуги расширенного комплекса IPTV реализуются в комплексах, которые обеспечивают активное взаимодействие абонента с системой, которая пре-

доставляет услугу. Для таких комплексов характерно наличие и активное использование обратных каналов. К услугам, предоставляемым в составе расширенного комплекса IPTV, относятся:

- различные варианты реализации услуги "Видео по запросу" — *VOD* (Video On Demand);
- трансляция музыкальных программ по запросу абонента — *MOD* (Music on Demand); услуга электронного гида по транслируемым программам — *EPG* (Electronic Program Guide);
- услуга "Персональный видеомагнитофон" — *PVR* (Personal Video Recorder);
- услуга "Деловой канал" — *B2B hosting* (Business to Business hosting) — предполагает организацию выделенного канала для обмена оперативными данными и проведения видеоконференций между подразделениями одной компании;
- услуга "Персональный канал" — *C2C hosting* (Customer to Customer hosting) — обеспечивает организацию выделенного канала для внутреннего обмена групп пользователей;
- услуга "Углы зрения" — (Multi-angle service) — обеспечивает пользователю возможность оперативно изменять ракурс обзора представляемого в видеопрограмме объекта.

Комплекс интерактивных телематических услуг сетей IPTV представляет собой расширенный набор информационных сервисов сети Интернет, объединенных в пяти тематических категориях:

- информационная категория (T-information);
- коммерческая категория (T-commerce);
- коммуникационная категория (T-communication);
- развлекательная категория (T-entertainment);
- образовательная категория (T-learning).

Услуги информационной категории обеспечивают возможность получения оперативных сообщений информационных служб, например, региональные и мировые новости, прогноз погоды.

Услуги IPTV, отнесенные к коммерческой категории, предназначены для поддержки сервисов, связанных с финансовыми расчетами и требующих повышенный уровень информационной безопасности. К таким сервисам в первую очередь можно отнести электронные покупки, участие в электронных аукционах, электронные операции с платежными средствами.

К услугам коммуникационной категории в описываемом документе отнесены классические информационные сервисы сети Интернет — электронная почта,

WWW, различные службы обмена сообщениями. В эту же категорию включены услуги VoIP, видеоконференции и видеофоны.

Развлекательная категория включает в себя сервисы, которые обеспечивают организацию сетевых видеоигр, фотоальбомов и караоке.

Услуги образовательной категории предназначены для организации и поддержки дистанционного обучения различных уровней — начиная от начальной школы вплоть до высших учебных заведений. Специальные образовательные услуги, такие, например, как изучение иностранных языков, также отнесены к данной категории.

Нетрудно заметить, что по замыслу авторов документа комплексная система IPTV претендует на роль единой платформы, способной предоставить полный комплекс информационных услуг для организации или конечного абонента.

Основным преимуществом телевизионных систем, основанных на протоколе сети Интернет, является способ организации доставки телевизионных программ. В отличие от классических систем телевидения, которые основаны на вещании всем абонентам всего комплекса программ, абонент IPTV сам определяет состав и насыщенность приходящего к нему информационного потока, что существенно снижает требования к пропускной способности наиболее протяженной части канала доставки программ.

В противоположность системам классического телевидения, интернет-телевидение является интерактивным по своей природе и предполагает активное использование двунаправленного информационного обмена с абонентом. Это, естественно, намного упрощает внедрение в системах IPTV перспективных информационных, телевизионных и гибридных услуг, основанных на активном диалоге с абонентом.

В комплексах, основанных на протоколах сети Интернет, традиционно применяются только популярные и открытые протоколы, что не только снижает затраты на их построение, привлекает потенциальных абонентов, но и обеспечивает возможность их постоянного дальнейшего развития.

Естественно, невозможно оспорить тот факт, что протоколы сети Интернет в очень малой степени приспособлены для передачи интенсивного потокового трафика, но история развития телекоммуникаций уже видела немало примеров тому, как неприспособленная, но популярная технология успешно завоевывала новые области своего применения.

Некоммерческие видеоприложения

В течение достаточно долгого времени применение видеосистем в быту и на производстве было очень ограниченным вследствие высокой стоимости ви-

деооборудования. Еще не так давно только очень крупные и преуспевающие организации могли организовать и использовать системы оперативного видеонаблюдения или системы проведения видеоконференций. Успехи микроэлектронной промышленности привели к тому, что компактные видеосистемы высокого качества стали доступны не только для небольших организаций, но и для домашнего использования. Следует особо отметить, что внедрение технологий Ethernet и Интернета в различные компоненты некоммерческих видеосистем позволяет еще более удешевить и упростить построение гибких и управляемых комплексов на их основе.

Системы видеонаблюдения

Системы видеонаблюдения можно условно разделить на две основные категории:

- охранные системы оперативного наблюдения;
- бытовые системы видеонаблюдения.

Системы оперативного наблюдения, как правило, являются главной составной частью систем обеспечения безопасности любого объекта. Эти системы обеспечивают постоянный мониторинг и регистрацию всех событий, происходящих на контролируемой территории, и позволяют осуществить оперативную реакцию при возникновении нештатной или аварийной ситуации.

Основными компонентами систем оперативного видеонаблюдения являются:

- блок видеокамер оперативного наблюдения;
- устройства регистрации и обработки;
- устройства управления и мониторинга.

Современные системы оперативного наблюдения, как правило, строятся на основе цифровых технологий, что существенно упрощает процессы создания, эксплуатации и обслуживания компонентов системы. Например, организация видеоархива в аналоговых системах видеонаблюдения не может быть выполнена без участия оператора, который периодически выполняет установку и замену видеокассет, и, при необходимости — обслуживание видеомагнитофона. Цифровые видеоархивы автоматически создаются и хранятся на резервированном запоминающем устройстве сервера видеонаблюдения.

Обычная система оперативного видеонаблюдения включает в себя 5—10 специализированных цифровых видеокамер, основной и резервный серверы видеоархива, блок мониторов оперативного наблюдения. Подключение всех этих компонентов осуществляется по технологии IEEE 802.3 Ethernet к общей или выделенной ЛВС объекта. Цифровые камеры видеонаблюдения обеспечивают формирование цветного или черно-белого изображения форматов QCIF-4CIF с периодом смены кадров 25—30 Гц, что при использовании в

камере компрессии MPEG-4 соответствует трансляции видеопотока с предельной скоростью 0,2—0,8 Мбит/сек. Таким образом, суммарный пиковый трафик всех видеокамер системы не превысит 1% пропускной способности магистрального канала обычного коммутатора Ethernet, что позволяет сделать вывод о том, что для построения цифровой системы оперативного видеонаблюдения небольшой организации вполне могут быть использованы резервы пропускной способности ЛВС этой организации.

В дополнение к сказанному выше следует отметить, что цифровые системы оперативного наблюдения, основанные на технологиях IEEE 802.3 Ethernet и Интернета, гораздо проще интегрируются с остальными компонентами системы обеспечения безопасности. Так, например, сигнал на включение видеокамеры оперативного наблюдения может быть передан от другого компонента системы безопасности — турникета или цифрового замка. Видеокомпоненты могут быть также использованы в составе системы автоматической идентификации — по внешнему облику или изображению радужной оболочки глаза.

Бытовые системы видеонаблюдения, как правило, не требуют наличия регистрирующих устройств и поэтому вполне могут быть реализованы с использованием аналоговых компонентов (видеокамера, коаксиальный кабель и телевизор). Однако даже в этом случае достаточно привлекательным является цифровой вариант (WWW-камера, IEEE 802.3 Ethernet, персональный компьютер), поскольку в этом варианте гораздо проще произвести объединение изображения, передаваемого видеокамерой, с основным изображением отображающего устройства.

Системы проведения видеоконференций

Видеоконференции, безусловно, представляют собой одну из наиболее современных форм делового общения. Сочетание активного многостороннего диалога с возможностью одновременного представления разнообразных форм информационных материалов делает видеоконференции незаменимым инструментом во многих областях человеческой деятельности.

Оперативные совещания и презентации, проводимые в форме видеоконференций, предельно сокращают время принятия ответственных решений и существенно снижают общие административные расходы организаций.

Особенно важным, а в некоторых случаях просто незаменимым представляется использование видеоконференций в сферах образования и здравоохранения. В последнем случае видеоконференция может являться единственной формой проведения консультации, от которой зависит здоровье или жизнь пациента.

Важность и насущность видеоконференций была достаточно давно осознана разработчиками телекоммуникационного оборудования. В системах, постро-

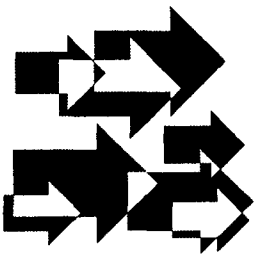
енных с использованием технологии ISDN, в частности, для обеспечения проведения видеоконференций предполагалось использовать оба гибридных канала "B"-типа из базового абонентского интерфейса BRI (совокупная пропускная способность — до 128 Кбит/сек). Однако применение одного BRI-канала существенно ограничивало возможности участников видеоконференции. Так, в частности, участники видеосовещания, подключенные к сети ISDN через один интерфейс BRI, не могли обмениваться оперативными данными через сеть общего пользования. Для проведения полнофункционального совещания или презентации необходимо было использовать несколько интерфейсов BRI, поэтому видеоконференции достаточно долго оставались дорогой и не очень полезной игрушкой для богатых.

Повышение скорости передачи данных в локальных сетях, построенных по технологии Ethernet, и развитие сервисов сети Интернет дали новую жизнь системам проведения видеоконференций. Такие свойственные этим технологиям качества, как гибкое и эффективное использование полосы пропускания канала, низкая стоимость оборудования и единство управления, делают построенные на их основе системы видеоконференций действительно полнофункциональными и дешевыми.

Основным компонентом системы организации видеоконференций ВКС (видеоконференц-связь) является видеотерминал, который представляет собой цифровой видеомонитор или проектор с установленной на нем видеокамерой. Видеотерминал выполняет функции формирования и отображения звуковых и видеопотоков в процессе проведения видеоконференции. Для организации минимальной двухточечной ВКС, таким образом, вполне достаточно двух видеотерминалов. Качество изображения ВКС целиком определяется параметрами используемых терминалов. Следует особо отметить, что в отличие от видеоизображений систем развлекательного телевидения, изображения ВКС имеют существенно более статичный характер, что обеспечивает гораздо более эффективное сжатие формируемого видеопотока стандартными кодеками MPEG-2 и MPEG-4. Так, например, при организации ВКС с изображениями форматов 4CIF или 16CIF интенсивность формируемого одним терминалом видеопотока не превысит значений порядка 0,5—1,0 Мбит/сек. Совершенно очевидно, что скорости передачи данных этого диапазона достаточно легко могут быть обеспечены в пределах современных ЛВС.

Существенное отличие ВКС от разнообразных систем видеонаблюдения заключается в том, что для распространения формируемого в них сигнала очень часто используются арендуемые каналы или сеть передачи данных общего пользования. В первом случае обеспечение требуемой для проведения видеоконференции полосы пропускания гарантируется специальным соглашением, которое заключается с провайдером арендуемого канала. Во втором случае требуемое значение пропускной способности может быть достигнуто использованием механизма QOS по схеме DiffServ.

ГЛАВА 4



Организация обмена в мультисервисных сетях

Наиболее популярным способом обмена в мультисервисных сетях является предоставление услуги по запросу (вызову). Параметрами такого вызова обычно являются адрес удаленного абонента и тип запрашиваемой услуги. Этот способ одинаково удобен и клиенту, и оператору, поскольку позволяет эффективно и экономично использовать выделяемые ресурсы. Информационный обмен, который выполняется в системах, основанных на этом принципе, разделяется на потоки двух категорий:

- *поток управляющих сообщений* — обмен, выполняемый системой для организации вызова;
- *поток мультисервисных данных* — обмен, выполняемый между вызываемым и вызывающим абонентами.

Для обеспечения надежного и эффективного управления потоками данных в мультисервисных сетях могут быть использованы разнообразные подходы. Так, например, в распределенных системах управления используется такая схема организации информационного обмена, когда в процессе создания и обслуживания вызова на равных правах участвует каждый из взаимодействующих абонентов. В иерархических системах задачи управления мультисервисным обменом распределены между центральным и оконечным оборудованием. Такой подход к построению систем управления применяется в системах традиционной телефонии и позволяет существенно снизить стоимость абонентских терминалов и упростить их обслуживание.

В первом разделе данной главы на примерах комплексов протоколов H.323 и SIP рассматриваются основные принципы построения распределенных систем управления информационным обменом в мультисервисных сетях.

Второй раздел посвящен рассмотрению принципов построения иерархических систем управления информационным обменом в мультисервисных се-

тях. В этом разделе, в частности, рассматриваются системы, основанные на использовании протоколов MEGAGO и MGCP. Кроме того, в этом разделе приведен обзор существующих технологий управления обменом в мультисервисных сетях и направлений дальнейшего развития этих технологий.

Распределенные системы управления

Распределенные системы управления используют такой же принцип организации информационного обмена, который обычно используется в сетях с коммутацией пакетов. Основное преимущество систем, построенных по распределенному принципу, заключается в их высокой надежности, поскольку в подобных системах отсутствует центральный координирующий элемент, неисправность которого приводит к отказу системы в целом.

Принцип распределенного управления информационным обменом в мультисервисных сетях использован при построении наиболее популярных технологий передачи мультимедийного трафика по сети с коммутацией пакетов — SIP (IETF) и H.323(ITU-T).

Принципы организации и компоненты сетей H.323

В рекомендации ITU-T H.323 "PACKET-BASED MULTIMEDIA COMMUNICATIONS SYSTEMS" приведены требования к составу и компонентам систем преобразования мультимедийных аналоговых сигналов для передачи их по сетям с коммутацией пакетов, в соответствии с которыми строятся современные системы интеграции трафика.

Управление информационным обменом в сетях H.323 основано на принципах, которые являются характерными для сетей с коммутацией каналов (PSTN, ISDN). В частности, система сигнализации H.323 основана на подмножестве стандартных сообщений, используемых для управления вызовом в системах ISDN, что облегчает организацию взаимодействия между этими системами.

Выполнение требований рекомендации H.323 обеспечивает:

- возможность управления полосой пропускания сети в интересах мультимедийных приложений;
- возможность взаимодействия компонентов сетей пакетной коммутации с компонентами сетей с коммутацией каналов;
- возможность организации многоточечных конференций;
- поддержку режима групповой адресации и многоадресной передачи;
- использование широкого спектра алгоритмов взаимного преобразования потоковых аналоговых сигналов в пакеты данных.

В соответствии с основными положениями рекомендации H.323 при построении подобных систем могут быть использованы следующие функциональные компоненты:

- терминалы или оконечные устройства (H.323 Terminals);
- шлюзы (H.323 Gateways);
- привратники (H.323 Gatekeepers);
- устройства управления многоточечными конференциями (H.323 MCU).

Терминал H.323 предназначен для обеспечения непосредственного доступа в сеть с коммутацией пакетов и выполняет прямое и обратное преобразование мультимедийных потоков данных в последовательность пакетов.

Шлюзы H.323 обеспечивают взаимодействие компонентов этой системы с внешними сетями. По сути, шлюз представляет собой устройство, осуществляющее взаимное преобразование форматов представления данных (например, между форматами H.225.0 и H.221) или взаимное преобразование процедур информационного обмена (например, между H.245 и H.242). В современных IP-сетях шлюзы H.323 обеспечивают взаимодействие с телефонной сетью общего пользования.

Привратник H.323 предназначен для управления шлюзами и терминалами H.323. При этом привратник выполняет следующие задачи:

- организацию и обслуживание процедур, трансляцию адресов, взаимный обмен адресной информацией с другими привратниками;
- регистрацию, аутентификацию и авторизацию пользователей, пользовательского оконечного оборудования и шлюза, сбор и накопление тарификационной информации;
- формирование запросов о выделении ресурсов сети с коммутацией пакетов (в данном случае — сети Интернет) для обеспечения передачи мультимедийной информации.

Устройства управления многоточечными конференциями H.323 предназначены для организации мультимедийного информационного обмена с участием трех и более абонентов. Эти устройства могут представлять собой отдельные объекты или могут быть реализованы в виде функциональных модулей, входящих в другие устройства H.323. Различают два вида модулей организации конференций:

- контроллеры конференций — Multipoint Controllers;
- процессоры конференций — Multipoint Processors.

Контроллеры конференций обеспечивают выполнение необходимых для организации конференций предварительных процедур по согласованию прото-

колов и форматов передачи данных. Контроллеры конференций могут в качестве функциональных модулей входить в такие устройства H.323, как терминал, шлюз и привратник.

Процессоры конференций предназначены для непосредственного управления потоками мультимедийной информации. Процессоры конференций могут в качестве функциональных модулей входить в такие устройства H.323, как шлюз и привратник.

Терминальные устройства H.323

Как уже было отмечено ранее, терминальные устройства H.323 выполняют прямое и обратное преобразование мультимедийных информационных потоков в последовательность блоков данных, предназначенных для передачи через сеть с коммутацией пакетов, в нашем случае — через сеть Интернет.

В состав терминального устройства H.323 могут входить следующие функциональные блоки:

- *видеокодек* (Video Codec);
- *аудиокодек* (Audio Codec);
- *канал передачи данных* (Data Channel);
- *блок управления системой* (System Control Unit).

Канал передачи данных не является обязательным компонентом терминалов H.323 и может быть использован для обеспечения информационного обмена между абонентами терминалов с использованием следующих режимов и функций:

- обмена файлами между участниками вызова (File exchange);
- совместного использования участниками вызова или конференции общего графического поля — электронной доски (Electronic whiteboard);
- доступа участников вызова к общим базам данных (Database access).

В зависимости от требований, предъявляемых реализуемым приложением, между терминалами H.323 может быть создан однонаправленный или двунаправленный канал передачи данных.

Рекомендация *T.120* "DATA PROTOCOLS FOR MULTIMEDIA CONFERENCING" определяет базовый набор требований по обеспечению взаимного информационного обмена при выполнении многоточечных конференций между терминалом H.323 и терминалами других типов (например, H.324). Формат данных, передаваемых по этому каналу, определен в рекомендации H.225.0.

В соответствии с требованиями рекомендации T.120, соединение создается при организации терминального вызова. Для обеспечения передачи данных

по этому соединению любая из взаимодействующих сторон может сформировать управляющее H.245-сообщение `Open Logical Channel`.

Примечание

Описание основных сообщений и функций управления логическими каналами H.245 приведено в последующих разделах настоящей главы.

Для обеспечения установления подлинности абонента сторона, инициирующая создание логического канала, должна передать в этом сообщении свой транспортный адрес (Transport Address). В том случае, если принимающая сторона согласна на установление логического канала с инициатором, то она формирует ответное сообщение `Open Logical Channel Acknowledge`.

Созданный таким образом логический канал может быть использован как для обеспечения информационных потребностей пользовательских приложений, так и для формирования команд управления для удаленного устройства.

Основные функции шлюза H.323

Необходимость использования шлюза возникает всякий раз, когда требуется обеспечить взаимодействие компонентов, использующих разные системы информационного обмена и формирования сигнальных сообщений.

Как уже было отмечено ранее, шлюз H.323 обеспечивает взаимодействие терминального оборудования с внешними сетями общего пользования. Шлюз может быть использован для выполнения обмена терминала H.323 с абонентом сети PSTN, а также для обеспечения взаимодействия терминала PSTN с абонентом сети H.323. В данном случае шлюзы будут осуществлять взаимное преобразование сигнализации PSTN и сигнализации управления вызовом H.323. При этом каждый из шлюзов будет выполнять роли двух терминалов — терминала PSTN и терминала H.323.

Назначение шлюза, таким образом, состоит в выполнении прямого и обратного преобразования форматов представления данных и сигнальных сообщений между взаимодействующими системами. Для реализации своих функций шлюз H.323 принимает активное участие в выполнении процедур построения и завершения вызова.

Минимальный набор операций, которые должен выполнять шлюз H.323, включает в себя:

- преобразование форматов передаваемых данных;
- согласование процедур организации вызова;
- согласование сигналов и процедур управления вызовом.

Функции шлюза H.323 могут выполнять стандартные маршрутизаторы (при наличии соответствующих интерфейсных модулей) или отдельные специали-

зированные устройства. Обязательным условием для реализации основной функции шлюза является наличие у него как минимум двух интерфейсов для подключения к различным системам информационного обмена и формирования сигнальных сообщений.

В том случае, если шлюз не может правильно интерпретировать сигнализацию, используемую некоторым вызовом, он должен пропустить такой вызов в сеть без изменений.

Задачи привратника в сети H.323

Привратник не является обязательным компонентом комплексов H.323. Задачей привратника является выполнение вспомогательных функций при организации вызовов терминалами H.323. Хотя привратник представляет собой логически обособленное устройство, его функции может выполнять по совместительству любой из имеющихся функциональных компонентов комплексов H.323 (терминал, шлюз и т. д.). Основная задача привратника H.323 состоит в обеспечении функционирования терминалов в его зоне ответственности.

Определение

Зоной ответственности привратника H.323 называется ограниченная группа логически связанных с ним терминалов, которые осуществляют информационное взаимодействие с внешними абонентами, используя функции, реализуемые на этом привратнике.

Привратник, таким образом, принимает на себя основные и вспомогательные функции организации вызова для терминалов зоны. Несмотря на то, что количество устройств, выполняющих функции привратника, не ограничено, только одно из них может считаться активным привратником данной зоны и выполнять соответствующие действия. Все остальные привратники считаются вспомогательными.

Активный привратник H.323 обеспечивает выполнение следующих основных и дополнительных функций:

- управления доступом (Admissions Control);
- управления пропускной способностью (Bandwidth Control);
- обслуживания зоны (Zone Management);
- управления сигнализацией вызовов (Call Control Signaling);
- авторизации вызывающего абонента (Call Authorization);
- распределения пропускной способности канала (Bandwidth Management);
- обслуживания вызовов (Call Management);
- преобразования адресов (Alias Address Modification).

Функция управления доступом относится к основным функциям, исполняемым привратником H.323. Для управления доступом к сети привратник использует описанные далее сообщения ARQ/ACF/ARJ рекомендации H.225.0. В качестве критериев аутентичности при организации дисциплины доступа могут быть использованы разнообразные характеристики и параметры вызываемого абонента. Допускается применение нуль-дисциплины, при использовании которой доступ ничем не ограничивается.

Функция управления пропускной способностью относится к основным функциям, исполняемым привратником H.323. Для управления пропускной способностью привратник использует сообщения BRQ/BRJ/BCF рекомендации H.225.0. Допускается применение нуль-дисциплины, при использовании которой все запросы на изменение пропускной способности удовлетворяются.

Функция обслуживания зоны относится к основным функциям, исполняемым привратником H.323. Эта функция заключается в выполнении всех описанных выше функций для терминалов H.323 и шлюзов, прошедших специальную процедуру регистрации в зоне.

Функция управления сигнализацией вызовов относится к вспомогательным функциям привратника H.323. При выполнении данной функции привратник принимает участие в организации вызова, выполняемого терминалом. В некоторых случаях привратник может полностью взять на себя управление организацией вызова у терминала своей зоны.

Функция распределения пропускной способности канала также является вспомогательной функцией привратника H.323. Исполнение этой функции заключается в отклонении вызовов, сформированных абонентами в условиях перегруженности сети.

Функция модификации адресов является вспомогательной функцией привратника H.323. Выполнение этой функции состоит в изменении направленного ему внутреннего адреса (alias-address). После внесения этого изменения вызывающая сторона должна использовать исключительно предложенное значение для организации вызова при поддержке привратника H.323.

Управляющие сообщения H.323

В системах управления обменом H.323 могут быть использованы управляющие сообщения трех уровней:

- сообщения обмена с привратником;
- сообщения управления вызовом;
- сообщения управления мультимедийным обменом.

Сообщения первого уровня применяются для реализации общих процедур управления доступом к сетевым ресурсам с использованием привратника. При помощи этих сообщений выполняется регистрация терминала в сети,

получение им информации о размещении удаленного абонента. Сообщения этого типа не используются, если процедура информационного обмена H.323 выполняется без участия привратника.

Сообщения второго уровня используются для организации и обслуживания вызова удаленного абонента. Эти сообщения применяются для передачи удаленному абоненту запроса на организацию вызова (Call). Примерами таких вызовов в сети H.323 могут быть телефонный разговор двух абонентов или телеконференция.

Сообщения третьего уровня применяются для организации и согласования параметров обмена мультимедийным трафиком по логическим каналам между удаленными абонентами H.323. При помощи этих сообщений выполняются такие функции, как согласование типов используемых кодеков и управление информационными потоками мультимедийных конференций.

Для управления доставкой мультисервисного трафика в реальном масштабе времени между терминалами в сети H.323 используются протоколы: *RTP* (Real-time Protocol — протокол реального времени) и *RTCP* (Real-time Control Protocol — протокол управления реального времени), применение которых регламентировано рекомендацией H.225.

Управление информационным обменом в сетях H.323, таким образом, имеет иерархический характер: управляющие сообщения предыдущего уровня обеспечивают возможность организации управляющего обмена на последующих уровнях.

Управление доступом H.225 (RAS)

Для выполнения функций управления доступом — *RAS* (Registration, Admission and Status) терминалы и привратники H.323 используют специальную группу сообщений, описанных в рекомендации *H.225.0* "CALL SIGNALING PROTOCOLS AND MEDIA STREAM PACKETIZATION FOR PACKET-BASED MULTIMEDIA COMMUNICATION SYSTEMS".

Для передачи этих сообщений используется специальный канал сигнализации (RAS signaling channel), не зависимый от канала, используемого для управления вызовами, или логического канала передачи данных. Сообщения, передаваемые по этому каналу, обеспечивают выполнение привратником всего комплекса операций по обслуживанию зоны вызовов — установление подлинности, авторизацию, учет трафика и т. д.

Все сообщения H.225 RAS, которые используются в процессе информационного обмена между привратником и терминалами, можно условно разделить на две группы:

- управляющие сообщения H.225 RAS;
- служебные сообщения H.225 RAS.

Управляющие сообщения H.225 RAS предназначены для согласования основных параметров информационного обмена, который терминалы H.323 выполняют с использованием привратника.

В соответствии с выполняемыми функциями управляющие сообщения RAS можно разделить на шесть групп:

- сообщения обнаружения терминала и привратника — TERMINAL AND GATEWAY DISCOVERY — G. Управляющие сообщения этой группы терминалы H.323 используют для поиска привратников;
- сообщения регистрации и завершения регистрации — TERMINAL AND GATEWAY REGISTRATION / UNREGISTRATION — R / U. Управляющие сообщения этих групп используются терминалами H.323 для выполнения процедур регистрации и отмены регистрации на привратнике;
- сообщения управления доступом к сети с коммутацией пакетов — TERMINAL TO GATEKEEPER ADMISSION — A. Эти управляющие сообщения используются терминалами H.323 для определения параметров доступа к сетевому ресурсу;
- сообщения изменения параметров доступа — TERMINAL TO GATEKEEPER REQUESTS FOR CHANGES IN BANDWIDTH — B. Управляющие сообщения этой группы терминалы H.323 используют для того, чтобы изменить при необходимости установленные ранее параметры доступа к сетевому ресурсу;
- сообщения, применяемые для определения положения сетевого абонента — LOCATION — L. Этот тип управляющих сообщений применяется терминалами для определения сетевых адресов удаленного абонента;
- сообщения предписания или извещения о высвобождении занимаемых ресурсов — DISENGAGE — D. Управляющие сообщения этой группы терминалы и привратники H.323 применяют в тех случаях, когда возникает необходимость освобождения сетевых ресурсов, которые использовались ранее для организации вызова.

Каждую из групп управляющих сообщений RAS образуют сообщения трех категорий:

- запрос — REQUEST — RQ;
- подтверждение выполнения запроса — CONFIRMATION — CF;
- отказ в выполнении запроса — REJECT — RJ.

Инициатором некоторых запросов H.225 RAS может выступать как терминал, так и привратник. Смысл и порядок действий в таких случаях определяется типом конкретного сообщения. Так, например, сообщение DRQ, которое сформировал привратник, имеет директивный характер и предписывает терминалу

освободить сетевые ресурсы, занимаемые текущим вызовом. Запрос DRQ, полученный от привратника, не может быть отвергнут терминалом, его выполнение автоматически влечет за собой завершение соединения с удаленным абонентом, которое было установлено на этом терминале. Сообщение DRQ, сформированное терминалом, имеет информативный характер и предназначено для извещения привратника о высвобождении информационных ресурсов, которые были задействованы для организации завершенного вызова.

В табл. 4.1 приведен перечень основных управляющих сообщений H.225 RAS. В этой таблице для обозначения разнообразных терминальных компонентов H.323 — таких, например, как видеотерминал или шлюз, используется литера "T". Сочетание "GK" в этой таблице используется для обозначения привратника (Gatekeeper).

Таблица 4.1. *Основные управляющие сообщения H.225 RAS*

Сообщение	Запрос	Выполнение	Отказ	Инициатор запроса
TERMINAL AND GATEWAY DISCOVERY	GRQ	GCF	GRJ	T
TERMINAL AND GATEWAY REGISTRATION	RRQ	RCF	RRJ	T
TERMINAL / GATEKEEPER UNREGISTRATION	URQ	UCF	URJ	T, GK
TERMINAL TO GATEKEEPER ADMISSION	ARQ	ACF	ARJ	T
TERMINAL TO GATEKEEPER REQUESTS FOR CHANGES IN BANDWIDTH	BRQ	BCF	BRJ	T
LOCATION REQUEST	LRQ	LCF	LRJ	T
DISENGAGE	DRQ	DCF	DRJ	T, GK

Информационные сообщения RAS обеспечивают обмен служебной информацией между компонентами H.323, которые выполняют или обеспечивают доступ к сети коммутации пакетов. К сообщениям этого типа относятся:

- сообщения опроса текущего состояния выполняемого вызова (IRQ, IRR, IACK, INAK). Сообщения этой группы применяются для однократного или периодического предоставления привратнику дополнительной информации об указанном вызове;
- сообщения о доступности ресурсов (RAI, RAC);
- нестандартные сообщения (XRS, NSM);
- сообщение о паузе в обслуживании запроса (RIP).

В табл. 4.2 приведен перечень основных служебных сообщений H.225 RAS.

Таблица 4.2. *Основные служебные сообщения H.225 RAS*

Назначение сообщения	Обозначение	Источник сообщения
INFO REQUEST	IRQ	GK
INFO REQUEST RESPONSE	IRR	T
INFO REQUEST ACK	IACK	GK
INFO REQUEST NAK	INAK	GK
NON-STANDARD MESSAGE	NSM	GK, T, GW
MESSAGE NOT UNDERSTOOD	XRS	GK, T, GW
RESOURCE AVAILABILITY INDICATION	RAI	GW
RESOURCES AVAILABLE CONFIRMATION	RAC	GK
RAS TIMERS AND REQUEST IN PROGRESS	RIP	GK, T, GW

На рис. 4.1 приведена схема организации взаимодействия между терминалами и шлюзами H.323 с использованием протокола H.225 (RAS). На этой схеме представлены также три привратника — GK one.com, GK two.com и GK three.com, которые контролируют соответствующие зоны.

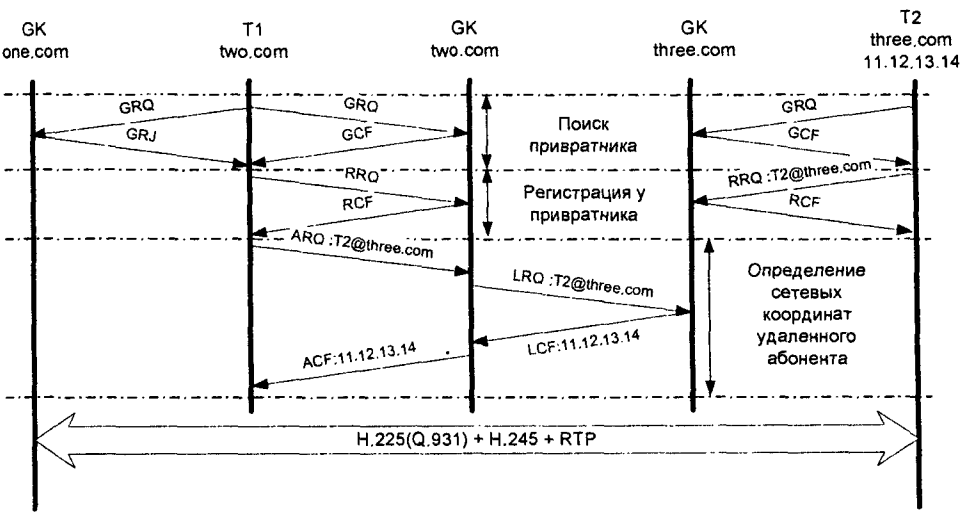


Рис. 4.1. Взаимодействие терминалов H.323 через сеть PSTN с использованием привратников

Оба терминала начинают свое взаимодействие с поиска привратников. Поиск терминалом T1 привратника GK1 (one.com) завершается неудачно, поскольку этот терминал находится вне зоны ответственности указанного привратника. На следующем этапе терминалы выполняют регистрацию на привратниках, после чего их сетевые координаты (адреса IP) становятся известными в зонах ответственности. После выполнения этого этапа привратники обмениваются адресами терминалов своих зон, что обеспечивает возможность организации непосредственного вызова между терминалами с использованием управляющих сообщений H.225(Q.931).

Управление вызовом H.225 (Q.931)

Для управления вызовом (Call Signaling) оконечные устройства H.323 используют те же процедуры и управляющие сообщения, которые применяются в системах классической телефонии. Именно эта особенность мультисервисных систем H.323 существенно упрощает их интеграцию и организацию взаимодействия с телефонными сетями общего пользования (PSTN). Основные принципы управления вызовом в телефонных сетях общего пользования определены в рекомендации *ITU-T Q.931 (1993)* "ISDN USER-NETWORK INTERFACE LAYER 3 SPECIFICATION FOR BASIC CALL CONTROL".

Описанные в этом документе процедуры и сообщения Q.931 обеспечивают выполнение следующих групп функций управления вызовом:

- *группа организации вызова* (Call Establishment). Функции этой группы обеспечивают передачу вызова удаленному абоненту и передачу оперативной информации о ходе установления вызова;
- *группа завершения вызова* (Call Clearing). Эта группа функций используется для обслуживания процесса завершения вызова, установленного между абонентами;
- *группа управления информационной фазой вызова* (Call Information Phase). Сообщения этой группы используются для реализации функций оперативного управления вызовом, таких, например, как приостановка и возобновление информационного обмена;
- *группа вспомогательных функций* (Miscellaneous). Эта группа включает в себя служебные функции Q.931, которые обеспечивают управление перегрузками, предоставление дополнительной информации о вызове.

Оконечные устройства — терминалы H.323 используют сокращенный набор управляющих сообщений Q.931, перечень которых приведен в H.225. Для указания подмножества сообщений Q.931, допустимых для использования в мультисервисных сетях H.323, принято использовать обозначение — H.225 (Q.931). Отсутствие в H.225 некоторых сообщений Q.931, принадлежащих к

группам организации, завершения и управления информационной фазой вызова объясняется спецификой информационного обмена в пакетных сетях. Именно по этой причине, в частности, функция завершения вызовом в H.225 реализуется в один этап с использованием одного сообщения (RELEASE COMPLETE). Аналогичная функция в сетях с коммутацией каналов использует три сообщения и реализуется в три этапа, поскольку кроме завершения вызова эта функция должна обеспечить высвобождение каналов, задействованных для его организации.

В табл. 4.3 приведены основные управляющие сообщения H.225 (Q.931).

Таблица 4.3. *Основные управляющие сообщения H.225 (Q.931)*

Сообщение*	Назначение сообщения	Группа Q.931
ALERTING	Передача уведомления о входящем вызове	Call Establishment
CALL PROCEEDING	Вызов обслуживается	Call Establishment
CONNECT	Вызов принят	Call Establishment
PROGRESS	Текущий статус процедуры установления вызова	Call Establishment
SETUP	Запрос на установление вызова	Call Establishment
SETUP ACKNOWLEDGE	Подтверждение запроса на установление вызова	Call Establishment
RELEASE COMPLETE	Вызов завершен	Call Clearing
USER INFORMATION	Доставка специальной информации абонента	Call Information
INFORMATION	Информация о состоянии вызова	Miscellaneous
NOTIFY	Уведомление о состоянии вызова	Miscellaneous
STATUS	Отчет о состоянии вызова	Miscellaneous
STATUS INQUIRY	Запрос о состоянии вызова	Miscellaneous

* Сообщения перечислены в алфавитном порядке.

На рис. 4.2 приведена схема организации взаимодействия между терминалами H.323 с использованием протокола H.225(Q.931). На первом этапе терминал T1 передает удаленному абоненту запрос на установление соединения.

После передачи сообщений, подтверждающих факт приема и установления вызова, между терминалами T1 и T2 начинается информационный обмен с использованием управляющих сообщений H.245.

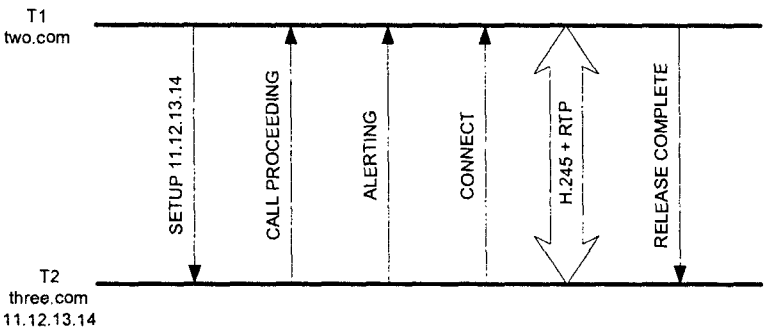


Рис. 4.2. Взаимодействие между терминалами H.323 с использованием протокола H.225 (Q.931)

Управление логическими каналами H.245

Функции управления логическими каналами обеспечивают реализацию специальных режимов мультисервисного взаимодействия между оконечными абонентами H.323. Для реализации этих функций в мультисервисных системах H.323 используются команды и сообщения, определенные в рекомендации *ITU-T H.245* "CONTROL PROTOCOL FOR MULTIMEDIA COMMUNICATION".

Все используемые в мультисервисных сетях H.323 функции управления логическими каналами H.245 можно условно разделить на следующие группы:

- определения ведущего и ведомого терминалов (Determination);
- обмена информацией о допустимых для терминалов режимах информационного обмена (Capability Set);
- управления логическими каналами (Open Logical Channel, Close Logical Channel, Request Channel Close);
- организации и обслуживания мультисервисных конференций;
- определения режима информационного обмена (Request Mode);
- вспомогательных и диагностических функций (Round Trip Delay, Maintenance Loop).

Для выполнения этих функций используются три категории информационного обмена между оконечными терминалами:

- обмен информационными сообщениями (Messages);
- передача управляющих команд (Commands);
- передача уведомляющих сообщений (Indication).

Информационные сообщения H.245, передаваемые в процессе информационного обмена между абонентами H.323, делятся на универсальные управляю-

щие сообщения и сообщения управления многоточечными конференциями. Обмен универсальными информационными сообщениями H.245 между терминалами имеет интерактивный характер и предполагает формирование следующих ответных сообщений:

- Подтверждение приема — `Acknowledge`;
- Отказ от выполнения — `Reject`;
- Завершение выполнения — `Release`;
- Подтверждение выполнения — `Confirm`.

Типичным примером универсального управляющего сообщения H.245 является сообщение `Open Logical Channel Confirm`, которое используется для подтверждения построения двунаправленного логического канала между терминалами.

В табл. 4.4 приведены универсальные управляющие сообщения H.245.

***Таблица 4.4.** Универсальные управляющие сообщения H.245*

Наименование	Объект управления	Сообщения
Determination	Статус терминала	`Acknowledge, Reject, Release`
Capability Set	Допустимые режимы обмена	`Acknowledge, Reject, Release`
Open Logical Channel	Логический канал — <номер>	`Acknowledge, Reject, Confirm`
Close Logical Channel	Логический канал — <номер>	`Acknowledge`
Request Channel Close	Логический канал — <номер>	`Acknowledge, Reject, Release`
Request Mode	Режим обработки данных	`Acknowledge, Reject, Release`
Maintenance Loop	Прием передаваемых данных	`Request, Acknowledge, Reject`
Round Trip Delay	Задержка распространения сигнала	`Request, Response`

Передача управляющих команд и уведомляющих сообщений H.245 выполняется терминалом H.323 в одностороннем порядке и не предполагает ответной реакции от абонента. В качестве примера управляющей команды можно привести команду `Broadcast My Logical Channel Me`, которая может быть использована для контроля потока, формируемого терминалом при проведении мно-

готочечной конференции. Типичным примером уведомляющего сообщения (Indication) H.245 является сообщение `Logical Channel Active`, которое используется для указания об изменении состояния выбранного логического канала.

Передача всех видов управляющих сообщений H.245 выполняется через специальный логический канал 0, который специально для этой цели создается между каждой парой взаимодействующих терминалов H.323.

На рис. 4.3 приведена схема организации взаимодействия между терминалами H.323 с использованием протокола H.245. На первом этапе терминалы обмениваются запросами о характеристиках удаленного терминала и о его статусе (Master/Slave). После согласования необходимых параметров терминалы T1 и T2 приступают к операциям по формированию между ними логических каналов. В дальнейшем по этим логическим каналам и будет осуществляться процесс информационного обмена между ними под управлением протокола RTP.

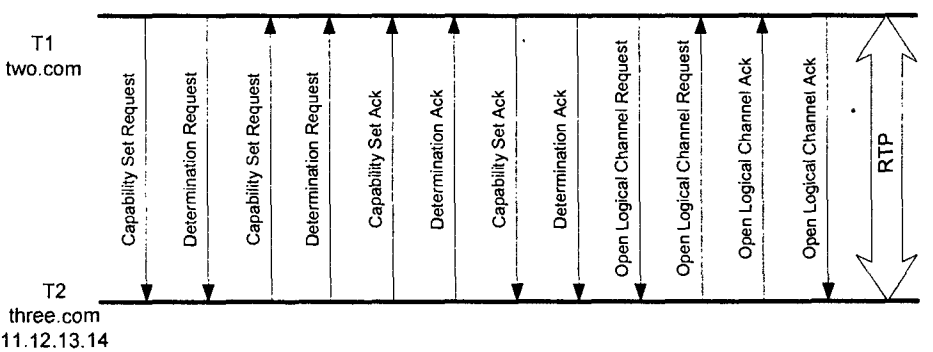


Рис. 4.3. Взаимодействие терминалов H.323 с использованием протокола H.245

Протокол SIP

Комплекс протоколов SIP так же, как и комплекс протоколов H.323, определяет основные компоненты и принципы реализации мультисервисных приложений в сетях общего пользования с коммутацией пакетов.

Основное назначение протокола организации вызова *SIP* (Session Initiation Protocol) состоит в обеспечении управления мультисервисным информационным обменом абонентов сети Интернет. Текущая версия спецификации протокола SIP представлена в документе IETF RFC 3261 SIP: Session Initiation Protocol: June 2002: Category — Standard Track.

Компоненты SIP

Компоненты сетей, построенных на основе протокола SIP, обеспечивают реализацию следующих этапов и функций информационного взаимодействия:

- *определение текущего положения мобильного абонента* (User location). Эта функция включает в себя автоматическую регистрацию абонента и динамическое определение параметров сетевого соединения с этим абонентом;
- *определение доступности абонента* (User availability). При реализации этой функции учитываются организационные аспекты установления соединения с удаленным абонентом;
- *определение возможностей абонента* (User capabilities). При реализации этой функции учитываются технические аспекты соединения с абонентом, например, способы кодирования передаваемых данных и особенности организации информационного обмена;
- *установление вызова* (Session setup). При организации вызова все вовлеченные в него абоненты используют информацию, полученную на предварительных этапах — (User location и User capabilities);
- *обслуживание вызова* (Session management). Включает в себя решение задач по изменению состояния реализуемого мультисервисного вызова, например, подключение новых абонентов в конференцию, прием нового телефонного вызова на фоне текущего.

При ближайшем рассмотрении у протокола SIP можно найти достаточно много общих черт с популярным протоколом сети Интернет HTTP. Отмеченное сходство не является случайным, поскольку оба этих протокола обеспечивают обмен разнородными данными между абонентами сети Интернет.

Так же, как и в протоколе HTTP, информационное взаимодействие между абонентами SIP построено с использованием популярной модели "клиент-сервер".

Базовым логическим элементом сетей, основанных на применении протокола SIP, является агент абонента — *UA* (User Agent), который состоит из двух функциональных элементов:

- клиентский элемент абонента SIP — *UAC* (User Agent Client);
- серверный элемент абонента SIP — *UAS* (User Agent Server).

Задачами клиентского элемента UAC являются подготовка и формирование вызова удаленному абоненту SIP. Основной задачей серверного элемента является прием и обслуживание вызовов, которые поступают от удаленных абонентов SIP. В процессе своего функционирования агент абонента (UA) может попеременно или одновременно выполнять функции клиента и сервера.

В спецификации SIP определен также ряд логических компонентов, предназначенных для выполнения стандартных функций, применяемых при организации информационного обмена:

- сервер регистрации абонента (SIP Registrar);
- сервер маршрутизации вызова (SIP Redirect Server);
- промежуточный сервер (SIP Proxy Server).

Сервер регистрации абонента обеспечивает выполняемое по запросу от абонента занесение текущих значений его сетевых данных в общую базу данных о расположении абонентов (Location Data Base). Сервер маршрутизации вызова представляет собой специализированный UAS, который обеспечивает возможность построения альтернативных маршрутов доступа к удаленному абоненту. Промежуточный (Proxy) сервер представляет собой логический элемент SIP, который одновременно выполняет функции UAC и UAS при организации одного и того же вызова. Компоненты этого типа при необходимости могут быть использованы для маршрутизации вызовов, организуемых в сети SIP, а также для обеспечения управления доступом абонентов к сетевым ресурсам.

Сообщения SIP

Для организации информационного обмена в сети SIP используются сообщения двух категорий:

- *запрос клиента* (SIP Request);
- *отчет сервера* (SIP Response).

Особенность информационного обмена, применяемого в протоколе SIP, состоит в использовании относительно небольшого количества различных запросов. При этом, однако, в теле каждого из передаваемых запросов содержится достаточно аргументов для его успешной обработки. Выбор такого способа формирования сообщений объяснятся тем, что эти сообщения SIP в первую очередь предназначены для обработки программным, а не аппаратным способом.

В табл. 4.5 приведены перечень и основные функции запросов SIP.

Таблица 4.5. *Перечень и основные функции запросов SIP*

Название запроса	Назначение
ACK	Подтверждение приема отчета по текущему запросу INVITE
BYE	Завершение текущего вызова
CANCEL	Завершение попытки установления вызова

Таблица 4.5 (окончание)

Название запроса	Назначение
INVITE	Вызов удаленного абонента
OPTION	Уточнение параметров информационного обмена
REGISTER	Регистрация расположения абонента в базе данных

Все возможные варианты отчетов, формируемых сервером UAS в результате выполнения принятого от UAC запроса, разделены на 6 групп, каждой из которых соответствует свой диапазон изменения кода.

- Предварительная информация (Provisional): 100—199;
- Успешное завершение (Successful): 200—299;
- Изменение вызова (Redirection): 300—399;
- Ошибка запроса (Request Failure): 400—499;
- Ошибка сервера (Server Failure): 500—599;
- Глобальная ошибка (Global Failures): 600—699.

Отчеты группы Provisional сервер формирует в том случае, когда он выполняет текущий запрос, но пока еще не может сформировать итоговый отчет о выполнении этого запроса. Отчеты группы Redirection также являются предварительными и указывают на необходимость выполнения вызывающим абонентом дополнительных действий для обеспечения выполнения запроса. Группу Successful образуют окончательные отчеты об успешном завершении выполнения запроса.

В табл. 4.6 приведены предварительные и окончательные отчеты SIP.

Таблица 4.6. Отчеты SIP групп Provisional, Successful и Redirection

Код отчета	Наименование	Содержание отчета
100	Trying	Запрос обрабатывается сервером
180	Ringing	Абоненту передается уведомление о вызове
181	Call Is Being Forwarded	Вызов будет переадресован
182	Queued	Вызов помещен в очередь для обслуживания
183	Session Progress	Текущее состояние вызова
200	OK	Запрос успешно выполнен
300	Multiple Choices	Множественный выбор
301	Moved Permanently	Абонент изменил адрес

Таблица 4.6 (окончание)

Код отчета	Наименование	Содержание отчета
302	Moved Temporarily	Абонент временно изменил адрес
305	Use Proxy	Рекомендованный посредник
380	Alternative Service	Альтернативный вариант обслуживания

Отчет группы Request Failure указывает на то, что запрос, полученный сервером, содержит ошибку, которая не позволяет выполнить данный запрос именно на этом сервере. Клиент, получивший подобный отчет, не должен повторно передавать отвергнутый запрос на сервер, от которого был получен этот отчет. Примеры отчетов об ошибке запроса приведены в табл. 4.7.

Таблица 4.7. Отчеты об ошибках запросов SIP

Код отчета	Наименование	Содержание отчета
400	Bad Request	Некорректный запрос
401	Unauthorized	Требуется санкция
403	Forbidden	Отказ в обслуживании запроса
404	Not Found	Запрашиваемый ресурс не найден
405	Method Not Allowed	Метод доступа не разрешен
406	Not Acceptable	Запрос не является приемлемым
407	Proxy Authentication Required	Требуется аутентификация на посреднике
408	Request Timeout	Превышение времени ожидания отчета
410	Gone	Ресурс перемещен
413	Request Entity Too Large	Недопустимый размер запроса
414	Request-URI Too Long	Недопустимый формат адреса абонента
415	Unsupported Media Type	Недопустимый формат сообщения
416	Unsupported URI Scheme	Недопустимая схема адресации
420	Bad Extension	Недопустимое расширение протокола
421	Extension Required	В запросе отсутствует необходимое расширение
423	Interval Too Brief	Интервал обновления слишком мал
480	Temporarily Unavailable	Ресурс временно недоступен
481	Call/Transaction Does Not Exist	Вызов не существует

Таблица 4.7 (окончание)

Код отчета	Наименование	Содержание отчета
482	Loop Detected	Обнаружено зацикливание вызова
483	Too Many Hops	Длина маршрута слишком велика
484	Address Incomplete	Адрес не является полным
485	Ambiguous	Неоднозначный запрос
486	Busy Here	Вызываемый абонент занят
487	Request Terminated	Запрос прекращен
488	Not Acceptable Here	Указанный ресурс недоступен
491	Request Pending	Ожидается запрос
493	Undecipherable	Запрос не может быть дешифрован

Получение отчета об ошибке сервера (Server Failure) указывает на то, что данный сервер не в состоянии корректно обработать принятый запрос из-за возникшей на нем внутренней ошибки. Отчеты о возникновении глобальной ошибки формируются в том случае, если вызываемый абонент по какой-либо причине отказался от обслуживания запроса. Перечень отчетов о глобальных и серверных ошибках приведен в табл. 4.8.

***Таблица 4.8.** Отчеты SIP о глобальных и серверных ошибках*

Код отчета	Наименование	Содержание отчета
500	Server Internal Error	Внутренняя ошибка сервера
501	Not Implemented	Запрос не может быть выполнен
502	Bad Gateway	Неправильный шлюз
503	Service Unavailable	Услуга недоступна
504	Server Time-out	Превышено время ожидания ответа сервера
505	Version Not Supported	Версия не поддерживается
513	Message Too Large	Недопустимая длина сообщения
600	Busy Everywhere	Абонент занят и отказывается принимать вызов
603	Decline	Абонент отказывается принимать вызов
604	Does Not Exist Anywhere	Вызываемого абонента не существует
606	Not Acceptable	Параметры вызова неприемлемы для абонента

Организация информационного обмена SIP

Как уже было отмечено в предыдущих разделах данной главы, способы управления информационным обменом между абонентами сети SIP достаточно сильно отличаются от тех, которые используются в сетях коммутации каналов и гораздо больше напоминают методы, применяемые в сети Интернет. Так, например, используемый в SIP формат идентификатора сетевого ресурса — URI (Uniform Resource Identifier) — SIP: <USERNAME>@<DOMAIN> имеет много общего с форматом адреса сетевых ресурсов Интернета. Общность SIP с протоколами сети Интернет не только упрощает взаимную интеграцию стандартных сетей передачи данных и мультимедийных сетей, но и позволяет использовать проверенные и отработанные технологии при построении гибридных сетей. Так, в сетях, построенных на основе технологии SIP, успешно используются услуги стандартных приложений системы доменных имен — *DNS* (Domain Name System) для локализации сетевых ресурсов. Универсальный протокол описания сеансов связи в сети Интернет — *SDP* (IETF RFC 4566 — Session Description Protocol — July 2006 Category — Standards Track) применяется в сетях SIP для согласования параметров мультисервисного обмена. Малое количество используемых запросов и простота их обработки позволяет существенно упростить и ускорить процесс организации вызова в мультимедийных сетях SIP.

На рис. 4.4 приведена схема организации вызова с использованием Proxy-сервера в сети SIP.

Даже при использовании промежуточного сервера, или иначе Proxy-сервера, общее количество формируемых в данном случае запросов (5) будет существенно меньше, чем при реализации аналогичной схемы с использованием технологии H.323.

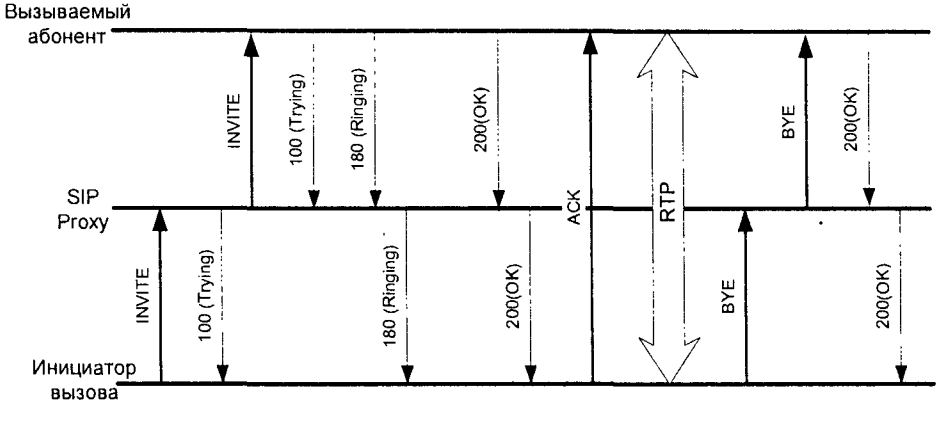


Рис. 4.4. Схема организации вызова в сети SIP с использованием Proxy-сервера

Обмен управляющими сообщениями в SIP организован таким образом, чтобы максимально повысить эффективность обработки этих сообщений в сетях с коммутацией пакетов. Так, например, логически завершенная последовательность управляющих сообщений SIP образует транзакцию (SIP Transaction). Каждая из таких транзакций изначально имеет уникальный идентификатор, что позволяет упростить их обработку на промежуточных серверах. В свою очередь последовательность транзакций, выполняемых между парой абонентов SIP, образует диалог между ними (SIP Dialog). Диалоги, определяемые идентификаторами вызывающего и вызываемого абонентов, образуют верхний уровень управляющего информационного взаимодействия SIP. Для управления непосредственной передачей мультимедийного трафика между абонентами в сетях SIP так же, как и в сетях H.323, используется протокол RTP.

Иерархические и гибридные системы управления

Несомненными достоинствами распределенных систем управления вызовами мультисервисных сетей, которые были представлены в предыдущих разделах данной главы, являются их гибкость и функциональная эффективность. В распределенных системах все функции организации и управления вызовом выполняются собственно терминальными устройствами, которые взаимодействуют с другими терминальными устройствами через имеющиеся в их распоряжении средства передачи данных.

Основными недостатками систем, в которых используются интеллектуальные терминалы, являются существенное увеличение стоимости приобретения и обслуживания оконечного оборудования. Кроме того, дальнейшая модернизация систем управления вызовами, построенных по распределенному принципу, может вызвать существенные трудности, поскольку при появлении новых услуг в мультисервисной сети соответственные изменения должны быть проведены на абсолютно всех терминалах.

Системы управления MEGACO/MGCP

В иерархических системах управления вызовом мультисервисных сетей используются принципы централизации управляющих функций и распределения функции обработки данных. Использование этих принципов позволяет существенно снизить стоимость построения и обслуживания мультисервисных сетей, а также облегчить процесс их дальнейшей модернизации.

Функция управления вызовом в иерархических системах выполняется центральным сигнальным шлюзом, а функции управления средой передачи дан-

ных возлагаются на периферийные канальные шлюзы, которые используются для управления информационными потоками в процессе обслуживания вызова. Для организации обмена управляющими и информационными сообщениями между сигнальным шлюзом и канальными шлюзами используются специальные управляющие протоколы.

Для создания иерархических систем управления вызовом могут быть использованы две независимые спецификации:

- *Протокол MEGACO* (Media Gateway Control) — IETF RFC 3015/ITU-T H.248;
- *Протокол MGCP* (Media Gateway Control Protocol) — IETF RFC 3435.

Протокол MEGACO

Протокол MEGACO (Media Gateway Control) предназначен для управления компонентами иерархических систем в процессе организации и обслуживания мультисервисного вызова с передачей данных по сети общего пользования.

Протокол MEGACO представляет собой плод совместных усилий специалистов IETF и ITU-T. Основные принципы организации этого протокола описаны в документах ITU-T H.248 "Gateway control protocol" и IETF RFC 3015 — Megaco Protocol Version 1.0. — November 2000 — Status:PROPOSED STANDARD.

Основными компонентами иерархических систем управления вызовом, построенных с использованием протокола MEGACO, являются:

- *сигнальный шлюз — MGC* (Media Gateway Controller);
- *канальный шлюз — MG* (Media Gateway).

Подключение информационных потоков к канальному шлюзу MEGACO выполняется через специальные элементы, которые называются *окончаниями* (MEGACO Terminations).

Определение

Окончание представляет собой логический компонент канального шлюза, который используется для коммуникации с внешними системами.

В состав канального шлюза могут входить физические и виртуальные окончания. Примером физического окончания у канального шлюза является подключенный к нему цифровой поток. В отличие от физического, виртуальное окончание организуется только на время обслуживания вызова. Примером виртуального окончания у канального шлюза является поток данных, который организуется и обслуживается с использованием команд протокола RTP.

Для описания способа обработки и коммутации потоков, поступающих или передаваемых через информационные окончания, используется понятие *контекста* канального шлюза (MEGACO Context).

Определение

Контекстом называется логический компонент канального шлюза, который используется для описания топологии коммутации информационных потоков между двумя и более окончаниями канального шлюза.

Одно окончание может принадлежать только к одному контексту. Все окончания, которые не принадлежат к какому-либо контексту, являются, по сути, изолированными и автоматически приписываются к нулевому контексту.

Таким образом, протокол MEGACO описывает перечень команд, которыми сигнальный шлюз управляет обработкой и коммутацией информационных потоков на канальном шлюзе. В табл. 4.9 приведены основные команды, которые используются для обмена между сигнальным и канальным шлюзами в протоколе MEGACO.

***Таблица 4.9.** Основные команды, которые используются в протоколе MEGACO*

Команда MEGACO	Назначение
ADD	Добавляет окончание к существующему контексту или создает новый контекст
MODIFY	Изменяет характеристики окончания
SUBTRACT	Удаляет окончание из существующего контекста или полностью удаляет контекст
MOVE	Переносит окончание из одного контекста в другой
AUDITVALUE	Возвращает текущее состояние окончания
AUDITCAPABILITIES	Возвращает текущие характеристики окончания
NOTIFY	Информирует сигнальный шлюз об изменении состояния канального шлюза
SERVICECHANGE	Информирует сигнальный шлюз об изменении состояния одного или нескольких окончаний канального шлюза

Протокол MGCP

Протокол MGCP (Media Gateway Control Protocol) так же, как и протокол MEGACO, предназначен для управления компонентами иерархических систем в процессе организации и обслуживания мультисервисного вызова с передачей данных по сети общего пользования. Основные положения протоко-

ла MGCP описаны в документе IETF RFC 3435 Media Gateway Control Protocol (MGCP) Version 1.0. January 2003 Status: INFORMATIONAL.

Так же, как и в протоколе MEGACO, подключение информационных потоков к канальному шлюзу MGCP выполняется через специальные элементы, которые называются в данном случае *оконечными точками* (MGCP END.POINT).

В состав канального шлюза могут входить физические и виртуальные оконечные точки. Для описания способа обработки и коммутации потоков, поступающих или передаваемых через информационные окончания, используется понятие *соединения канального шлюза* (MGCP CONNECTION).

Таким образом, сигнальный шлюз, для обозначения которого в описываемом протоколе используется также понятие *агент вызова* — (MGCP Call Agent), в процессе организации вызова обеспечивает управление соединениями различных оконечных точек на канальном шлюзе. Для обеспечения этого управления агент вызова MGCP использует примерно такой же набор управляющих команд, который применяется для аналогичных целей в протоколе MEGACO. В табл. 4.10 приведены основные команды, которые используются для обмена между сигнальным и канальным шлюзами в протоколе MGCP.

Таблица 4.10. *Основные команды, которые используются в протоколе MEGACO*

Команда	Назначение	Источник
ENDPOINT.CONFIGURATION	Указание ожидаемого способа кодирования принимаемых данных	CA*
NOTIFICATION.REQUEST	Указание об ожидании специального события	CA
NOTIFY	Наступление ожидаемого события	GW**
CREATE.CONNECTION	Создать соединение с использованием выбранных оконечных точек	CA
MODIFY.CONNECTION	Изменить параметры установленного соединения	CA
DELETE.CONNECTION	Удалить установленное соединение	CA
AUDIT.ENDPOINT	Контролировать состояние оконечной точки	CA
AUDIT.CONNECTION	Контролировать состояние соединения	CA
RESTART.IN.PROGRESS	Изменение состояния оконечной точки	GW

Примечание:

* CA — источником сообщения является MGCP Call Agent — сигнальный шлюз.

** GW — источником сообщения является MGCP Media Gateway — канальный шлюз.

Перспективные системы управления мультисервисным обменом

История создания и развития мультимедийных систем насчитывает более 10 лет, в течение которых параллельно развивались и технологии управления мультисервисным обменом. Мультимедийные системы первого поколения были основаны на технологиях коммутации каналов — PSTN, ISDN. Соответственно, разработанные ITU-T в период с 1988 по 1992 годы спецификации первого поколения систем управления мультисервисным обменом (H.320, H.321, H.322) учитывали особенности организации информационного обмена именно в этих сетях.

Второе поколение мультимедийных систем представляет собой гибридные комплексы, обеспечивающие возможность совместного использования систем коммутации каналов и систем коммутации пакетов (Интернет). Описанные в предыдущих разделах настоящей главы протоколы можно отнести ко второму поколению протоколов управления компонентами мультимедийных систем: с 1992 по 2005 годы. Характерными особенностями этого периода являются:

- неуклонное повышение роли сетей с коммутацией пакетов в реализации мультисервисного информационного обмена (Интернет, Ethernet);
- появление и интенсивное развитие новых форм и способов выполнения мультисервисного обмена.

Протоколы управления мультисервисным обменом второго поколения имеют много недостатков, вызванных гибридным характером систем, в которых они были реализованы. Перспективные разработки систем управления мультисервисным обменом призваны устранить существующие недостатки и обеспечить возможность дальнейшего развития мультисервисных информационных систем.

Недостатки систем управления второго поколения

Как уже было отмечено, подавляющее большинство недостатков, свойственных второму поколению систем управления мультисервисным обменом (H.323, SIP, MGCP/MEGACO), объясняется гибридным характером сетевых технологий, которые используются для их реализации. Развитие и внедрение этих технологий происходило в период первоначального становления мультисервисных систем, основанных на принципах коммутации пакетов. В этот период большое внимание уделялось проблемам совместимости с существующими системами, основанными на принципах коммутации каналов — в первую очередь с классическими телефонными системами. Технологиям,

которые описаны в предыдущих разделах данной главы, в разной степени свойственны следующие недостатки:

- ориентация на реализацию голосовых приложений;
- ограниченные возможности по обнаружению и устранению неисправностей;
- отсутствие необходимого разделения между информационными и управляющими каналами;
- сложность реализации в системах мобильной связи;
- отсутствие должного внимания к таким аспектам информационного обмена, как обеспечение заданного уровня качества обслуживания, информационная безопасность и защита прав собственности;
- ограничение возможности использования стандартных процедур сети Интернет для наращивания функций терминального оборудования.

Большинство из отмеченных недостатков являются довольно серьезными и, безусловно, оказывают сдерживающее влияние на процессы развития и внедрения систем мультисервисного обмена по сетям с коммутацией пакетов.

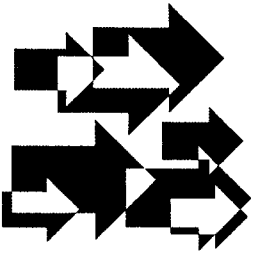
Направления дальнейшего развития

Развитие систем мультисервисного обмена происходит одновременно во многих направлениях. В процесс создания технологий управления мультисервисным обменом вовлечены такие организации, как ITU, IEEE и IETF. Многие крупные производители коммуникационного оборудования и неформальные организации активно предлагают новые и оригинальные подходы к решению этой проблемы.

Хотя отсутствие единой концепции приводит к появлению несовместимых технических решений и отодвигает сроки внедрения действительно перспективных систем мультисервисного обмена, уже определились общие принципы построения таких систем, к которым относятся следующие:

- использование разнообразных технологий коммутации пакетов для передачи всех видов трафика;
- обеспечение реализации всех информационных сервисов предшествующих технологий;
- эффективное совмещение функций распределенного и централизованного управления вызовом;
- обеспечение возможности гибкого наращивания функций и снижение стоимости терминального оборудования;
- значительное улучшение основных характеристик информационного обмена в мультисервисных сетях и, в первую очередь, его безопасности, надежности и доступности.

ГЛАВА 5



Особенности построения современных МСС

Коммерческий успех любого современного предприятия во многом определяется эффективностью функционирования его информационной подсистемы. Предоставление информационных услуг, оперативный обмен финансовой и технологической документацией, разнообразные формы связи с партнерами и клиентами — все это в большей или меньшей степени вошло в повседневную деятельность современного предприятия. Разнообразные информационные сервисы стали неотъемлемой частью технического процесса, развитие которого немыслимо без соответствующей модернизации информационной подсистемы.

Определение

Информационная подсистема предприятия — комплекс аппаратных и программных средств, которые обеспечивают реализацию информационных процессов предприятия.

Очевидно, что удачный выбор принципа построения и направления развития информационной подсистемы может существенно повлиять на долгосрочную перспективу деятельности практически любого современного предприятия. Именно этим объясняется повышенный интерес к технологиям построения универсальных мультисервисных систем, которые способны обеспечить предоставление или получение всего комплекса информационных услуг.

В технологиях построения мультисервисных систем сегодня завершается окончательный переход от принципов коммутации каналов (PSTN, ISDN) к системам пакетной коммутации (Ethernet, Интернет). В перспективных телефонных и телевизионных системах, в дополнение к снижению стоимости построения и эксплуатации, такой переход обеспечивает внедрение дополнительных приложений и услуг, таких, например, как центры обработки телефонных вызовов или интегральные системы "Видео по запросу".

Внедрение технологий пакетной коммутации в мультисервисные информационные подсистемы происходит поэтапно и в некоторых случаях может быть сопряжено со значительными проблемами. Эти проблемы могут быть вызваны как недостатками и недоработками постоянно развивающихся технологий пакетной коммутации, не всегда способных обеспечить требуемый уровень качества услуг, так и ошибками внедрения этих технологий. Данная глава посвящена рассмотрению основных принципов и аспектов построения современных мультисервисных систем и особенностей внедрения в эти системы технологий пакетной коммутации.

Первый раздел посвящен разбору общих вопросов построения и принципов организации информационного обмена мультисервисных систем. В этом разделе, в частности, рассматриваются варианты создания следующих типов мультисервисных информационных подсистем:

- информационных подсистем с раздельными каналами;
- информационных подсистем с интегральным каналом.

Во втором разделе анализируются основные принципы и особенности реализации мультисервисных информационных подсистем на основе комплекса технологий пакетной коммутации Ethernet — Интернет.

Общие принципы построения мультисервисных сетей

Безусловно, наиболее важной особенностью информационного обмена в мультисервисных сетях является потоковый характер этого обмена. Порции информации, создаваемые мультисервисными приложениями, как правило, должны следовать одна за другой в строгом порядке через фиксированные интервалы времени.

Другая особенность информационного обмена в мультисервисных сетях определяется неоднородностью передаваемого в них трафика, поскольку каждое из мультисервисных приложений ЛВС создает в этой сети трафик специфического типа. Зачастую при этом по коммерческим или технологическим соображениям следует обеспечить взаимную изоляцию различных типов трафика, передаваемых в единой сети.

Кроме того, повышенное внимание при построении мультисервисной сети должно быть уделено обеспечению надежности ее функционирования, что позволит избежать ситуации, когда отказ одного из ее элементов приведет к отказу в получении или предоставлении всех видов услуг.

Надежность и безопасность информационного обмена

Построение мультисервисной сети и объединение на ее основе всех информационных сервисов предприятия имеет, наряду со многими достоинствами, ряд существенных недостатков. Одним из таких недостатков является снижение надежности функционирования всей системы в целом вследствие возрастания степени воздействия единственного отказа на функции, выполняемые этой системой.

Другой недостаток мультисервисной сети вызван тем, что в ней, в процессе передачи по единым каналам, перемешивается трафик разнородных приложений, что может привести, с одной стороны, к возникновению их нежелательного взаимного влияния, а с другой — к снижению общего уровня безопасности информационной подсистемы предприятия.

В этом разделе рассматриваются основные способы преодоления отмеченных выше недостатков при построении мультисервисных информационных подсистем.

Устойчивость к отказам компонентов МСС

Мультисервисная сеть организации обычно используется для передачи информационного трафика нескольких видов приложений:

- трафика сетей передачи данных (доступ в сеть Интернет);
- трафика голосовых приложений (VoIP);
- трафика видеоприложений (видеоконференции, видеонаблюдение).

Важность каждого из типов приложений для обеспечения технологического процесса в конкретной организации определяется в первую очередь направлением деятельности данной организации. В том случае, если для передачи каждого из видов трафика в этой организации используются независимые системы и каналы, выход из строя любого из компонентов обеспечивающих систем приведет к потере только части из необходимых сервисов. Допустимость полной или частичной потери сервисов также определяется производственным профилем предприятия. Крупные организации, для которых даже кратковременная потеря любого из используемых сервисов является недопустимой, часто используют резервирование систем, обеспечивающих подключение к внешним сетям. На рис. 5.1 приведена схема организации информационной подсистемы предприятия, в которой для повышения надежности используется принцип полного канального резервирования.

Использование метода полного канального резервирования обеспечивает бесперебойное функционирование информационной подсистемы предприятия

при отказе или выходе из строя любого ее компонента. Однако информационные подсистемы, построенные по такому принципу, являются очень дорогими и недостаточно эффективными. Действительно, и без того немалые расходы на создание, содержание и эксплуатацию таких информационных подсистем увеличиваются в два раза. Обеспечить одновременное использование основного и резервного канального оборудования путем распределения нагрузки между ними оказывается во многих случаях невозможным. Так, например, достаточно трудно обеспечить динамическую маршрутизацию входящих телефонных вызовов PSTN. Это, в свою очередь, может привести к существенному увеличению времени простоя информационной подсистемы при переключении на резервный комплект канального оборудования.

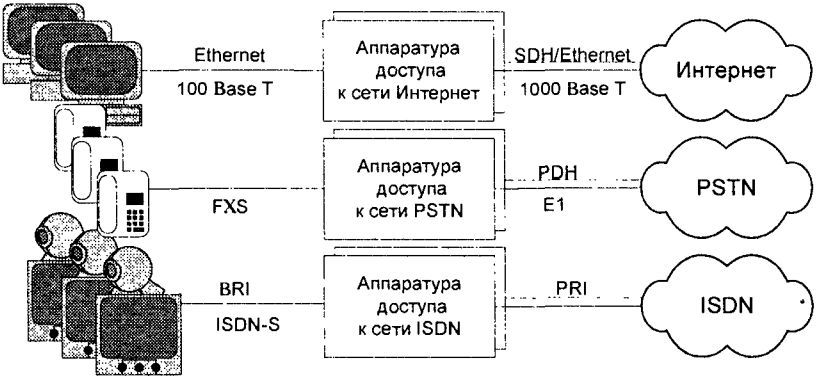


Рис. 5.1. Применение полного дублирования для повышения надежности информационной подсистемы

Существенно снизить затраты на построение резервированной информационной подсистемы можно благодаря применению многофункциональных устройств. Такие устройства обеспечивают возможность использования различных каналов для получения или предоставления соответствующей услуги. На рис. 5.2 приведена схема организации информационной подсистемы предприятия, в которой для повышения надежности используются многофункциональные канальные и терминальные устройства (на рисунке они отмечены утолщенным контуром). Многофункциональный терминал может содержать несколько интерфейсов, при помощи которых выполняется его подключение к канальному оборудованию различных типов сетей. Примером такого терминала является видеотерминал с интерфейсами ISDN-S и Ethernet, который может быть подключен в систему видеоконференц-связи через каналы любой из этих технологий. Многофункциональные терминалы, впрочем, имеют существенно более высокую стоимость, чем аналогичные по функциям стандартные устройства, что существенно ограничивает область их возможного применения.

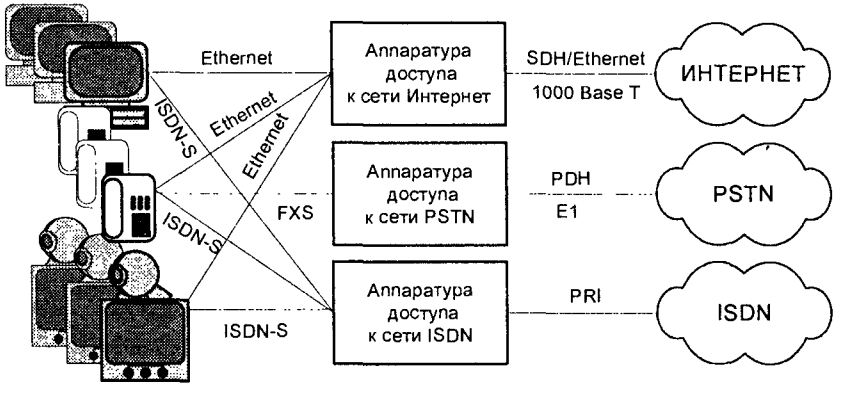


Рис. 5.2. Применение многофункциональных компонентов в информационной подсистеме

Существенно более перспективным в информационной подсистеме с раздельными каналами представляется применение многофункциональных канальных устройств. На таких устройствах обычно устанавливаются дополнительные интерфейсы, к которым могут быть впоследствии подключены терминалы, не являющиеся специфическими для этого типа устройств.

В качестве примера подобного многофункционального канального устройства можно рассмотреть маршрутизатор, который обычно используется для организации доступа в сеть Интернет по каналам Ethernet. На таком маршрутизаторе можно установить специальные платы расширения с абонентскими телефонными интерфейсами FXS или E1/PRI/ISDN, что позволит подключать к этому маршрутизатору обычные аналоговые телефонные аппараты или всю офисную АТС организации. Этот вариант организации информационной подсистемы, безусловно, более гибкий и перспективный, чем ранее рассмотренный, также не свободен от существенных недостатков. Главным недостатком многофункциональных канальных устройств является их высокая цена, состоящая из стоимости дополнительного оборудования и программного обеспечения, которая будет удваиваться в случае построения резервированной информационной подсистемы.

Таким образом, можно отметить, что общим недостатком мультисервисных информационных подсистем с раздельными каналами, помимо высокой стоимости построения, эксплуатации и обслуживания, является высокая стоимость их резервирования. Хотя применение многофункциональных канальных и терминальных устройств в разной степени позволяет решить часть проблем, возникающих при резервировании подобных систем, все такие решения имеют ряд существенных недостатков, которые не позволяют считать эти решения достаточно целесообразными и перспективными. Поэтому в тех случаях, когда надежное функционирование всех категорий информационных сервисов является одинаково важным для успеха производственной дея-

тельности предприятия, более экономичным и перспективным следует признать построение единой мультисервисной информационной подсистемы с интегральным каналом, по которому будет передаваться трафик всех используемых информационных служб.

Вопрос выбора технологии, на основе которой наилучшим образом осуществляется интеграция разнородных информационных потоков, имеет богатую историю (см. *главу 1*) и не может быть решен однозначно без учета специфики конкретной реализации. В то же время нельзя не отметить, что в последнее время все большую популярность приобретают более дешевые и доступные интегральные системы, основанные на технологиях Ethernet и Интернет. Сегодня даже не очень крупная организация может построить информационную подсистему подобного типа на основе собственной локальной вычислительной сети.

Основным препятствием на пути широкого распространения таких систем сегодня является относительно высокая стоимость терминального оборудования. Известно, например, что VoIP-телефон сегодня стоит во много раз больше, чем аналоговый телефонный аппарат. Частично решить эту проблему можно путем использования специализированных адаптеров, которые позволяют подключать к мультисервисной сети Ethernet терминальные устройства других систем. Так, например, относительно дешевые устройства типа "VoIP-шлюз" различных производителей способны обеспечить подключение от четырех и более обычных телефонных аппаратов к сети Ethernet. Специальные разновидности подобных устройств можно применять и для подключения офисной АТС через интерфейсы FXO или ISDN/PRI к сети IP-телефонии.

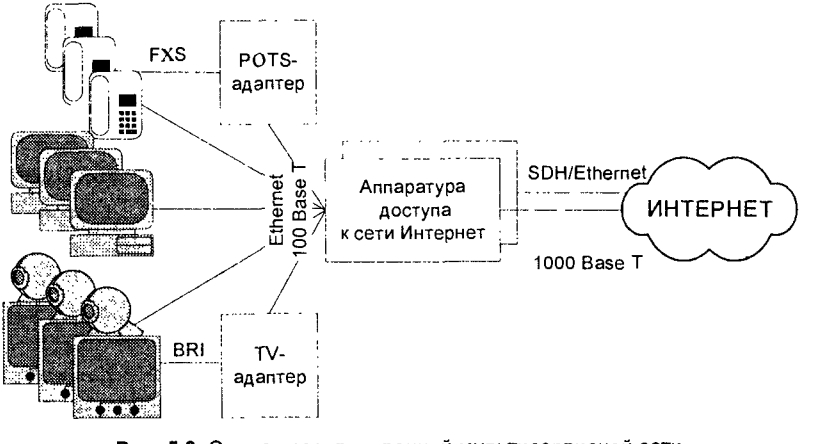


Рис. 5.3. Схема резервированной мультисервисной сети, основанной на технологиях Ethernet и Интернет

На рис. 5.3 приведена схема резервированной мультисервисной информационной подсистемы, основанной на технологиях Ethernet и Интернет.

Повышенный уровень надежности представленной системы реализуется путем дублирования аппаратуры, которая применяется для организации доступа в сеть Интернет. Для обеспечения возможности постепенного перехода к мультисервисной структуре с единым каналом в данной сети используются специализированные Ethernet-адаптеры.

Взаимная изоляция компонентов мультимедийного трафика

Одним из наиболее важных и неизбежных последствий создания мультисервисной информационной подсистемы предприятия с единым интегральным каналом является слияние в нем разнородного трафика. Такое слияние, как правило, приводит к возникновению ряда проблем, среди которых, в первую очередь, следует отметить устранение взаимного влияния и пропорциональное распределение пропускной способности каналов между компонентами разнородного трафика.

Наиболее простое и надежное решение второй из отмеченных выше проблем может быть достигнуто путем применения постоянного разделения пропускной способности каналов между компонентами разнородного трафика по принципу TDM (Time Division Multiplexing), которое практикуется, например, в сетях ISDN. При использовании такого способа разделения каждое из приложений получает в свое распоряжение фиксированную долю пропускной способности канала. Очевидно, что такое распределение никак нельзя назвать эффективным, поскольку все основные составляющие мультисервисного трафика — передача данных, телефония и видеопотоки имеют пульсирующий характер. В часы максимальной нагрузки, например, количество одновременных телефонных вызовов обычно превышает среднее значение в 3—4 раза, а в нерабочее время телефонных вызовов не будет вообще.

Эффективное динамическое распределение пропускной способности каналов между компонентами разнородного трафика может быть оформлено в виде политики качества обслуживания (QoS). Эта политика должна учитывать не только специфику передачи в едином канале каждого из компонентов трафика, но и степень важности этого компонента для производственной деятельности предприятия.

Передача в едином канале разнородного трафика

Понижение уровня информационной безопасности также относится к неизбежным последствиям передачи разнородного трафика в едином канале. Снижение вызвано тем, что общий уровень информационной безопасности

для единого потока, построенного из нескольких компонентов, очевидно, соответствует минимальному значению из уровней безопасности этих компонентов.

Среди основных способов обеспечения заданного уровня информационной безопасности при передаче разнородного трафика в едином канале можно выделить следующие:

- логическую изоляцию компонентов трафика;
- шифрование передаваемого трафика.

Логическая изоляция предполагает создание и использование специальных признаков — меток, которые ассоциируются с каждым из компонентов трафика, передаваемого в едином канале. Таким образом, анализируя значение метки, можно однозначно определить тип передаваемого трафика, что позволит реализовать на каждом из промежуточных узлов единую политику обеспечения информационной безопасности.

Шифрование передаваемых данных также является эффективным средством для достижения требуемого уровня информационной безопасности при передаче разнородного трафика в едином канале. Особенно актуальным использование шифрования становится в том случае, когда для трансляции трафика применяется сеть передачи данных общего пользования. Основным достоинством шифрования является избирательный характер его действия, что позволяет наиболее эффективно использовать этот инструмент при обработке различных компонентов разнородного трафика.

Совместное использование принципов логического разделения и шифрования трафика позволяет добиться повышения эффективности применения каждого из этих методов обеспечения информационной безопасности.

Требования современных приложений к параметрам МСС

Требования к характеристикам информационной подсистемы у всех реализуемых в ней приложений различные, а зачастую — противоречивые. Кроме того, в дополнение к общим требованиям, которые предъявляются приложениями к характеристикам мультисервисной сети передачи данных, для реализации каждого из таких приложений может потребоваться выполнение специфических требований и условий.

Нетрудно предположить, что недостаточно экономичной и неэффективной будет реализация информационной системы, которая способна реализовать максимально возможные требования мультисервисных приложений к значениям всех ее параметров.

Очевидно, что оптимальная конфигурация мультисервисной информационной подсистемы должна обеспечивать целенаправленную и эффективную реализацию требований, наиболее существенных для реализуемых в ней приложений.

Реализация видеоприложений в мультисервисной ЛВС

Специфическими требованиями современных видеоприложений к параметрам и характеристикам информационной подсистемы в первую очередь следует считать:

- обеспечение высокой пропускной способности;
- обеспечение режима группового вещания;
- синхронизация со звуковым потоком;
- обеспечение канала оперативного управления.

Обобщенные характеристики наиболее популярных видеоприложений приведены в табл. 5.1.

Таблица 5.1. *Обобщенные характеристики видеоприложений*

Характеристика	Телевизионное вещание	Видео-конференции	Видеонаблюдение
Пропускная способность (Мбит/сек)	6—1000	0,5—1,0	0,2—0,8
Потоковое вещание	Обязательно	Обязательно	Обязательно
Групповое вещание	Обязательно	Желательно	Желательно
Синхронный звук	Обязательно	Обязательно	Желательно
Канал управления	Обязательно	Неприменимо	Неприменимо

В зависимости от использованных методов кодирования видеопотока и характеристик передаваемого изображения (см. *главу 3*), значение пропускной способности, которое необходимо для реализации видеоприложения, может изменяться в пределах от десятков килобит до сотен мегабит в секунду. Следует отметить, что наиболее высокие требования к пропускной способности предъявляются в системах трансляции телевизионных и видеопрограмм.

Общей для всех типов современных видеоприложений является необходимость передачи данных в потоковом формате. Реализация этого требования предполагает выполнение следующих дополнительных условий:

- обеспечения установленного порядка следования блоков данных, передаваемых в потоке;

- обеспечения требуемых значений задержки передаваемых в потоке блоков данных и допустимых диапазонов ее изменения.

Следует отметить, что применение алгоритмов MPEG-2 для сжатия и кодирования изображений существенно уменьшает требования видеоприложений не только к пропускной способности используемого канала передачи данных, но и к стабильности значений остальных параметров этого канала. Так, например, при использовании последовательности чередования кадров (GOP) 15/3, полный кадр потеря или искажение которого существенно сказывается на качестве изображения, передается обычно только в каждом пятнадцатом из последовательных циклов чередования кадров. Следовательно, в зависимости от частоты формирования кадров, значение задержки сигнала, влияющей на качество видеоизображения, будет находиться в диапазоне от 0,1 до 2,0 сек.

Достаточно характерным для видеоприложений является требование организации режима широковещательного или группового обмена, при использовании которого несколько приемников принимают один и тот же сигнал, сформированный передатчиком для данной группы.

Примечание

Разумеется, проще всего реализовать это требование на физическом уровне модели OSI ISO 7498 (см. *главу 6*), как это сделано, например, в сетях кабельного телевидения. Такое решение, впрочем, может привести к существенному ограничению зоны распространения видеосигнала.

Требование синхронизации с транслируемым потоком в той или в другой степени свойственно всем видеоприложениям, в то время как требование наличия обратного канала, с помощью которого выполняется управление выбором программ, присутствует только в системах коммерческого телевизионного вещания. Таким образом, наиболее жесткие требования к параметрам информационной подсистемы предъявляются в системах коммерческого телевидения.

Требования голосовых приложений к параметрам МСС

Наиболее популярным, и одновременно, наиболее требовательным к параметрам информационной подсистемы голосовым приложением является цифровая телефония. Другие популярные разновидности голосовых приложений, например, такие, как трансляция информационных и развлекательных звуковых программ, реализуются, как правило, теми же средствами и приложениями, что и трансляция видеопрограмм.

Аналоговая телефонная связь, безусловно, является наиболее доступной, зрелой и демократичной информационной услугой. За многие годы существова-

ния этой услуги многочисленные пользователи успели по достоинству оценить и привыкнуть к следующим положительным качествам телефонной связи:

- постоянной доступности;
- высокому качеству передачи человеческой речи (при использовании цифровых магистральных каналов);
- возможности передачи графической информации (факсимильные сообщения) и использованию дополнительных сервисов (определитель номера, телефонные конференции).

Поэтому, когда неизбежный сегодня процесс постепенного перехода к пакетной телефонии иногда сопровождается заметным ухудшением качества телефонной связи, это может дать основания для резкой критики или полного отказа от данной технологии. Однако более низкое качество пакетной телефонии по сравнению с аналоговой телефонией — эхо, пропадание и искажение звука, как правило, объясняется ошибками проектирования интегрированных информационных подсистем. Именно поэтому при проектировании мультисервисных систем в первую очередь следует обращать внимания на реализацию требований, специфических для систем пакетной телефонии, наиболее существенными среди которых являются:

- обеспечение требуемых значений пропускной способности для передачи телефонного сигнала;
- обеспечение стабильного значения величины задержки формирования и распространения телефонного сигнала;
- наличие и, при необходимости, применение систем подавления эхосигнала;
- обеспечение дополнительных сервисов телефонных сетей общего пользования.

Для организации одного телефонного разговора, в зависимости от характеристик используемых кодеков (см. *главу 2*), требуется от 8 до 80 Кбит/сек полосы пропускания интегрального информационного канала. Следует особо отметить, что выделение полосы пропускания для систем пакетной телефонии должно быть гарантированным, недопустимым является применение для этой цели остаточного принципа. Действительно, на фоне возможностей современных интерфейсов и каналов передачи данных требования систем пакетной телефонии кажутся достаточно скромными. Не следует, однако, забывать, что пренебрежение этими требованиями при формировании интегрального информационного потока неминуемо отразится на качестве телефонного сигнала. Дело в том, что любой канал, какой бы высокой ни была его пропускная способность, может быть введен в состояние перегрузки приложениями передачи данных или видеопотоков. Именно отсутствие гарантированной

полосы пропускания для передачи телефонного трафика в таких ситуациях приводит к пропаданиям голосового сигнала, заиканиям и искажению речи.

Наличие эхо в принимаемом сигнале является еще одним популярным недостатком систем пакетной телефонии. Наличие эхо, как правило, бывает обусловлено не столько неизбежными задержками в системах формирования и распространения голосового сигнала, сколько неправильным функционированием встроенных систем компенсации эхо-сигнала. Известно, что заметное влияние на качество телефонного разговора эхо-сигнал начинает оказывать при значении совокупной задержки, превышающем 50 мсек.

Примечание

Более половины значения совокупной задержки (20—38 мсек) составляет, как правило, неизбежная алгоритмическая задержка, вызванная преобразованием голосового сигнала в последовательность информационных пакетов.

Следовательно, если время распространения голосового сигнала не превышает 50 мсек, отсутствие или неправильное функционирование схемы эхокомпенсации не будет оказывать влияния на качество телефонной связи. В этом случае, однако, нормальная телефонная связь может периодически частично или полностью нарушаться при увеличении времени распространения телефонного сигнала, например, вследствие изменений маршрута передачи пакетов через сеть общего пользования.

Таким образом, для обеспечения нормального качества связи в системах пакетной телефонии необходимо обеспечить требуемые значения параметров информационного обмена:

- гарантированное значение полосы пропускания — от 8 до 80 Кбит/сек;
- стабильное значение величины задержки формирования и распространения телефонного сигнала — не более 120 мсек;
- наличие и правильное функционирование систем подавления эхо-сигнала;
- поддержка дополнительных сервисов телефонных сетей общего пользования.

Особенности построения мультисервисных ЛВС

Как уже было неоднократно отмечено, сегодня для построения мультисервисных информационных подсистем с интегральным каналом наиболее привлекательным представляется использование комплекса технологий Ethernet и Интернет, обеспечивающих передачу данных в современных ЛВС. Благодаря постоянному развитию технологий современные ЛВС, как правило, об-

ладают значительным резервом пропускной способности, который с успехом может быть использован для реализации мультисервисных приложений. Для того чтобы правильно использовать этот резерв, при построении или модернизации ЛВС должны быть учтены специфические требования, которые предъявляются мультисервисными приложениями к основным характеристикам этих сетей.

Следует отметить, что применение технологий сети Интернет и Ethernet для построения мультисервисных сетей является далеко не бесспорным и отнюдь не безальтернативным. Ранее уже говорилось о том, что при создании этих популярных технологий в очень малой степени учитывалась возможность их использования для передачи специфических форм трафика мультисервисных сетей. Однако присущая технологиям сети Интернет и Ethernet возможность масштабирования, а также постоянно растущий объем инвестиций в соответствующие области телекоммуникационной индустрии, обеспечивают возможность постоянной модернизации этих технологий и внедрения новых технических решений, расширяющих область их применения.

Реализация потокового обмена в пакетных МСС

При построении комплексной информационной подсистемы, которая предназначена для одновременной передачи информационных потоков нескольких приложений, неизбежно возникает задача согласования режимов и способов распространения этих потоков.

Несмотря на то, что потоковый режим информационного обмена, разумеется, не является характерным для сетей Интернет или Ethernet, он вполне может быть реализован в ЛВС, построенных на основе этих технологий, благодаря использованию соответствующих технических решений.

Передача потоков данных в сетях с коммутацией пакетов

В приложениях реального времени отправитель генерирует поток данных с постоянной скоростью и предполагается, что приложение на стороне получателя должно принимать эти данные с той же самой скоростью. Такие приложения включают, например, аудио- и видеоконференции, живое видео, удаленную диагностику в медицине, компьютерную телефонию, распределенное интерактивное моделирование, игры, мониторинг в реальном времени и др.

В настоящее время протокол *TCP* (Transmission Control Protocol) является наиболее широко используемым протоколом транспортного уровня. Этот протокол, безусловно, является достаточно универсальным и позволяет поддерживать множество разнообразных распределенных приложений, но, к сожалению, совершенно не подходит для обеспечения транспорта потокового трафика приложений реального времени.

Использование TCP в качестве транспортного протокола для этих приложений невозможно по следующим причинам:

- протокол TCP предполагает организацию соединения между двумя конечными точками, следовательно, не может быть использован для многоадресной передачи, когда количество передатчиков и приемников заранее неизвестно;
- повторная передача протоколом TCP потерянных сегментов неминуемо будет приводить к дополнительным нарушениям информационного обмена, поскольку эти сегменты будут прибывать в тот момент, когда принимающее потоковое приложение уже их не ждет;
- протокол TCP не обладает механизмом привязки информации о синхронизации к сегментам, который является обязательным для потоковых приложений.

Другой протокол транспортного уровня сети Интернет — *UDP* (User Datagram Protocol) не имеет некоторых из перечисленных ограничений протокола TCP, однако этот протокол также не обладает возможностью предоставления информации о временной синхронизации передаваемых данных.

Несмотря на то, что различные потоковые приложения могут иметь свои собственные механизмы для поддержки передачи в реальном масштабе времени, все они имеют достаточно много общих черт, что делает использование единого универсального протокола весьма желательным.

Потоковое приложение, как правило, формирует свои выходные блоки данных — пакеты с постоянной периодичностью. Однако ввиду изменения времени задержки при передаче пакетов по сети эти пакеты могут прибывать к получателю через нерегулярные интервалы времени. Поэтому для восстановления исходного вида сигнала реального времени необходимо, чтобы каждый пакет, передаваемый по сети, содержал метку времени. При наличии такой метки получатель сможет определить взаимное расположение во времени получаемых порций и воспроизвести поступающие данные в том же временном масштабе, в котором они были сформированы отправителем.

Эту задачу и призван решить специальный *транспортный протокол реального времени — RTP* (Real-Time Transport Protocol), который способен передавать данные с привязкой к моменту времени их формирования.

Принципы построения протокола RTP

Ранее было отмечено, что основная особенность потокового голосового и видеотрафика состоит в наличии жесткой привязки каждого передаваемого фрагмента данных к определенному моменту времени. Именно поэтому для обозначения подобных разновидностей трафика иногда используют обоб-

щенный термин — *трафик реального времени*. В том случае, если для выполнения оцифровки входящего аналогового потока используются стандартные прямые методы, порции данных формируются и должны передаваться с постоянным интервалом времени.

Для повышения эффективности использования канала передачи данных при выполнении преобразования аналогового потока могут быть также использованы модифицированные алгоритмы сжатия. При использовании таких алгоритмов сжатия порции данных формируются с переменным интервалом времени. В те моменты времени, когда источник аналогового трафика проявляет активность, эти интервалы уменьшаются, при понижении активности источника они увеличиваются. Однако, как в одном, так и в другом случае, для того, чтобы выполнить адекватное восстановление исходного вида аналогового сигнала на приемной стороне, приемник должен получать информацию о взаимном временном расположении полученных порций входных данных.

Строго говоря, протокол RTP не является отдельным транспортным протоколом, а представляет собой лишь универсальную надстройку для стандартного протокола транспортного уровня (в рассматриваемом варианте — для протокола UDP).

Примечание

Следует особо отметить, что протокол RTP не поддерживает каких-либо механизмов гарантированной доставки блоков данных, обеспечения достоверности их передачи или контроля надежности соединения. При необходимости все эти функции могут быть возложены на протокол транспортного уровня.

Функции, выполняемые протоколом RTP, разделены между двумя функционально-обособленными протоколами:

- собственно транспортным протоколом реального времени — *RTP* (Real-Time Transport Protocol);
- управляющим протоколом RTP — *RTCP* (RTP Control Protocol).

Назначение протокола RTP состоит в непосредственной передаче блоков данных трафика реального времени, снабженных метками времени.

Управляющий протокол RTCP обеспечивает оперативный обмен управляющей информацией между узлами, выполняющими прием и передачу потоковых данных в соответствии с правилами протокола RTP.

Поскольку подавляющее большинство сетевых приложений, формирующих трафик реального времени, предназначено для использования в режиме многоадресной передачи (MULTICAST), комплекс протоколов RTP также имеет ряд механизмов и функций, учитывающих особенности информационного обмена в этом режиме.

В частности, *сеансом RTP* (RTP Session) принято называть отношения между группой участников информационного обмена с использованием протокола RTP. Для каждого из участников такой сеанс определяется совокупностью трех значений:

- IP-адресом узла назначения;
- номером порта протокола транспортного уровня, используемого для передачи сообщений протокола RTP;
- номером порта протокола транспортного уровня, используемого для передачи сообщений протокола RTCP.

В том случае, если для информационного обмена в сеансе используется групповая адресация, то число участников может быть переменным. При проведении мультимедийных конференций (например: "голос + видео") для каждого из компонентов мультимедийного потока должен быть использован отдельный сеанс.

Если для организации сеанса используется обычный режим UNICAST, в нем могут принимать участие только два абонента, каждый из которых в качестве IP-адреса узла назначения будет использовать адрес своего партнера.

Любой из узлов сети может одновременно принимать участие в нескольких групповых и одноадресных сессиях. Для разделения информационных потоков в подобной ситуации используются различные адреса назначения.

Протокол RTP обеспечивает выполнение двух основных функций преобразования и объединения трафика:

- преобразование (Translation);
- объединение или смешивание (Mixing).

Применение преобразования целесообразно в тех случаях, когда, например, некоторые участники многоточечной сессии подключены к сети низкоскоростными каналами, что не позволяет передатчику применять кодирующие схемы, обеспечивающие высокое качество воспроизведения голосового сигнала всем участникам сессии. Подобная проблема может быть решена двумя путями:

- использованием одинаковых низкоскоростных кодеков всеми участниками сессии;
- преобразованием (трансляцией) формы представления аналоговых сигналов на промежуточных узлах — маршрутизаторах.

Совершенно очевидно, что второй метод является более предпочтительным, поскольку позволяет обеспечить максимальное качество передачи голосового сигнала в условиях ограниченной пропускной способности используемого канала передачи данных.

Транслятор создает один исходящий пакет RTP для каждого поступающего пакета RTP. Транслятор может изменить формат данных в пакете или использовать иной комплект низкоуровневых протоколов для передачи данных из одного домена в другой. Трансляция адресов, например, обязательно должна присутствовать в том случае, когда область распространения группового трафика сессии административно ограничивается некоторой зоной, за пределами которой оказывается часть участников этой сессии. В тех случаях, когда вследствие особенностей топологии сети информационный обмен с некоторыми из участников сессии должен быть выполнен с использованием особого режима адресации, также может возникнуть необходимость в применении функции трансляции.

Функция смешивания позволяет объединить несколько однонаправленных информационных потоков в один и при необходимости выполнять преобразование порций информации, сформированных с использованием различных кодирующих схем. При объединении порций, принадлежащих разным потокам одной сессии, обеспечиваются дополнительные возможности повышения качества воспроизведения передаваемого потокового сигнала и экономия сетевых ресурсов.

Очень важным для протокола RTP является понятие *источника синхронизации* (Synchronization Source).

Определение

Источником синхронизации называется участник сессии, который формирует временные метки и прикрепляет их к порциям оцифрованного потокового трафика.

В качестве источников синхронизации могут выступать как первичные источники трафика (например, видео- или аудиокодеки), так и вторичные источники (например, микшеры). Уже было отмечено, что микшеры выполняют функцию объединения нескольких потоков, принадлежащих к одной сессии, в единый поток. При выполнении этого преобразования сам микшер становится источником синхронизации, поскольку он прикрепляет к сгруппированным порциям трафика, поступающего от источников заполнения (Contributing Source), свои временные метки.

Для обеспечения однозначной идентификации каждого из участников сессии применяются сформированные случайным образом 32-разрядные числа. Следует отметить, что уникальность идентификатора должна быть обеспечена только в пределах данной сессии. Один узел может иметь разные идентификаторы для каждой из сессий, в которых он принимает участие.

Заголовок сообщения протокола RTP содержит следующие поля: идентификатор отправителя, указывающий источник принимаемых данных, отметку

о времени генерирования пакета, информацию о порядке передачи, а также указание о характере содержимого пакета, например, о типе кодировки видеоданных.

Назначение протокола RTCP

Протокол RTP, описание которого приведено в предыдущем разделе, используется только для передачи пользовательских данных — обычно с использованием многоадресного режима — между участниками сеанса. Все функции управления передачей данных, выполняемой протоколом RTP, осуществляются специальным управляющим протоколом реального времени — *RTCP* (Real-Time Transport Control Protocol). Основной задачей протокола RTCP, таким образом, является организация и обслуживание сессий протокола RTP.

Для передачи управляющих сообщений протокола RTCP применяется обычно тот же самый базовый транспортный протокол, что и для протокола RTP (обычно UDP), однако при этом для протокола RTCP используется номер порта, отличный от того, который используется для протокола RTP.

Среди основных функций, выполняемых протоколом RTCP, в первую очередь следует выделить:

- обеспечение обратной связи между передатчиками и приемниками группового трафика;
- идентификацию источника передаваемых данных;
- определение оптимального периода формирования сообщений RTCP.

Обеспечение обратной связи между передатчиками и приемниками группового трафика выполняется для оперативного определения качества передаваемого сигнала. Поскольку диагностические сообщения протокола RTCP передаются приемниками потокового трафика в режиме групповой адресации, то все заинтересованные участники сеанса могут оценить качество передаваемого сигнала и степень загруженности сети. Диагностические сообщения протокола RTCP содержат информацию о проблемах, которые возникли при приеме потокового трафика, например, потеря пакетов или большая неравномерность передачи.

Обратная связь с получателями важна также для диагностирования ошибок при распространении потокового трафика по сети. Например, анализируя сообщения всех участников сеанса, администратор сети может определить, является ли возникшая проблема локальной проблемой одного участника или носит глобальный характер. Если приложение-отправитель или администратор сети приходит к выводу, что проблема характерна для системы в целом, допустим, по причине перегруженности одного из используемых каналов

связи, то они могут, например, сформировать предложения по изменению, или изменить степень сжатия данных, передаваемых по этому каналу.

Для обеспечения идентификации источника передаваемых данных сообщения протокола RTCP содержат стандартное текстовое описание отправителя. Использование сообщений протокола RTCP, таким образом, обеспечивает однозначную идентификацию пользователя, участвующего в нескольких различных сеансах одновременно.

Определение оптимального периода формирования сообщений RTCP выполняется на основе полученной оценки числа участников сеанса. Очевидно, что число передаваемых сообщений протокола RTCP будет расти с увеличением числа участников сессии. При небольшом количестве участников один пакет RTCP посылается максимум каждые 5 сек. Цель определения оптимального периода формирования сообщений RTCP состоит в том, чтобы трафик сообщений протокола RTCP не превышал установленной доли от общего трафика сеанса.

Вспомогательной функцией протокола RTCP является передача управляющей информации сессии для отображения ее на пользовательском интерфейсе. Предполагается, что формирование и передача подобной информации будут целесообразными для обслуживания сессий, имеющих упрощенные процедуры членства. Поскольку для участия в такой сессии, как правило, не требуется выполнения процедур опознавания пользователя, полезным может оказаться наличие специального канала для передачи дополнительной информации об ее участниках.

Формат сообщений протокола RTP

Как уже было ранее отмечено, протокол RTP предназначен для передачи потоковых данных в реальном масштабе времени. Сообщения протокола RTP состоят из заголовка, в котором размещается управляющая информация, и поля нагрузки, в которое помещаются блоки передаваемых данных. Заголовки сообщений протокола RTP содержат информацию о порядке следования порций и временном положении передаваемых порций оцифрованных потоковых данных, с тем, чтобы обеспечить адекватное восстановление переданного сигнала на приемной стороне.

Каждое сообщение протокола RTP снабжается основным (фиксированным) заголовком, к которому, при необходимости, могут быть добавлены дополнительные поля, специфичные для конкретного приложения.

В табл. 5.2 представлена структура фиксированного заголовка сообщения протокола RTP.

Поле V предназначено для размещения номера версии протокола RTP. Номер текущей версии протокола — 2.

Таблица 5.2. *Структура фиксированного заголовка сообщения протокола RTP*

Номер поля	Содержание поля	Номер байта/ полубайта	Длина поля в битах
1	V — номер версии протокола RTP	0/0	2
2	P — признак заполнения	0/0	1
3	X — признак расширения заголовка	0/0	1
4	CC — количество использованных источников заполнения (CSRC)	0/1	4
5	M — признак маркера	1	1
6	PT — признак типа полезной нагрузки	1	7
7	SEQUENCE NUMBER — порядковый номер сообщения	2, 3	16
8	TIMESTAMP — метка времени	4—7	32
9	SSRC IDENTIFIER — идентификатор источника синхронизации	8—11	32
10	CSRC IDENTIFIER — идентификатор источника заполнения	>12	32

В поле P размещается признак наличия заполнения в фиксированном заголовке сообщения протокола RTP. Этот признак сигнализирует о наличии заполняющих байтов в конце полезной нагрузки. Заполнение применяется в тех случаях, когда по требованию принимающего приложения размер полезной нагрузки устанавливается кратным целому числу байтов. В том случае, если в фиксированном заголовке сообщения протокола RTP бит P установлен в 1, то последний байт этого сообщения содержит число заполняющих байтов.

Поле X предназначено для размещения признака расширения заголовка. Если в сообщении протокола RTP бит X установлен в 1, то за основным заголовком следует еще один дополнительный, используемый в экспериментальных расширениях протокола RTP.

Поле CC применяется для указания количества использованных источников заполнения. В этом поле содержится количество источников потоковых данных, передаваемых в настоящем сообщении протокола RTP.

В поле M размещается признак маркера. Назначение этого признака определяется типом полезной нагрузки. Бит маркера обычно используется для указания границ потока данных. В случае видеоизображения он задает конец кадра. При использовании в голосовых приложениях этот признак задает начало речи после периода молчания.

Поле PT идентифицирует тип полезной нагрузки и формат данных. В этом поле, в частности, размещаются наименования кодеков, использованных для сжатия и шифрования полезной нагрузки. Как правило, отправитель использует только один тип полезной нагрузки в течение сеанса. Соответствие структуры поля полезной нагрузки и значения поля PT определяется профилем приложения.

Поле SEQUENCE NUMBER используется для размещения текущего значения счетчика порядкового номера сообщения, значение которого увеличивается на единицу при передаче очередного сообщения RTP. Наличие порядкового номера позволяет обнаружить потерю сообщений или определить порядок следования нескольких сообщений, имеющих одинаковую метку времени.

Примечание

Несколько последовательных сообщений могут иметь одну и ту же отметку о времени, если логически они порождены в один и тот же момент, как, например, сообщения, переносящие порции информации, принадлежащие одному и тому же видеокадру. Для обеспечения противодействия возможным атакам на приемники каждый источник начинает нумеровать пакеты с произвольного случайно выбранного номера.

Поле TIMESTAMP предназначено для размещения метки времени. Это поле содержит линейно и монотонно возрастающее значение, соответствующее моменту времени, в который был создан первый байт данных полезной нагрузки. Точность, с которой формируется это значение, должна быть достаточной для обеспечения временной синхронизации для всех типов полезной нагрузки. Значение поля TIMESTAMP определяется по локальным часам отправителя, причем стартовое значение этих локальных часов для каждой сессии одного и того же устройства определяется случайным образом.

В поле идентификатора источника синхронизации SYNCHRONIZATION SOURCE (SSRC) IDENTIFIER помещается случайное число, предназначенное для однозначной идентификации этого источника. Уникальность этого идентификатора в пределах сессии обеспечивает возможность выявления и устранения петель, возникающих при передаче потокового трафика в сети. Смеситель, используемый в качестве источника синхронизации, может объединять в одно сообщение протокола RTP порции данных, полученных от нескольких источников, и, при необходимости, изменять формат представления данных. Предположим, что новая система хочет принять участие в сеансе аудиоконференции, но ее канал до сети не имеет достаточной пропускной способности. В этом случае смеситель, который получает информационные потоки данного сеанса, объединяет их в один, который и передает новому члену сеанса, используя при этом более экономичный способ кодирования.

Заголовок сообщения протокола RTP, генерируемого смесителем, включает идентификаторы всех передатчиков, чьи данные присутствуют в этом сообщении.

В поле CONTRIBUTING SOURCE IDENTIFIER (CSRC) (источник входящих данных), занимающем 32 бита в заголовке сообщения протокола RTP, помещается идентификатор источника данных, представленных в данном сообщении. Количество таких полей в сообщении протокола RTP может быть от 0 до 15.

Типы сообщений протокола RTCP

Сообщения протокола RTCP предназначены для управления компонентами, выполняющими формирование и передачу группового трафика с использованием протокола RTP. Для решения этой задачи используются следующие типы сообщений протокола RTCP:

- отчет источника — SR (Sender Report);
- отчет приемника — RR (Receiver Report);
- описание источника — SDES (Source Description);
- завершение сессии — BYE;
- специфическая функция — APP.

Сообщения SR формируются активными участниками сессии для передачи диагностической информации о передаваемых и принимаемых порциях потоковых данных. Поле PT таких сообщений содержит признак сообщения SR — константу "200".

Сообщения RR формируются пассивными участниками сессии для передачи диагностической информации о принимаемых порциях потоковых данных. В поле PT таких сообщений помещается признак сообщения RR — константа "201".

Сообщения SDES содержат описания источников потоковых данных. Поле PT содержит признак сообщения SDES — константу "202".

Сообщение BYE формируется одним участником сессии для информирования остальных участников о том, что данный узел перестал участвовать в сессии. Поле PT таких сообщений содержит признак сообщения SR — константу "203".

Сообщение APP предназначено для выполнения специфических функций конкретных приложений. Поле PT таких сообщений содержит признак сообщения SR — константу "204".

Каждое сообщение протокола RTCP представляет собой информационный блок, имеющий стандартный заголовок, похожий на заголовок сообщения

протокола RTP. Особенность протокола RTCP заключается в том, что несколько различных типов сообщений этого протокола могут объединяться в одно композиционное сообщение, передаваемое единым блоком без использования каких-либо внутренних разделителей. При формировании композитного сообщения протокола RTCP должны быть соблюдены некоторые специальные правила. Сообщение BYE, например, может появиться только в завершающей части композитного сообщения, а сообщение SDES, содержащее каноническое имя источника потокового трафика, должно включаться в композитное сообщение настолько часто, чтобы обеспечить достаточно быструю взаимную синхронизацию мультимедийных потоков.

В табл. 5.3 приведен перечень параметров, используемых для описания источников в сообщении SD.

Таблица 5.3. *Параметры описания источника сообщения SD*

Признак	Обозначение	Назначение
1	CNAME	Канонический идентификатор источника
2	NAME	Имя пользователя
3	EMAIL	Электронная почта
4	PHONE	Телефонный номер
5	LOC	Географическое размещение
6	TOOL	Тип используемого приложения
7	NOTE	Текущее состояние источника
8	PRIV	Расширение описания

Режим многоадресного обмена

Для распространения каждого из компонентов объединенного трафика по мультисервисной сети должны быть использованы режимы информационного обмена, свойственные этому компоненту.

Так, например, приложения, применяемые для передачи данных в пакетных сетях Ethernet/Интернет, изначально использовали два режима информационного обмена: одноадресный — индивидуальный и безадресный — широковещательный. В то же время голосовые и разнообразные видеоприложения были ориентированы на применение исключительно широковещательного обмена.

За последнее время в сфере информационного и развлекательного вещания наметилась отчетливая тенденция постепенного перехода от безадресных широковещательных режимов к режимам группового, многоадресного веща-

ния, когда передатчик отправляет свои сообщения ограниченной группе приемников. Это изменение характера вещания, в свою очередь, вызвано появлением и развитием новых форм предоставления и неуклонно растущими объемами потребления информационных сервисов.

В современных приложениях передачи данных также возрастает роль многоадресного информационного обмена, который начинает использоваться вместо широковещательного обмена везде, где это возможно. Такая замена позволяет обеспечить существенное повышение эффективности использования ресурсов ЛВС за счет уменьшения зоны распространения невостребованного трафика.

Таким образом, нетрудно предположить, что доля многоадресного (группового) трафика в интегральном потоке будет постоянно увеличиваться, а это означает, что оборудование мультисервисных ЛВС должно обеспечивать эффективное распространение этого трафика.

Базовые технологии ЛВС — Интернет и Ethernet изначально обеспечивали поддержку режима многоадресного (Multicast) информационного обмена. Повышение роли режима многоадресного информационного обмена привело к разработке и внедрению новых технологий, которые еще более повышают эффективность выполнения этого вида информационного обмена в мультисервисных ЛВС.

Реализация специальных требований потоковых приложений

При реализации потоковых приложений в сетях с пакетной коммутацией особое внимание должно уделяться выбору способа и формы доставки блоков передаваемых данных. Изначально эти сети не были предназначены для передачи потокового трафика и разнообразные дополнительные протоколы призваны повысить эффективность реализации специальных требований потоковых приложений в этих сетях.

Протокол STCP управления передачей потоков

Основным назначением протокола управления передачей потоков — *STCP* (Stream Control Transmission Protocol — IETF RFC 2960 — October 2000 — Status — STANDARDS TRACK) является передача сигнальных сообщений, формируемых в сетях пакетной телефонии, по сетям Интернет.

Протокол STCP представляет собой протокол транспортного уровня сети Интернет, который сочетает в себе потоковую ориентацию протокола UDP с возможностями надежной и упорядоченной доставки блоков данных, свойственной протоколу TCP. В дополнение к этому протокол STCP обеспечивает

возможность использования альтернативных путей в сети общего пользования — Интернет. Характерными особенностями протокола STCP являются:

- наличие и использование механизма квитирования для обеспечения гарантированной доставки;
- возможность выбора наиболее надежного маршрута доставки данных;
- управление информационными потоками и предотвращение возникновения перегрузок в процессе передачи данных.

Транспортное соединение между двумя сетевыми узлами по протоколу STCP принято называть *ассоциацией* (STCP Association). В процессе передачи данных каждая ассоциация проходит три последовательных стадии — построение, обслуживание передачи данных и отключение. Для передачи управляющей информации и собственно данных в протоколе STCP используются независимые виртуальные потоки (STCP Streams). Управляющие или информационные данные в пределах каждого потока передаются независимыми порциями (STCP Chunks), которые объединяются в единый транспортный блок протокола STCP — *пакет* (STCP Packet).

Надежная и гарантированная доставка компонентов информационных потоков обеспечивается при помощи передачи через управляющие виртуальные каналы специальных управляющих сообщений для управления порядком получения блоков данных. Этот же механизм в сочетании со специальным кодом аутентификации используется для предотвращения воздействия DoS-атак на сетевые компоненты.

Возможность выбора наиболее надежного маршрута доставки данных обеспечивается благодаря тому, что на стадии создания ассоциации каждый из ее компонентов получает от удаленного абонента полный перечень его IP-адресов. Это позволяет каждому из компонентов ассоциации создавать и контролировать состояние одновременно нескольких альтернативных маршрутов передачи данных удаленному абоненту. В том случае, если уровень ошибок при передаче данных по основному маршруту превысит допустимые значения, то может быть выполнено автоматическое переключение на резервный маршрут.

Управление информационными потоками и предотвращение возникновения перегрузок в процессе передачи данных в протоколе STCP обеспечивается благодаря применению механизма скользящего окна. Для этого компоненты ассоциации обмениваются значениями переменных *"окно приемника"* — RWND (Receiver Window) и *"окно перегрузки"* — CWND (Congestion Window).

Таким образом, протокол STCP обеспечивает управляемый и надежный потоковый обмен информационными блоками на транспортном уровне сети

Интернет. Основным недостатком протокола STCP следует считать относительно большой размер заголовка (20 байт плюс 20 байт на каждый из виртуальных потоков), что приводит к снижению эффективности передачи данных с его использованием.

Передача факсимильных сообщений по сети IP

Необходимость использования специального протокола для передачи факсимильных сообщений по сети IP объясняется тем фактом, что стандартные кодеки, применяемые в системах IP-телефонии, ориентированы в первую очередь на преобразование человеческой речи и по этой причине не способны осуществлять эффективную передачу выходного сигнала факсимильного аппарата.

Рекомендация ITU-T T.38 (09/05) "PROCEDURES FOR REAL-TIME GROUP 3 FACSIMILE COMMUNICATION OVER IP NETWORKS" описывает основные принципы построения и реализации специальных шлюзов, которые обеспечивают передачу факсимильных сообщений по сети IP.

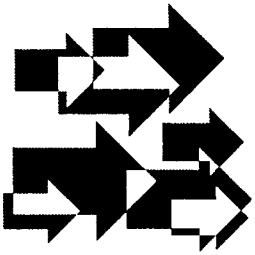
В соответствии с требованиями этой рекомендации, шлюз T.38 выполняет двунаправленное преобразование сигналов стандартного факсимильного аппарата в блоки данных, предназначенные для передачи по сети IP. В табл. 5.4 приведены основные значения скорости передачи факсимильных сообщений, которые поддерживаются шлюзом T.38.

Таблица 5.4. *Скорости передачи факсимильных сообщений T.38*

Спецификация	Скорость передачи данных (Кбит/сек)
V.27ter	2400, 4800
V.29	7200, 9600
V.17	7200, 9600, 12000, 14400

Следует особо отметить, что на шлюз T.38 не возлагаются функции организации и обслуживания телефонного вызова, которые обычно выполняются стандартными сигнальными системами. Именно стандартная сигнальная система инициирует включение шлюза T.38 для обработки телефонного вызова в том случае, если он поступил от факсимильного аппарата. Таким образом, функции, выполняемые шлюзом T.38, полностью соответствуют функциям стандартного кодека, которые обычно используются для преобразования сигналов в мультимедийных системах. Именно поэтому T.38 легко и логично интегрируется в стандартный набор кодеков, которые используются в мультимедийных системах, построенных на протоколах H.323 или SIP.

Применение протокола T.38 не только обеспечивает передачу по сети IP-сообщений с одного факсимильного аппарата на другой, но и позволяет передавать и принимать эти сообщения на обычный персональный компьютер, подключенный к сети Интернет через оборудование Ethernet ЛВС. Использование этого режима существенно снижает расходы на комплектующие материалы и позволяет внедрять дополнительные сервисы в информационную подсистему предприятия, такие, например, как организация факс-сервера или автоматическое архивирование переданных и принятых сообщений.



ЧАСТЬ II

Технологии построения мультисервисных ЛВС

Глава 6. Управление потоками данных в ЛВС

Глава 7. Обеспечение безопасного подключения абонентов

Глава 8. Повышение надежности магистралей мультисервисных ЛВС

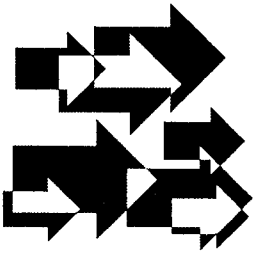
Глава 9. Выравнивание загрузки резервированных узлов мультисервисных ЛВС

Глава 10. Увеличение пропускной способности каналов ЛВС

Глава 11. Организация группового вещания в мультисервисных ЛВС

Глава 12. Управление трафиком приложений мультисервисных ЛВС

ГЛАВА 6



Управление потоками данных в ЛВС

Информационное взаимодействие абонентов современных вычислительных систем является сложным и многоплановым, однако обязательно основано на использовании стандартных решений. Это, с одной стороны, дает возможность применять универсальные устройства и программные модули для реализации этого взаимодействия и, с другой стороны, позволяет осуществлять при необходимости дальнейшее развитие построенных систем.

Вместе с тем, информационное взаимодействие в мультисервисных ЛВС имеет свои особенности, которые необходимо учитывать для их правильного проектирования и эксплуатации. Задача любого проектирования состоит не только в том, чтобы реализовать требования, предъявляемые к характеристикам проектируемого объекта, но и при этом обеспечить максимальную эффективность использования ресурсов.

Эта глава посвящена рассмотрению ресурсов, которые используют современные мультисервисные сети. В ней рассматриваются общие вопросы и специфика информационного взаимодействия в сетях Ethernet/IEEE 802.3, а также особенности построения используемого для его организации оборудования.

В первом разделе приведены общие правила организации потоков данных в современных ЛВС и стандартные способы управления ими, а также определения и краткие описания терминов и понятий, которые используются во второй части книги.

Второй раздел посвящен рассмотрению принципов коммутации и маршрутизации в современных сетях Ethernet/IEEE 802.3. В нем также приведено описание особенностей обработки данных на сетевом и транспортном уровне в мультисервисных сетях и рассматриваются основные принципы построения базовых устройств современных ЛВС — многоуровневых коммутаторов.

Принципы информационного обмена в ЛВС

Информационное взаимодействие в современных ЛВС удобно описывать в терминах эталонной модели организации взаимодействия открытых систем, представленной в международном *стандарте ISO 7498*. Этот стандарт имеет тройной заголовок "Информационно-вычислительные системы — Взаимодействие открытых систем — Эталонная модель". Обычно его называют короче *"Эталонная модель взаимодействия открытых систем" — модель OSI* (Open System Interconnect). Основной идеей, которая положена в основу этого документа, является разбиение процесса информационного взаимодействия между системами на уровни с четко разграниченными функциями. Преимущества слоистой организации взаимодействия заключаются в том, что она обеспечивает независимую разработку уровневых стандартов, модульность аппаратуры и программного обеспечения информационно-вычислительных систем и способствует тем самым техническому прогрессу в сфере телекоммуникаций. Иерархическая организация сетевого взаимодействия позволяет обеспечивать преемственность разработанных структур и их быструю адаптацию к изменениям, происходящим в технологиях передачи данных. Например, при переходе на новый способ передачи данных изменения коснутся только нижних уровней и совсем не затронут верхние в том случае, если система протоколов организована в соответствии с требованиями ISO 7498.

Уровни взаимодействия

В соответствии с ISO 7498 могут быть выделены семь уровней (слоев) информационного взаимодействия.

- *Уровень приложения* (Application Layer) — уровень 7 модели OSI. Протоколы, седьмого уровня OSI, предназначены для обеспечения доступа к ресурсам сети программ-приложений пользователя. В качестве примера протоколов прикладного уровня можно привести протокол *Telnet*, который обеспечивает доступ пользователя к узлу сети в режиме удаленного терминала.
- *Уровень представления* (Presentation Layer) — уровень 6 модели OSI. На этом уровне обычно выполняется преобразование форматов данных, алгоритмы шифрования и компрессии данных.
- *Сеансовый уровень* (Session Layer) — уровень 5 модели OSI. На данном уровне устанавливаются, обслуживаются и разрываются сессии между представительными объектами приложений. В качестве примера протокола сеансового уровня можно рассмотреть протокол *RPC* (Remote Procedure Call).

- *Транспортный уровень* (Transport Layer) — уровень 4 модели OSI. Основной задачей протоколов транспортного уровня является управление доставкой блоков данных протоколов верхних уровней. Протокол TCP — пример протокола транспортного уровня, обеспечивающий гарантированную доставку сегментов данных до объекта назначения и восстановление исходного сообщения. Для выполнения этой задачи протокол TCP устанавливает и разрывает соединение между сетевыми узлами. Протокол UDP обеспечивает передачу данных между сетевыми узлами без функции гарантированной доставки.
- *Сетевой уровень* (Network Layer) — уровень 3 модели OSI. Задачей протоколов сетевого уровня является построение сетевого адреса и определение маршрута доставки информационных блоков протоколов верхних уровней (маршрутизация).
- *Канальный уровень* (Data Link Layer) — уровень 2 модели OSI. Назначением протоколов канального уровня является обеспечение передачи данных по физическому носителю — среде передачи. При использовании топологий "общая шина" средствами протокола канального уровня должны быть определены физические адреса, с помощью которых будет производиться обмен данными по разделяемой среде передачи и процедура доступа к этой среде. Примерами таких протоколов являются протоколы Ethernet (в соответствующей части) и HDLC.
- *Физический уровень* (Physical Layer) — уровень 1 модели OSI. Протоколы физического уровня обеспечивают непосредственный доступ к среде передачи данных для протоколов канального и последующих уровней. На этом уровне определяются набор сигналов, которыми обмениваются системы, параметры этих сигналов — временные и электрические, а также последовательность формирования этих сигналов при выполнении процедуры передачи данных.

Термины и определения

Информационное взаимодействие двух или более объектов, таким образом, представляет собой совокупность информационных взаимодействий уровневых подсистем этих объектов, причем каждый слой локальной информационной системы взаимодействует только с соответствующим слоем удаленного объекта.

Определение

Протоколом мы будем называть набор алгоритмов (правил) взаимодействия объектов одноименных уровней.

Слои (уровни) одной информационной системы также взаимодействуют между собой, причем в непосредственном взаимодействии участвуют только

соседние уровни одного объекта. Как правило, промежуточный уровень использует услуги, которые ему предоставляет нижний уровень, а сам в свою очередь предоставляет услуги для верхнего уровня. Уровни 7—5 считаются верхними уровнями OSI и не отражают специфики конкретной сети. Протоколы этих уровней, как правило, реализуются программными модулями, которые выполняются на каждом из взаимодействующих объектов. Уровни 1—4 считаются нижними уровнями OSI, их выбор целиком определяется требованиями к характеристикам проектируемой сети:

- требованиями к способу доставки данных (транспортный уровень);
- типом используемой сети (сетевой уровень);
- топологией сети (канальный уровень);
- типом используемой среды передачи данных (физический уровень).

Алгоритмы протоколов нижних уровней обычно реализуются на сетевых устройствах, которые обеспечивают передачу данных между взаимодействующими объектами.

Главной характеристикой протокола физического уровня является пропускная способность образованного на его основе канала передачи данных.

Определение

Пропускная способность канала передачи данных — число битов, передаваемых через него за секунду.

На каждом из нижних уровней, кроме физического, используются специфические протоколы, определяющие форматы передаваемых блоков данных и алгоритмы взаимодействия объектов.

Блок данных — PDU (Protocol Data Unit) любого из остальных протоколов нижнего уровня состоит, как правило, из двух основных компонентов:

- *заголовка* (Header);
- *полезной* нагрузки (Data).

В заголовке обычно размещается управляющая информация, которая используется для выполнения правил соответствующего протокола. В заголовке PDU, например, могут размещаться адреса источника и приемника полезной нагрузки этого блока данных, а также уровень его приоритетности по отношению к другим блокам данных или другая информация, определяющая особенности его обработки. Другими словами, структура заголовка полностью определяется типом протокола, который был использован для создания PDU.

Информация, размещаемая в поле полезной нагрузки, обычно представляет собой PDU вышестоящего протокола. Например, в поле полезной нагрузки PDU канального уровня обычно помещается блок данных сетевого уровня.

Определение

Инкапсуляцией называют процесс помещения фрагментированных блоков данных одного уровня в блоки данных другого уроаня.

Обычно инкапсулируются блоки данных протоколов верхних уровней в поле полезной нагрузки протоколов нижних уровней, но также может выполняться инкапсуляция для протоколов одноименных уровней. Например, при построении туннелей PPTP блоки данных протокола канального уровня — PPP инкапсулируются в блоки данных другого протокола канального уровня — Ethernet (см. *главу 8*), при построении виртуальных частных сетей блоки данных сетевого уровня IP инкапсулируются в блоки данных этого же протокола (см. *главу 7*). При этом соответственно увеличивается количество заголовков и, следовательно, возрастает та часть пропускной способности канала передачи данных, которая используется для служебного обмена. А поскольку служебная информация протоколов и данные пользователя передаются в одном канале, то увеличение общего размера заголовков приводит к уменьшению эффективности использования пропускной способности канала.

Определение

Эффективность использования пропускной способности канала передачи данных — отношение скорости, с которой передается полезный трафик к задействованной для его передачи пропускной способности канала.

Для повышения эффективности использования пропускной способности при проектировании мультисервисных ЛВС необходимо соблюдать равновесие между сложностью используемых протоколов и возможностями применяемых каналов передачи данных.

Протоколы современных ЛВС

Подавляющее большинство современных сетей основано на использовании двух технологий — Интернет (TCP/IP) и Ethernet (IEEE 802.3). В табл. 6.1 приведены характеристики основных протоколов, наиболее часто применяемых для организации информационного обмена в современных ЛВС.

Таблица 6.1. *Протоколы, применяемые для обмена данными в современных ЛВС*

Название протокола	Уровень ISO 7498	Обозначение PDU	Документ
TCP (Transmission Control Protocol)	Транспортный	Сегмент	IETF RFC 793
UDP (User Datagram Protocol)	Транспортный	Дейтаграмма	IETF RFC 768
IP (Internet Protocol)	Сетевой	Пакет	IETF RFC 791
Ethernet	Канальный	Кадр	IEEE 802.3

Популярность протоколу Ethernet принесло его использование для организации информационного взаимодействия на канальном уровне в локальных сетях, построенных на среде передаче данных с общим доступом абонентов (коаксиальный кабель — Ethernet-II, IEEE 802.3 — 10 Base 5). В наши дни этот протокол применяется в локальных, районных и городских сетях, которые строятся на средах передачи данных с раздельным доступом абонентов (медный и волоконно-оптический кабель).

Протокол *IP* (Internet Protocol) определяет структуру сетевого адреса и основные принципы построения маршрутов доставки сообщений в сети Интернет.

В сети Интернет используются два протокола транспортного уровня:

- *UDP* (User Datagram Protocol) — протокол дейтаграмм пользователя;
- *TCP* (Transmission Control Protocol) — протокол управления передачей.

Протокол UDP относится к транспортным протоколам доставки дейтаграмм и используется в том случае, если к процессу доставки не предъявляется повышенных требований в части обеспечения надежности, гарантированности доставки и управления темпом информационного обмена.

Протокол TCP является основным транспортным протоколом сети Интернет и обеспечивает возможность управления информационным потоком и гарантированную доставку блоков данных приложений пользователя.

Примечание

В мультисервисных сетях также может использоваться транспортный протокол *RTP* (Real-Time Transport Protocol). Он предназначен для обеспечения приложений, требующих от процесса доставки выполнения установленных временных ограничений.

Протокол канального уровня Ethernet

Современный комплекс протоколов IEEE 802.3 — ISO/IEC 8802-3 хотя и сохраняет название Ethernet, однако очень сильно отличается от первоначального варианта одноименного протокола, разработанного в компании XEROX. Наименьшим изменениям подверглись структура блока данных и общие принципы информационного взаимодействия. Информационное взаимодействие на канальном уровне сетей стандарта Ethernet разделено на два дополнительных уровня:

- LLC (Logical Link Control) — управление логическим каналом;
- MAC (Media Access Control) — управление доступом к среде передачи.

На уровне MAC реализуются алгоритмы протокола, которые отражают специфику используемой среды передачи, например, способы кодирования дан-

ных или обнаружения коллизий. На уровне LLC реализуются общие функции и алгоритмы формирования блоков данных протокола. Такое разделение позволяет с наименьшими изменениями реализовывать алгоритмы протокола Ethernet для различных сред передачи данных.

Технология Ethernet позволяет реализовать три режима передачи данных:

- Unicast — индивидуальная передача;
- Multicast — групповая передача;
- Broadcast — широковещательная передача.

Тип используемого режима передачи данных определяется форматом адреса канального уровня, который называется в Ethernet *MAC-адресом* (MAC-address).

Примечание

Ethernet MAC-адрес (MAC-address) принято также называть *физическим адресом*, поскольку он однозначно определяет точку подключения абонента к среде передачи. Следует, однако, иметь в виду, что MAC-адрес Ethernet является атрибутом канального уровня.

Формат MAC-адреса обеспечивает возможность использования специфических режимов многоадресной передачи данных в сети Ethernet и, одновременно, исключает возможность появления в пределах одной локальной сети двух станций которые имели бы одинаковый адрес.

Физический адрес Ethernet состоит из двух компонентов:

- *идентификатора производителя оборудования* (Vendor code) — 3 байта;
- *индивидуального идентификатора устройства* — 3 байта.

Для обеспечения уникальности MAC-адреса значения идентификатора производителя оборудования (Vendor code) выделяются по запросам фирм-производителей телекоммуникационного оборудования специальной организацией в составе IEEE. Наиболее часто используется шестнадцатеричная форма написания MAC-адреса, в которой байты отделяются друг от друга символами "-", например, 00-e0-14-00-00-00.

При использовании режима адресации Unicast, когда станция-источник адресует передаваемый пакет только одному получателю данных, два младших разряда старшего байта MAC-адреса равны 0. В этом случае в поле DA кадра Ethernet указывается адрес приемника информации.

Режим адресации типа Multicast используется для того, чтобы передавать специальные сообщения для всех компонентов сети, которые имеют одинаковые коды производителя оборудования. Этот режим, в частности, может быть использован для обмена информацией между коммутаторами одного

производителя. Признаком использования режима адресации Multicast является нечетное значение старшего байта MAC-адреса, например, 01-00-0C-CC-CC-CC.

Кадр, содержание поля DA которого принадлежит типу Multicast, будет принят и обработан всеми станциями, которые входят в группу 01-00-0C — в данном случае — это сетевые устройства Cisco. Приведенный Multicast-адрес используется сетевыми устройствами данной фирмы для взаимодействия в соответствии с правилами протокола *CDP* (Cisco Discovery Protocol).

Станция сети Ethernet и IEEE 802.3 может также использовать режим адресации Broadcast. Адрес станции назначения типа Broadcast кодируется специальным значением: FF-FF-FF-FF-FF-FF.

При использовании данного адреса переданный пакет будет принят всеми станциями, которые находятся в том же сегменте сети, где расположена передающая станция. Использование такого режима полезно, например, в том случае, когда передающая станция не может определить адрес получателя данных.

Помимо адреса, который жестко определен при изготовлении (Universally Administered Address), сетевое устройство может получить с помощью специального программного обеспечения адрес, который будет иметь только локальное значение (Locally Administered Address). Признаком использования адреса такого типа является наличие в MAC-адресе источника 1 во втором бите старшего байта идентификатора производителя оборудования.

Структура кадра Ethernet приведена в табл. 6.2.

Таблица 6.2. *Структура кадра Ethernet*

Номер поля	Содержание поля	Длина поля (байт)
1	DESTINATION ADDRESS — адрес назначения кадра	6
2	SOURCE ADDRESS — адрес источника кадра	6
3	LENGTH/TYPE — тип или длина полезной нагрузки кадра	2
4	MAC CLIENT DATA + PAD — полезная нагрузка кадра	46—1500
5	FRAME CHECK SEQUENCE — контрольная сумма кадра	4

В поле DESTINATION ADDRESS отправитель размещает MAC-адрес получателя. Адрес назначения может иметь любой из разрешенных типов — Unicast/Broadcast/Multicast.

В поле SOURCE ADDRESS отправитель размещает свой собственный MAC-адрес, для того чтобы получатель мог его идентифицировать. Адрес источника может быть только индивидуальным (Unicast).

Поле LENGTH/TYPE в зависимости от размещенного в нем значения может быть использовано для указания длины или типа полезной нагрузки данного кадра. Поскольку длина поля полезной нагрузки кадра Ethernet не может быть более 1500 байт, то значения поля LENGTH/TYPE превышающие 1536 (600_{16}) можно использовать для указания типа полезной нагрузки кадра. В табл. 6.3 приведены значения поля LENGTH/TYPE для некоторых протоколов сетевого и канального уровня.

Таблица 6.3. *Значения поля LENGTH/TYPE для популярных протоколов*

Значение поля LENGTH/TYPE		Название протокола	Документ
Система счисления			
10	16		
2048	0800	*IP v4* (Internet Protocol)	IEEE 802.3
2054	0806	*ARP* (Address Resolution Protocol)	
33100	814C	*SNMP* (Simple Network Management Protocol)	
34525	86DD	*IP v6* (Internet Protocol)	
34827	880B	*PPP* (Point To Point Protocol)	
34915	8863	*PPPoE* (PPP over Ethernet Protocol)	

Если значение поля LENGTH/TYPE меньше или равно 1500, тип содержимого поля полезной нагрузки и режим информационного обмена для данного кадра определяется дополнительным заголовком LLC PDU. Заголовок LLC PDU размещается сразу после поля LENGTH/TYPE. Структура заголовка приведена в табл. 6.4.

Таблица 6.4. *Структура заголовка LLC PDU*

Номер поля	Содержание поля	Длина поля (байт)
1	DSAP — адрес службы назначения	1
2	SSAP — адрес службы источника	1
3	CONTROL — управление	1 или 2
4	INFORMATION — полезная нагрузка	Переменная

Поле DSAP (Destination Service Access Point) LLC PDU содержит адрес канального уровня порта назначения данного кадра.

Поле SSAP (Source Service Access Point) LLC PDU содержит адрес канального уровня порта источника для данного кадра. Значение старшего бита данного поля определяет тип данного кадра.

Поле CONTROL занимает один или два байта в LLC PDU и предназначено для передачи управляющего слова или последовательного номера PDU. Управляющее слово может иметь один из следующих форматов:

- I — (information) информационный формат;
- S — (supervisory) служебный формат;
- U — (unnumbered) управляющий формат.

Использование управляющих слов S- и I-типов позволяет при необходимости реализовать режим гарантированной доставки и управление темпом информационного обмена на канальном уровне Ethernet. Более часто, однако, используются LLC PDU U-типа.

В поле MAC CLIENT DATA размещается полезная нагрузка кадра. Длина этого поля является переменной и определяется размером инкапсулируемого блока данных верхнего уровня. Для обеспечения установленного размера коллизионного домена длина передаваемого кадра не должна быть менее 64 байт. При этом минимальная длина поля полезной нагрузки должна составлять 46 байт. В том случае, если инкапсулируемый блок данных имеет меньший размер, содержимое поля данных дополняется произвольными кодировками до величины 46 байт. Поэтому фактически поле данных состоит из двух полей: собственно поля полезной нагрузки, величина которого изменяется от 0 до 1500 байт, и поля заполнения (Pad), размер которого изменяется от 46 байт до 0. Совокупный размер этих полей не может быть меньше 46 байт и больше 1500 байт.

Примечание

Ограничение длины минимального кадра имеет смысл только при использовании разделяемой среды передачи данных. Во всех остальных случаях выполнение этого требования только приводит к снижению эффективности использования канала передачи данных.

Поле FRAME CHECK SEQUENCE занимает 4 последних байта кадра Ethernet и содержит 32-разрядную контрольную сумму, которая вычисляется суммированием содержимого всех информационных полей кадра.

Протокол сетевого уровня IP

В настоящее время применяется две версии этого протокола — версия 4 (IP v4 — современная) и версия 6 (IP v6 — перспективная). Несмотря на то, что перспективная версия обеспечивает существенное улучшение всех характеристик протокола IP, и то, что она поддерживается всеми ведущими производителями телекоммуникационного оборудования и системного программного

обеспечения, она до сих пор не получила большого распространения. Блок данных протокола IP v4 — дейтаграмма состоит из двух частей:

- заголовка дейтаграммы (Datagram Header);
- поля данных дейтаграммы (Datagram Data Area).

Полезная нагрузка (блоки данных протоколов транспортного уровня) размещается в поле данных дейтаграммы. В заголовке дейтаграммы размещается информация, необходимая для доставки полезной нагрузки в узел назначения сети. Структура заголовка дейтаграммы IP представлена в табл. 6.5.

Таблица 6.5. *Структура заголовка дейтаграммы IP*

Номер поля	Содержание поля	Номер байта/ полубайта	Длина поля (бит)
1	VERS — версия протоколв	0/0	4
2	HLEN — длина заголовка	0/1	4
3	PRECEDENCE — приоритет дейтаграммы	1	8
4	TOTAL LENGTH — общая длина	2	16
5	IDENTIFICATION — идентификатор фрагмента	4	16
6	FLAGS — флаги фрагментации	6/0	3
7	FRAGMENT OFFSET — смещение фрагмента	7	13
8	TIME TO LIVE — время жизни дейтаграммы	8	8
9	PROTOCOL — протокол верхнего уровня	9	8
10	HEADER CHECKSUM — контрольная сумма	10	16
11	SOURCE IP ADDRESS — адрес источника	12	32
12	DESTINATION IP ADDRESS — адрес назначения	16	32

В поле VERS заголовка дейтаграммы IP размещается номер версии протокола IP, который был использован для формирования данной дейтаграммы.

Поле HLEN используется для размещения выраженной в 32-битовых словах длины заголовка дейтаграммы.

В поле PRECEDENCE размещается признак относительного приоритета данной дейтаграммы.

Примечание

Содержимое именно этого поля формируется и анализируется с целью обеспечения гарантированного качества обслуживания (специальных методов обработки в сети) для выделенного типа трафика.

Поле TOTAL LENGTH предназначено для указания выраженного в байтах размера поля данных.

В поле IDENTIFICATION содержится уникальный идентификатор, обеспечивающий отличие фрагментов одной дейтаграммы от фрагментов другой дейтаграммы. Все фрагменты одной дейтаграммы должны иметь уникальное сочетание IDENTIFICATION + IP Source Address указанных полей.

Примечание

Фрагментация дейтаграммы выполняется в том случае, если ее длина превышает размер максимального передаваемого блока — *MTU* (Maximum Transfer Unit) данных при инкапсуляции в PDU протокола канального уровня. Например, для протокола Ethernet это ограничение составляет 1500 байт.

Значение младшего бита поля FLAGS определяет, возможно или нет выполнение фрагментации данной дейтаграммы. Средний бит имеет название MF (More Fragments). Значение этого бита определяет порядок данного фрагмента в общей цепочке фрагментов данного сообщения. У всех, кроме последнего, фрагментов одного сообщения бит MF должен быть установлен в 1.

Содержимое поля FRAGMENT OFFSET определяет смещение, которое выражено в 8-байтовых отрезках и соответствует месту данного фрагмента в исходном сообщении.

Поле TIME TO LIVE используется для размещения времени жизни дейтаграммы в сети Интернет. При перемещении дейтаграммы по сети значение поля TIME TO LIVE уменьшается на время, которое было затрачено на ее обработку в каждом активном узле. В том случае если значение этого поля становится равным 0, то дейтаграмма считается просроченной и уничтожается.

В поле PROTOCOL размещается тип протокола, который был использован при формировании полезной нагрузки данной дейтаграммы. Наиболее часто таким протоколом является протокол транспортного уровня. Однако некоторые протоколы маршрутизации и управления сетью также способны внедрять свои PDU непосредственно в поле полезной нагрузки протокола пакета IP. В табл. 6.6 приведены значения поля PROTOCOL для некоторых популярных протоколов современных ЛВС.

Таблица 6.6. *Значения поля PROTOCOL для популярных сетевых протоколов*

Значение/ обозначение		Назначение протокола
1	*ICMP*	Internet Control Message Protocol — обмен управляющими сообщениями сети Интернет
2	*IGMP*	Internet Group Management Protocol — управление MULTICAST-трафиком

Таблица 6.6 (окончание)

Значение/ обозначение		Назначение протокола
6	*TCP*	Transmission Control Protocol — управление доставкой данных
17	*UDP*	User Datagram Protocol — передача дейтаграмм
46	*RSVP*	Resource Reservation Protocol — резервирование ресурсов сети
88	*IGRP*	Internet Gateway Routing Protocol — передача сообщений протокола маршрутизации IGRP (Cisco Systems)
89	*OSPF*	Open Shortest Path First — передача сообщений протокола маршрутизации OSPF

Поле HEADER CHECKSUM используется для размещения контрольной суммы заголовка дейтаграммы.

Транспортный протокол UDP

Протокол *UDP* (Transmission Control Protocol) реализует обмен между приложениями удаленных абонентов, используя для этого минимальное количество управляющих параметров. Как уже было отмечено, протокол UDP не обеспечивает достоверность при доставке данных, защиту от дублирования данных и защиту от потери данных при передаче. Достоинствами протокола UDP являются простота его реализации и экономичность. За исключением параметров приложения — номеров портов отправителя и получателя пакета — UDP практически ничего не добавляет к исходной дейтаграмме, полученной от сетевого уровня IP.

Блоки данных, которые передаются протоколом UDP на транспортном уровне, также называются *дейтаграммами*. Дейтаграммы UDP имеют переменную длину и состоят из заголовка сообщения и поля полезной нагрузки. Признаком размещения дейтаграммы протокола UDP в поле полезной нагрузки дейтаграммы протокола IP служит значение поля PROTOCOL. В табл. 6.7 представлена структура заголовка дейтаграммы UDP.

***Таблица 6.7.** Структура заголовка дейтаграммы UDP*

Номер поля	Содержание поля	Длина поля (байт)
1	UDP SOURCE PORT — порт источника дейтаграммы	2
2	UDP DESTINATION PORT — порт получателя дейтаграммы	2
3	UDP MESSAGE LENGTH — длина дейтаграммы	2
4	UDP CHECKSUM	2
5	DATA	> 0

В поле UDP SOURCE PORT должен быть помещен номер порта, с которого был отправлен пакет. Если значение этого поля не используется в информационном обмене между приложениями, то оно должно быть заполнено нулями. В табл. 6.8 приведен перечень портов, используемых наиболее популярными приложениями.

Таблица 6.8. *Перечень портов популярных приложений Интернета*

Порт	Протокол	Приложение	Назначение
21	*FTP*	File Transfer Protocol	Передача файлов
23	*Telnet*	Telnet Protocol	Виртуальный терминал
25	*SMTP*	Simple Mail Transfer Protocol	Отправка почтовых сообщений
69	*TFTP*	Trivial File Transfer Protocol	Передача файлов
80	*HTTP*	World Wide Web (HTTP) Protocol	Разметка страниц WWW
110	*POP3*	Post Office Protocol	Получение почтовых сообщений
123	*NTP*	Network Time Protocol	Синхронизация часов
161	*SNMP*	Simple Network Management Protocol	Управление сетью
1812	*RADIUS*	Remote Access	Управление доступом абонента

Поле UDP DESTINATION PORT определяет порт назначения — интерфейс приложения, на который должна быть доставлена данная дейтаграмма.

В поле UDP MESSAGE LENGTH помещается значение, соответствующее длине данной дейтаграммы. Минимальное значение UDP Message Length равно 8.

Поле UDP CHECKSUM используется для размещения контрольной суммы дейтаграммы протокола UDP.

Протокол UDP полезен в таких ситуациях, когда мощные механизмы обеспечения надежности протокола TCP не требуются или будут только помехой для решения определенного рода задач, например, для передачи потокового трафика. Дополнительным преимуществом протокола UDP является то, что он требует минимум установок и параметров для соединения двух процессов между собой.

Транспортный протокол TCP

Протокол *TCP* (Transmission Control Protocol) используется для организации надежного информационного обмена в сети Интернет и обеспечивает:

- потоковый режим информационного обмена;
- организацию виртуальных соединений;

- согласование скорости информационного потока и пропускной способности канала передачи данных;
- возможность одновременного приема и передачи информации.

Надежный информационный обмен на транспортном уровне может быть представлен в виде виртуального логического соединения. На начальной стадии одна из взаимодействующих сторон инициирует установление соединения, используя при этом по мере необходимости процедуры аутентификации. В процессе информационного обмена через установленное соединение обе стороны контролируют качество этого обмена и при возникновении неразрешимых проблем могут инициировать процесс разрыва соединения и формировать соответствующие сообщения для протоколов верхних уровней.

Использование буферов позволяет согласовать скорость информационного обмена в канале передачи данных со значением скорости передачи данных приложением пользователя. В том случае, если скорость передачи данных в канале намного превышает скорость формирования данных приложением, целесообразно накапливать передаваемые данные в буфере и передавать их затем в виде блока. Такой способ позволит повысить эффективность использования канала передачи данных, поскольку обеспечивает существенное снижение накладных расходов.

Для обеспечения требования доставки трафика, который чувствителен к временным задержкам, в дополнение к буферу может быть использован дополнительный механизм "push" — поршень. Использование данного механизма обеспечивает форсирование передачи содержимого буфера в тот момент, когда в него попадают данные, чувствительные к временным задержкам.

Надежное транспортное соединение должно обеспечивать передачу и прием данных взаимодействующими приложениями одновременно. Помимо увеличения результирующей скорости информационного обмена, этот режим обеспечивает повышение эффективности использования канала передачи данных.

При передаче данных протокол TCP использует схему позитивного подтверждения с повторной передачей (positive acknowledgement with retransmission). Применение подобной схемы обеспечивает динамическое управление скоростью информационного обмена, что позволяет успешно применять протокол TCP на самых разнообразных каналах передачи данных.

Для предотвращения появления в сети пакетов с одинаковыми номерами при установлении нового соединения генерируется 32-битное число ISN (Initial Sequence Number).

Поврежденные пакеты отсеиваются механизмом проверки величины контрольной суммы данных, которая размещается в каждом передаваемом пакете.

Инициализация соединения начинается с обмена пакетами, которые отправляются при открытии канала пользователем и содержат флаг SYN и свой начальный порядковый номер пакетов данных. Соединение закрывается, когда абоненты обмениваются пакетами, содержащими команду FIN. При этом все ресурсы системы, занятые этим соединением, должны быть освобождены.

Протокол TCP позволяет получателю регулировать передаваемый отправителем поток данных. При передаче флага подтверждения получения пакета (ACK) в TCP-сегменте получатель информации передает размер "окна" — блока данных, который может быть передан отправителем без получения подтверждения от получателя. Размер "окна" задается количеством байтов, отсчитываемых от номера, заданного в поле Acknowledgment Number последнего полученного сообщения. Нулевой размер окна означает для отправителя команду приостановить передачу до готовности принимать данные получателем.

Протокол TCP имеет в своем распоряжении механизм работы с флагом важности пакетов — URG. Этот механизм позволяет отправителю "настоятельно сообщать" получателю о том, что тот или иной пакет содержит срочную информацию, и позволяет получателю сигнализировать, когда вся срочная информация им получена. Такой механизм уведомления, т. е. манипулирование с URG-флагом TCP-пакета, используется, например, при обработке асинхронных событий.

Для обеспечения достоверной и управляемой передачи данных протокол TCP разбивает входящий информационный поток на блоки — сегменты. Признаком размещения сегмента протокола TCP в поле полезной нагрузки дейтаграммы протокола IP служит значение поля PROTOCOL. Каждый из сегментов состоит из заголовка — TCP-header и поля передаваемых данных. Структура заголовка сегмента TCP представлена в табл. 6.9.

Таблица 6.9. *Структура заголовка сегмента TCP*

Номер поля	Содержание поля	Длина поля (бит)
1	SOURCE PORT — порт источника данных	16
2	DESTINATION PORT — порт получателя данных	16
3	SEQUENCE NUMBER — номер первого байта передаваемого сегмента	32
4	ACKNOWLEDGMENT NUMBER — номер первого байта сегмента, ожидаемого к приему	32
5	DATA OFFSET — длина заголовка сегмента, измеренная в 32-битных словах	4

Таблица 6.9 (окончание)

Номер поля	Содержание поля	Длина поля (бит)
6	RESERVED — зарезервировано для дальнейшего использоаания	6
7	FLAGS — флаги	6
8	WINDOW — размер сегмента, разрешенный к приему	16
9	CHECKSUM — контрольная сумма	16
10	URGENT POINTER — указатель на фрагмент повышенной срочности в теле передаваемого сегмента	16

Поля SOURCE PORT и DESTINATION PORT в заголовке сегмента TCP имеют такое же значение, как и одноименные поля в протоколе UDP.

Содержимое поля Sequence Number определяет номер первого байта передаваемых данных в этом сегменте. Если в пакете присутствует флаг SYN, то номер данного пакета становится номером начала последовательности (ISN) и номером первого байта данных становится номер ISN+1.

В поле ACKNOWLEDGMENT NUMBER обычно размещается номер следующего сегмента данных отправителя, который ожидает получатель. При установленном соединении сегмент подтверждения отправляется всегда.

Содержимое поля DATA OFFSET определяет смещение расположения поля данных в пакете.

Поле RESERVED заголовка сегмента TCP зарезервировано для возможного использования в будущем.

В поле FLAGS размещаются флаги управления информационным обменом протокола TCP:

- URG — флаг срочности;
- ACK — флаг пакета, содержащего подтверждение получения;
- PSH — флаг форсированной отправки;
- RST — переустановка соединения;
- SYN — синхронизация чисел последовательности;
- FIN — флаг окончания передачи со стороны отправителя.

В поле WINDOW помещается размер окна — количество байт данных, которое отправитель данного сегмента может принять без уведомления о получении, отсчитанное от номера байта, указанного в поле Acknowledgment Number.

В поле CHECKSUM помещается контрольная сумма сегмента. Если сегмент содержит нечетное число байт заголовка и данных, то последний байт дополняется справа нулями.

Поле URGENT POINTER предназначено для размещения указателя срочных данных. В нем содержится значение порядкового номера, начиная с которого размещаются данные повышенной срочности.

Структура информационных потоков ЛВС

Информационные потоки современных ЛВС, как правило, имеют сложную структуру, которая отражает иерархический характер выполняемого информационного взаимодействия. Передаваемая в информационном потоке последовательность битов представляет собой иерархически инкапсулированные блоки данных протоколов различных уровней. В листинге 6.1 представлена структура одного из кадров Ethernet/IEEE 802.3 из потока доступа к серверу 10.11.0.2 по протоколу Telnet.

Примечание

Этот и все следующие ниже листинги структур кадров были получены при помощи программного анализатора кадров (IPgrab packet sniffer — Mike Borella).

Листинг 6.1. Кадр Ethernet доступа к серверу по протоколу Telnet

```
*************************************************************
                        Ethernet (1132725226.271737)
-------------------------------------------------------------
Hardware source:        00:c0:7b:9f:75:f8
Hardware destination:   00:04:9b:82:10:00
Type / Length:          0x800 (IP)
Media length:           62
-------------------------------------------------------------
                        IP Header
-------------------------------------------------------------
Version:                4
Header length:          5 (20 bytes)
TOS:                    0x00
Total length:           48
Identification:         34521
Fragmentation offset:   0
Unused bit:             0
Don't fragment bit:     1
More fragments bit:     0
```

```
Time to live:           64
Protocol:               6 (TCP)
Header checksum:        25841
Source address:         10.11.0.2
Destination address:    27.16.17.44
-------------------------------------------------------------
TCP Header
-------------------------------------------------------------
Source port:            23 (telnet)
Destination port:       2184 (unknown)
Sequence number:        2683083310
Acknowledgement number: 4039718033
Header length:          5 (20 bytes)
Unused:                 0
```

Данные, представленные в листинге 6.1, показывают содержимое заголовков блоков данных трех уровней информационного взаимодействия: канального — Ethernet, сетевого — IP, и транспортного — TCP.

Анализ содержимого заголовка канального уровня показывает, что этот кадр был сформирован станцией с MAC-адресом 00:c0:7b:9f:75:f8, имеет полезную нагрузку, сформированную протоколом IP, и отправлен станции с MAC-адресом 00:04:9b:82:10:00. Данные заголовка сетевого уровня (IP HEADER) указывают на то, что этот пакет сформирован узлом, имеющим адрес 10.11.0.2, содержит сегмент данных, передаваемых транспортным протоколом TCP, и предназначен для узла с IP-адресом 27.16.17.44. В заголовке сегмента TCP имеется указание о том, что полезная нагрузка сегмента предназначена для обработки процессом прикладного уровня Telnet (порт 23).

Совсем необязательно, однако, чтобы в кадре Ethernet находились блоки данных всех вышестоящих уровней. В некоторых случаях вся процедура информационного обмена может быть выполнена в пределах одного канального уровня. В листинге 6.2 представлена структура одного из кадров Ethernet/IEEE 802.3, которыми обмениваются между собой прозрачные мосты при выполнении процедур протокола Spanning Tree (подробнее о протоколе Spanning Tree см. в *главе 8*).

Листинг 6.2. Кадр Ethernet, содержащий BPDU протокола Spanning Tree

```
*************************************************************************
                        Ethernet (1132725224.684009)
-------------------------------------------------------------------------
Hardware source:        00:04:9a:b6:bd:c7
Hardware destination:   01:80:c2:00:00:00 //Адрес MULTICAST - STP
```

```
Type / Length:          0x26 (unknown)
Media length:           60
------------------------------------------------------------------------

                        LLC header
------------------------------------------------------------------------

DSAP:                   66
SSAP:                   66
Control:                3
************************************************************************

Flags:                  PA
Window size:            4380
Checksum:               9865
Urgent:                 0
************************************************************************
```

Этот кадр сформирован прозрачным мостом с MAC-адресом 00-04-9a-b6-bd-c7, имеет полезную нагрузку, сформированную протоколом STP, и отправлен по групповому MAC-адресу 01-80-c2-00-00-00 для того, чтобы обеспечить его прием всеми остальными прозрачными мостами.

Принципы построения и компоненты сегментированных ЛВС

В современных вычислительных сетях взаимодействующие объекты очень редко бывают непосредственно связаны друг с другом. Обычно их разделяют (и в то же время — связывают) одно или несколько промежуточных устройств-посредников. Необходимость использования подобных устройств может быть вызвана различными причинами: физическими ограничениями используемой среды передачи данных, требованиями по обеспечению информационной безопасности, особенностями реализации процедуры доступа к среде и т. д. В любом случае устройство-посредник является активным компонентом ЛВС и обеспечивает информационный обмен на одном или нескольких уровнях OSI ISO 7498 между взаимодействующими устройствами. При этом общая сеть, соединяющая абонентов, разделяется на отдельные участки — *сегменты*.

Определение

Сегментом называется отделенный посредником от остальной сети фрагмент ЛВС, который может включать в себя рабочие станции абонентов и связывающие их активные компоненты.

Задача построения сегментов — сегментирование ЛВС — является очень важной, поскольку правильность ее решения во многом определяет основные

эксплуатационные характеристики проектируемой ЛВС, к которым относятся:

- степень доступности сетевых ресурсов;
- скорость информационного обмена в сегменте;
- уровень информационной безопасности;
- обеспечение требуемого уровня качества обслуживания.

Типы сегментов ЛВС

Сегменты ЛВС представляют собой административные блоки, для каждого из которых администратор может определить независимые политики обеспечения информационной безопасности и качества обслуживания. Тип сегмента определяется тем, какое именно активное оборудование было использовано для его построения. В дальнейшем будут рассматриваться сегменты физического канального и сетевого уровней. На рис. 6.1 представлена схема информационного взаимодействия двух абонентов, обозначенных буквами A и B, в сегментированной ЛВС.

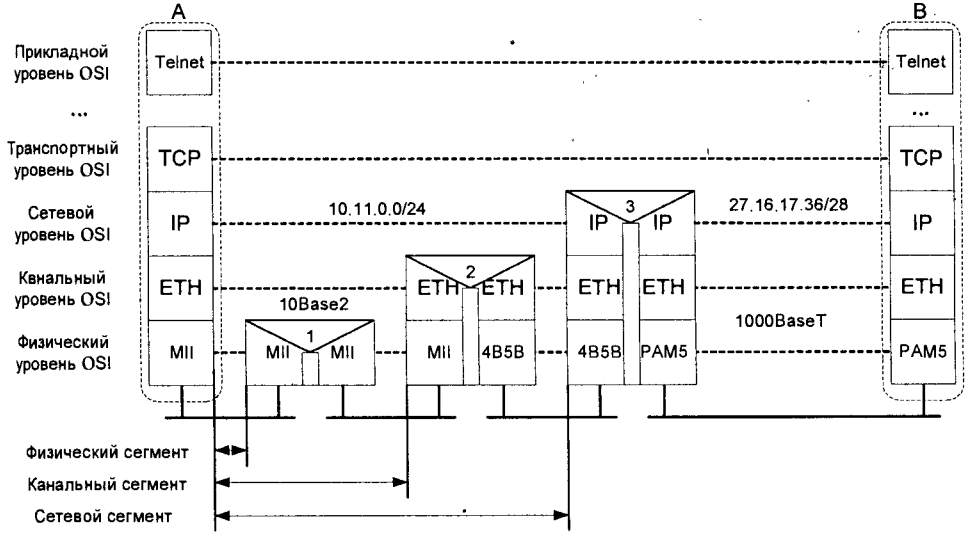


Рис. 6.1. Схема информационного взаимодействия в сегментированной ЛВС

Цифрами 1, 2 и 3 на рисунке обозначены посредники физического, канального и сетевого уровня соответственно. Аббревиатура "ETH" — здесь использована для обозначения протокола канального уровня Ethernet/IEEE802.3, "MII" — обозначает протокол физического уровня *Manchester-II*. Как видно

на рисунке, сетевой сегмент ЛВС может включать в себя один или несколько канальных сегментов, а канальный — один или несколько физических. Для каждого типа сегментов определяются значения ключевых атрибутов соответствующего уровня информационного взаимодействия, например, значения адресов канального или сетевого уровней. Функции протоколов 1, 2 и 3 уровня реализуются посредниками, как правило, аппаратно. Аппаратная реализация в данном случае призвана обеспечить необходимые уровни быстродействия и надежности.

В зависимости от характера реализуемой политики обслуживания и возможностей используемого активного оборудования, в каждом из сегментов администратор может также определить специальные процедуры обработки данных для каждого из сегментов. Так, например, в сети может быть создан специальный сетевой сегмент с повышенной защитой для размещения оборудования учета клиентского трафика. Правильно выбрав схему сегментирования и активные компоненты ЛВС, администратор может легко проводить дальнейшее развитие сети, распределяя новых абонентов между существующими сегментами, или создавая при необходимости новые сегменты и политики обслуживания.

Физический сегмент ЛВС

Физический сегмент ЛВС образуется фрагментом среды передачи данных, который соединяет взаимодействующих абонентов. В зависимости от типа этой среды физический сегмент может соединять двух (витая пара, ВОЛС) или более (коаксиальный кабель) абонентов. На сегменте физического уровня определяются тип кодирования, скорость и режим передачи данных (на физическом сегменте, отмеченном на рис. 6.1, это Manchester-II, 10 Мбит/сек и Half Duplex — соответственно). Активные устройства, соединяющие сегменты физического уровня, называются *повторителями* или *репитерами* (Repeater).

Репитеры выполняют задачу объединения сегментов локальной сети на физическом уровне. Для каждого типа среды передачи данных существуют ограничения на размер сегмента, число подключенных станций, расстояния между ними и т. д. Эти ограничения определяются собственно типом среды передачи данных и протоколом физического уровня, который на ней реализован. Для преодоления этих ограничений и предназначены устройства данного типа. Основной функцией репитера (повторителя) является компенсирование деградации параметров сигнала (амплитуды электрического импульса, длительности переднего и заднего фронтов), которая неминуемо возникает при прохождении сигнала от источника через среду передачи данных к приемнику.

Канальный сегмент ЛВС

Канальный сегмент ЛВС образуется фрагментом среды передачи данных, к которому подключены абоненты, выполняющие специальную процедуру обработки передаваемых данных. На данном сегменте определяются параметры передаваемых кадров (например, Maximum Transfer Unit — MTU), а также выполняются специальные процедуры обеспечения нормального функционирования (Spanning Tree). Активные устройства, соединяющие сегменты канального уровня, называются *мостами* (Bridge) или *коммутаторами* (Switch).

Мосты выполняют задачу объединения сегментов локальной сети на канальном уровне. Одновременно этими устройствами выполняется задача разделения этих же сегментов на физическом уровне (это особенно важно для сетей с CSMA/CD). Мост анализирует проходящие через его интерфейсы кадры протокола канального уровня в части физического адреса источника и на основании этого анализа формирует внутренние таблицы. Пользуясь этой таблицей, мост может выполнять задачу перенаправления кадров в соответствующие интерфейсы в зависимости от содержания поля адреса назначения. Многопортовые мосты принято называть коммутаторами. К портам коммутатора могут быть подключены как отдельные станции, так и физические сегменты ЛВС (через повторители). Современные коммутаторы, кроме того, позволяют управлять возможностью подключения абонентов и взаимодействия между ними (подробнее см. *главу 8*).

Сетевой сегмент ЛВС

Сетевой сегмент включает в себя один или несколько связанных канальных сегментов, к которым подключены абоненты, настроенные на использование одного значения адреса сети. Следовательно, для сетевых сегментов должны быть определены диапазоны связанных с ними адресов сетевого уровня — Network Addresses (в данном случае — 10.11.0.0/24 и 27.16.17.36/28). Активные устройства, соединяющие сегменты сетевого уровня, называются *маршрутизаторами* или *роутерами* (Router).

Маршрутизаторы выполняют задачу объединения локальных сетей на третьем уровне OSI ISO 7498 — сетевом. Основная функция, которую выполняет маршрутизатор, соответствует его названию — определение пути, по которому должны быть переданы пакеты для того, чтобы достичь заданного сетевым адресом пункта назначения. Для решения этой задачи маршрутизатор анализирует сетевые адреса назначения приходящих на его интерфейсы пакетов и может использовать различные способы и алгоритмы маршрутизации. В качестве маршрутизатора может быть использовано как специальное устройство *(аппаратный маршрутизатор)*, так и рабочая станция, на которой установлено соответствующее программное обеспечение *(программный*

маршрутизатор). Помимо своей основной задачи, маршрутизаторы также могут выполнять множество дополнительных функций: обслуживание списков доступа, сетевой мониторинг и т. д.

Основные функции коммутатора Ethernet

Общие принципы функционирования моста (Bridge), или иначе коммутатора (Switch), в сети Ethernet описаны в документе IEEE/ANSI 802.1D, который является прообразом стандарта ISO/IEC 15802-3:1998.

Как уже было ранее отмечено, мост выполняет функцию *распределения кадров* в локальной вычислительной сети. Принцип действия моста достаточно прост: он анализирует адрес канального уровня станции назначения, который размещен в пришедшем на его входной порт кадре и на основании этого анализа принимает решение о *трансляции* (forwarding) этого кадра на тот или иной свой выходной порт. При этом мост использует таблицу фильтрации (filter), которую сам создает и обслуживает в процессе *обучения* (learning). *Таблицу фильтрации*, в соответствии с которой выполняется трансляция кадров, мост формирует автоматически в динамическом режиме.

Формирование таблицы фильтрации

В момент первоначального включения моста его таблица фильтрации пуста. Для того чтобы заполнить таблицу, мост использует режим самообучения. В этом режиме мост анализирует содержимое поля адреса источника у принятого кадра и формирует соответствующую запись в своей таблице, указывая в ней номер порта, на который был принят кадр и MAC-адрес источника этого кадра. В итоге через некоторое время у моста появляется таблица, в которой находятся MAC-адреса компонентов локальной сети, проявивших активность во время выполнения процедуры обучения моста, и номера портов коммутатора, на которые были приняты переданные ими кадры. После завершения процедуры обучения мост переходит к выполнению своей основной функции — *трансляции* входящих кадров на те порты, за которыми размещены их получатели. Если в процессе своего последующего функционирования мост принимает кадр, адрес назначения которого отсутствует в его таблице, мост транслирует такой кадр через все свои порты, за исключением того, с которого этот кадр был получен — эта функция называется *затоплением* (flooding). В том случае, если мост принимает кадр, адрес назначения которого закреплен в таблице за тем же портом, на который он был принят, то такой кадр подлежит уничтожению.

Обработка принимаемых кадров

Сформированная на этапе обучения таблица может дополняться в процессе функционирования моста — в частности, из таблицы, по соображениям эко-

номии места, могут удаляться записи, содержащие адреса абонентов, которые в течение установленного интервала времени не проявляли активности. В том случае, если адрес назначения принятого кадра имеет тип Broadcast канального уровня (FF-FF-FF-FF-FF-FF), мост должен передать этот кадр через все свои порты, за исключением того порта, на который он был принят. Такой же способ может быть использован для обработки кадров, адресом назначения которых является Multicast канального уровня.

Примечание

Более эффективного использования пропускной способности сети при обработке MULTICAST-трафика можно добиться, если использовать дополнительные возможности, предоставляемые современными многопортовыми мостами, иначе — коммутаторами (см. *главу 11*).

У всех принятых кадров мост проверяет соответствие контрольной суммы кадра (FCS) и записанного в теле кадра значения FCS. В том случае если эти значения не совпадают, то кадр подлежит уничтожению.

Таким образом, функционирование прозрачного моста заключается в выполнении следующих процедур:

- *фильтрация и трансляция кадров*;
- *построение и модификация служебных таблиц*;
- *общее управление процессом передачи данных и обеспечение надежности функционирования.*

Поскольку для выполнения основных процедур моста (построение таблицы фильтрации, трансляция кадров) не требуется выполнение информационного обмена между мостом и абонентами сети, а также информационный обмен между мостами, то можно сказать, что мост такого типа является невидимым в ЛВС. По этой причине мосты данного типа принято называть *прозрачными* (transparent bridge). На рис. 6.2 приведен пример формирования таблицы фильтрации прозрачного моста.

Таким образом, использование мостов при построении локальной вычислительной сети обеспечивает ряд преимуществ:

- повышение эффективности информационного обмена;
- увеличение размера сети;
- изолирование ошибок, которые могут возникнуть в сети;
- обеспечение подключения большего количества станций.

Повышение эффективности информационного обмена при использовании мостов достигается за счет того, что мост передает в каждый сегмент только кадры, адресованные абонентам данного сегмента. Вследствие этого умень-

шается нагрузка на каналы передачи данных и снижается вероятность возникновения коллизии в сегменте при использовании полудуплексного (Half-Duplex) режима обмена.

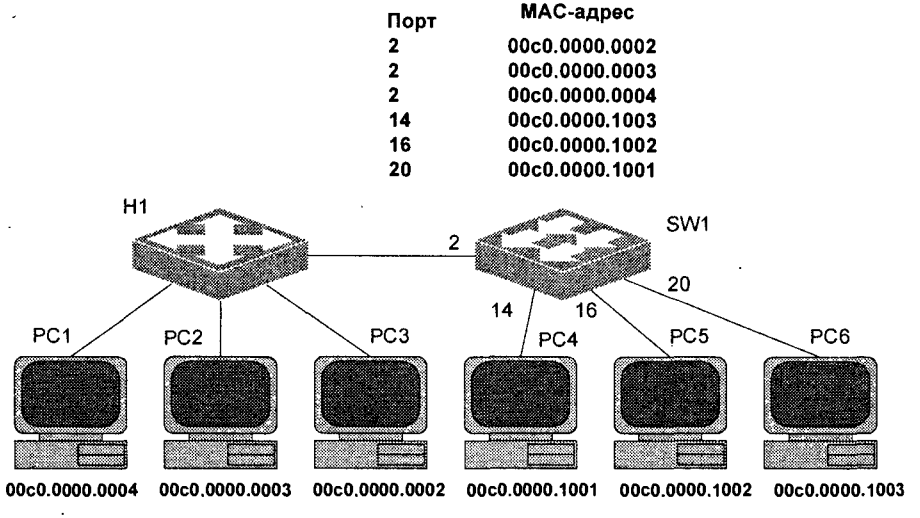


Рис. 6.2. Пример формирования таблицы фильтрации прозрачного моста

Поскольку в коммутаторе прием и передача данных осуществляется по независимым каналам, то он выполняет функцию разделения общего коллизионного домена сети на коллизионные домены сегментов. Путем применения каскадного включения мостов можно легко добиться увеличения геометрического размера сети и числа подключенных станций. Фильтрация, которую на канальном уровне осуществляет мост, автоматически изолирует неисправные сегменты от остальной сети, обеспечивая повышение уровня готовности всей системы в целом.

Способы построения коммутаторов

Как уже было ранее отмечено, основными функциями прозрачного моста IEEE 802.1D являются фильтрация и трансляция кадров. В зависимости от способа выполнения этих функций и особенностей внутренней организации различают следующие типы коммутаторов:

- *сквозные* (Cut-through);
- *запоминающие* (Store and forward);
- *гибридные* (Fragment-free).

Сквозные коммутаторы начинают передачу входящего кадра на выходной порт уже после приема первых шести байтов, в которых размещается адрес

назначения этого кадра. Очевидно, что такие коммутаторы обеспечивают максимальную скорость трансляции кадра, однако они принципиально не способны обеспечить фильтрацию искаженных кадров.

Наиболее распространены в настоящее время запоминающие коммутаторы. Коммутаторы этого типа начинают передачу принятого кадра только после того, как он был полностью принят и проверен на соответствие принятых и рассчитанных значений контрольных сумм кадра. Таким образом, запоминающие коммутаторы используют потенциально наименее быструю схему коммутации, однако способны обеспечить наиболее полную и корректную обработку кадров. Некоторые коммутаторы имеют возможность динамического переключения режимов обработки кадров из сквозного к запоминающему режиму и обратно, в зависимости от установленного порогового значения уровня ошибок в принятых кадрах.

Гибридный метод построения коммутаторов является наименее распространенным и предусматривает обработку кадров минимальной длины (64 байта) по методу с запоминанием и обработку всех остальных кадров в соответствии с принципом сквозной коммутации.

Примечание

Следует отметить, что кадры, имеющие длину именно 64 байта, достаточно часто используются для передачи данных в сети Ethernet/IEEE 802.3. В некоторых случаях их доля может составлять до 30% от общего объема передаваемых кадров. Дело в том, что 64 байта — это минимально возможная длина кадра в сети Ethernet/IEEE 802.3 и, следовательно, именно эту длину будут иметь кадры, размер полезной нагрузки которых не превышает 46 байт. К числу таких, например, относятся кадры, переносящие короткие сообщения протоколов ICMP, SNMP, Telnet и т. д.

Современные коммутаторы различаются также по типу внутренней структуры и способу реализации фильтрации кадров. Наиболее распространены три разновидности архитектур, к которым относятся:

- *Общая память* (Shared-memory)

  Входящий кадр запоминается в едином оперативном запоминающем устройстве коммутатора. После обработки этот кадр направляется для передачи на один или несколько выходных портов. Следует отметить, что эта архитектура предполагает наличие у коммутатора буферной памяти, где размещается очередь кадров, подлежащих обработке и отправке.

- *Коммутирующая матрица* (Matrix)

  При использовании данной архитектуры входы и выходы коммутатора соединяются с матрицей, которая управляется таблицей фильтрации и обеспечивает одновременную трансляцию нескольких кадров.

- *Шинная архитектура* (Bus-architecture)

  Этот тип архитектуры коммутатора в некотором смысле является упрощенным вариантом матричной архитектуры и предполагает наличие общей шины, доступ подключенных портов к которой для трансляции кадров выполняется по схеме разделения времени (Time Division Multiplexing).

Наиболее распространенной в настоящее время для коммутаторов Ethernet/IEEE 802.3 является архитектура с общей памятью и ее разновидности, использующие элементы матричной и шинной архитектур. Некоторые производители используют также разнообразные аппаратные и программные решения, которые позволяют сократить время обработки кадра на коммутаторе. В частности, у коммутаторов Cisco Catalyst трансляция кадров выполняется под управлением *таблицы CAM* (Content Addressable Memory — запоминающее устройство, доступ к которому осуществляется по содержимому). При этом все поступающие кадры, содержание которых соответствует установленному шаблону, обращаются к одной записи в CAM, содержащей номера портов коммутатора, через которые данный кадр должен быть отправлен. Формирование и обслуживание записей в CAM производится следующим образом:

- начальная запись формируется в соответствии со значением MAC-адреса источника по стандартной процедуре обучения порта прозрачного моста IEEE 802.1D. При этом каждая запись снабжается меткой времени создания;
- временная метка модифицируется новым значением при получении очередного кадра, подтверждающего данную запись в таблице CAM;
- если в течение установленного интервала времени (по умолчанию 300 сек) коммутатор не получит кадров, подтверждающих данную запись в таблице CAM, то эта запись подлежит удалению;
- в том случае, если в таблице CAM появится более одной записи соответствующей одному MAC-адресу, то система управления оставит в таблице только запись с наиболее поздним значением метки времени. Остальные записи будут удалены до истечения интервала тайм-аута, что исключает возможность бесконечной циркуляции кадра внутри коммутатора.

Основные и вспомогательные функции маршрутизатора

Как уже было выше отмечено, основной функцией маршрутизатора является определение пути, по которому должны быть переданы пакеты для того, чтобы достичь заданного сетевым адресом пункта назначения. В современных

ЛВС, однако, маршрутизатор выполняет также множество дополнительных функций. Это объясняется тем, что прежде маршрутизатор всегда являлся наиболее интеллектуальным из активных компонентов ЛВС. Функции маршрутизатора обычно были реализованы в виде отдельных задач-процессов выполняемых на мощной ЭВМ, действующей под управлением надежной OS. Поэтому кроме построения и обслуживания таблиц маршрутов на маршрутизаторе могут выполняться:

- *трансляция сетевых адресов*;
- *обслуживание списков доступа*;
- *межсетевое экранирование*;
- *функции универсального посредника*;
- *обнаружение вторжений и сетевой мониторинг*.

Несмотря на то, что для выполнения некоторых из отмеченных функций сегодня используются специальные устройства, а остальные успешно реализуются на активном оборудовании канального уровня, все эти функции попрежнему считаются дополнительными функциями маршрутизатора.

Построение маршрута передачи пакетов

Для упрощения решения задачи маршрутизации сетевой адрес протокола IP составляется из двух частей — адреса сети и адреса узла. Таким образом, задача построения маршрута распадается на две подзадачи — поиск сети и поиск узла в этой сети. Маршрут в сети IP строится по адресу сети с использованием принципа *Hop-By-Hop*. Этот принцип предполагает, что каждый из маршрутизаторов определяет не весь маршрут передачи пакета, а только фрагмент этого пути до следующего маршрутизатора. Следовательно, для решения задачи построения пути маршрутизатору достаточно построить таблицу маршрутизации, в которой для каждой из сетей надо определить адрес ближайшего соседа или номер подключенного к нему интерфейса.

Сетевой адрес у протокола IP состоит из четырех байтов. Адрес сети может занимать в нем от 1 до 3 байтов. Таблица маршрутизации может быть построена двумя способами:

- *статическим*;
- *динамическим*.

Использование статической маршрутизации целесообразно в тех случаях, когда сеть имеет простую и стабильную архитектуру. Примером такой сети может быть локальная частная сеть небольшой организации, которая пользуется услугами только одного провайдера сети Интернет. Динамический способ является более предпочтительным для использования в сетях крупных

организаций, имеющих в своем составе множество региональных офисов и нескольких провайдеров. Использование динамической маршрутизации в данном случае позволяет учитывать изменения, происходящие в сети. Динамический способ реализуется при использовании алгоритмов маршрутизации. Современные алгоритмы маршрутизации обеспечивают не только быстрое переключение маршрута в обход неисправного участка, но и динамический анализ качества используемого канала передачи данных, а также перераспределение нагрузки между параллельными каналами и формирование маршрутных политик.

В мультисервисных сетях мощные протоколы маршрутизации целесообразно применять только на внешнем участке для сопряжения с открытой сетью Интернет. Внутри самой сети, как правило, вполне достаточно использования статической маршрутизации или простых динамических протоколов (например, OSPF).

Взаимодействие абонентов различных VLAN

Специфика современных ЛВС состоит в широком использовании логического сегментирования. Для образования логических сегментов в ЛВС используется аппарат виртуальных сетей — *VLAN* (Virtual Local Area Network). Поскольку абоненты различных виртуальных сетей находятся в изолированных канальных сегментах, между ними невозможно осуществить непосредственное информационное взаимодействие. Информационный обмен между такими сегментами возможен только на следующем уровне — сетевом, поэтому основное назначение маршрутизатора в современных ЛВС состоит в обеспечении взаимодействия абонентов различных VLAN.

Каждая виртуальная сеть представляется на маршрутизаторе в виде отдельного виртуального интерфейса, для которого могут быть выполнены практически все те же команды, которые используются для настройки обычного интерфейса (за исключением команд управления протоколами канального и физического уровня). Для управления трафиком на виртуальном интерфейсе VLAN также могут быть использованы специальные *списки доступа — VACL* (VLAN Access Control Lists). Эти списки доступа могут быть определены таким образом, чтобы обеспечить или предотвратить возможность информационного обмена между абонентами выделенных виртуальных сетей.

Вспомогательные функции маршрутизаторов

Наиболее востребованными в современных ЛВС являются функции различных посредников, которые возлагаются на маршрутизатор. В качестве примера можно привести функцию Proxy DHCP. Примечательно, что необходимость в такой функции также вызвана широким внедрением VLAN, огра-

ничивающих распространение широковещательных кадров, которые используются в протоколе DHCP для поиска сервера. Маршрутизатор, реализующий функцию Proxy DHCP, принимает соответствующие широковещательные запросы из выбранных сегментов (виртуальных сетей) и передает их в тот сегмент, где находится сервер. Подобная схема может быть использована и для других протоколов, для некоторых из них, впрочем, маршрутизатор может сам выполнять функцию сервера (например, для протокола ARP).

Под *трансляцией сетевых адресов* — *NAT* (Network Address Translation) обычно понимают определенный алгоритм преобразования сетевых адресов источника и назначения у проходящих через маршрутизатор пакетов. Основными задачами, для решения которых используется трансляция сетевых адресов, является экономия адресного пространства. Использование специального режима NAT позволяет, например, группе узлов внутренней сети осуществлять одновременный доступ в сеть Интернет через один открытый адрес.

Организация межсетевого экранирования выполняется по правилам, которые во многом напоминают правила NAT. Это сходство объясняется тем, что эти функции являются взаимодополняющими, поскольку в нормальной сети как доступ во внешние сети, так и защита от доступа извне должны выполняться по согласованным правилам. Это позволит, с одной стороны, избежать серьезных нарушений информационной безопасности, а с другой — предотвратить появление недостижимых зон во внешней сети.

Функции *обнаружения вторжений* (Intrusion Detection) и *сетевого мониторинга* наименее часто применяются на современных универсальных маршрутизаторах из-за того, что вызывают существенное увеличение нагрузки на центральный процессор маршрутизатора. Для реализации этих функций, также как и функции межсетевого экранирования в ЛВС, принято использовать специальные сетевые компоненты (Fire Wall, Intrusion Detection System).

Задачи и способы многоуровневой коммутации

Исторически сложилось так, что маршрутизаторы выполняли многие из наиболее важных функций ЛВС. Развитие информационных технологий привело к резкому повышению скоростей и объемов передаваемых данных в ЛВС. Кроме того, существенно изменилась и структура информационного обмена. Повсеместное использование интернет-технологий и VLAN-сегментирования привело к тому, что в современных ЛВС более 80% передаваемого и принимаемого трафика выходит за пределы канального сегмента и, следовательно, должно проходить обработку на сетевом уровне. Очевидно, что в современной ЛВС надежная реализация основных и дополнительных функций мар-

шрутизатора полностью определяет степень готовности ЛВС к передаче данных.

Также очевидно, что производительность центрального процессора маршрутизатора с программной реализацией функций при многократном повышении скорости и объемов обрабатываемых данных также должна быть многократно увеличена для обеспечения требуемой надежности и эффективности их обработки. Однако понятно, что такое решение приведет к резкому увеличению стоимости используемого оборудования и не кажется достаточно перспективным.

Гораздо более перспективным в этой ситуации выглядит использование аппаратной реализации основных функций маршрутизатора и перераспределение части этих функций между другими компонентами ЛВС.

Методы аппаратной реализации функций маршрутизатора

Суть аппаратной маршрутизации состоит в построении и использовании дополнительных таблиц, которые содержат ключевые значения полей обрабатываемых кадров Ethernet и содержащихся в них пакетов IP. В одном из таких полей, например, могут находиться адреса назначения IP. Аппаратный характер реализации позволяет в данном случае одновременно выполнять сравнение нескольких ключевых полей кадра с адаптированными таблицами шаблонов и, в зависимости от результатов этого сравнения, формировать решение по дальнейшей передаче принятого кадра.

Вместе с тем, применение аппаратной маршрутизации вовсе не означает полного отказа от использования программ, выполняемых на центральном процессоре. Дело в том, что использование протоколов динамической маршрутизации предполагает периодический обмен сообщениями, который может быть выполнен только при непосредственном участии центрального процессора. Кроме того, выполняемая на центральном процессоре программа-диспетчер может использоваться для периодического обслуживания адаптированных таблиц, например, для удаления из них просроченных записей.

Производители коммуникационного оборудования используют собственные фирменные методы аппаратной реализации функций маршрутизатора. Эти методы можно разделить на две основные группы:

- методы со статическими шаблонами потоков;
- методы с динамическими адаптированными таблицами.

Особенностью методов, принадлежащих к первой группе, является использование ресурсов центрального процессора для формирования адаптированных таблиц. При этом все данные, проходящие через маршрутизатор, разбиваются на виртуальные потоки. Каждый из потоков характеризуется уникальным

набором параметров сетевого и транспортного уровня, в который обычно входят:

- IP-адрес станции назначения;
- IP-адрес источника пакета;
- порт назначения протокола TCP или UDP;
- порт источника протокола TCP или UDP.

Поток описывает взаимодействие двух объектов с использованием одного протокола прикладного уровня. Очевидно, что при этом все пакеты, передаваемые через маршрутизатор, будут иметь одинаковые значения приведенных выше параметров и должны маршрутизироваться по одинаковым правилам. Поэтому стандартная процедура маршрутизации с использованием центрального процессора выполняется только для первого пакета потока, который и образует статический шаблон. При совпадении контролируемых параметров входящего пакета со значениями шаблона, он передается через маршрутизатор таким же образом, что и все его предшественники. В целях экономии используемых ресурсов время хранения каждого из шаблонов ограничено. В том случае если в течение выбранного интервала маршрутизатор не получит ни одного пакета из данного потока, то соответствующий шаблон подлежит уничтожению.

Примечание

Это означает, впрочем, только то, что первый из последующих пакетов того же потока снова должен будет пройти процедуру программной маршрутизации, для того чтобы вновь построить шаблон потока.

В отличие от метода, описанного немного ранее, метод аппаратной маршрутизации с динамическими адаптированными таблицами вообще не использует ресурс центрального процессора для построения своих таблиц. В данном случае динамические таблицы строятся непосредственно по таблице маршрутизации. В динамические адаптированные таблицы при этом могут быть внесены диапазонные значения. Например, для обозначения диапазона адресов 21.16.17.0/24 = 21.16.17.1-21.16.17.255 может быть использована примерно такая запись — 21.16.17.X, где X — означает любое значение в интервале от 0 до 255. Таким образом, для всех пакетов с адресами из этого диапазона процедура сравнения с шаблоном будет давать одинаковый результат, что приведет к выполнению для них одного правила маршрутизации. Поскольку при появлении новой записи в таблице маршрутизации соответствующая запись автоматически добавляется в адаптированную таблицу, непосредственного взаимодействия процессов аппаратной и программной маршрутизации в данном случае не происходит.

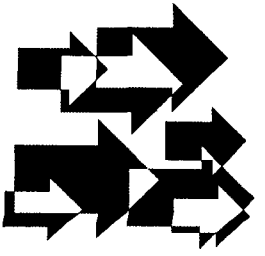
Базовые принципы многоуровневой коммутации

Методы со статическими шаблонами потоков, описанные в предыдущем разделе, могут быть использованы для ускорения выполнения основных процедур на обычном программном маршрутизаторе. Применение этого метода, безусловно, позволит существенно снизить нагрузку на его центральный процессор и существенно увеличить среднюю скорость обработки пакетов. Однако эффективность применения этого метода очень сильно зависит от структуры передаваемых через маршрутизатор потоков данных.

В то же время методы аппаратной маршрутизации с динамическими адаптированными таблицами являются достаточно универсальными и не требовательными к ресурсам, что позволяет успешно применять их на современных коммутаторах. Путем незначительной модификации адаптированных таблиц можно добиться включения в процедуру сравнения и параметров протоколов транспортного и последующих уровней, что позволит достаточно просто реализовать и аппаратную обработку списков управления доступом (Access Control List).

Все это означает возможность одновременной обработки на коммутаторе данных нескольких уровней OSI ISO 7498 — то, что принято сегодня называть *многоуровневой коммутацией*.

ГЛАВА 7



Обеспечение безопасного подключения абонентов

Обеспечение безопасности информационного взаимодействия является одной из наиболее важных задач при построении мультисервисных вычислительных сетей. С одной стороны, это объясняется экономическими соображениями, например, необходимостью ограничить или предотвратить несанкционированный доступ к платным сетевым ресурсам. С другой стороны, ресурсы мультисервисной сети могут быть использованы злоумышленником для перехвата или фальсификации передаваемых по ней данных. Таким образом, безопасное подключение абонентов предполагает наличие двусторонней защиты:

- защиты сетевых ресурсов от несанкционированного доступа абонента;
- защиты ресурсов абонента от сетевой атаки.

Наиболее простой и понятный способ обеспечения защиты сетевых ресурсов от несанкционированного доступа заключается в разделении вычислительной сети на виртуальные сети, предназначенные для передачи различных видов мультисервисного трафика. Позже мы увидим, что помимо повышения информационной безопасности такое решение обеспечивает возможность реализации требуемого качества предоставляемой услуги.

В первом разделе данной главы приведено описание принципов построения разнообразных виртуальных сетей.

Во втором разделе рассматриваются различные методы установления подлинности (аутентификации) абонентов, а также приемы управления доступом к сетевым ресурсам.

В разделах главы приведены рекомендации по обеспечению безопасности информационного взаимодействия в мультисервисных сетях различных конфигураций.

Виртуальные сети

Своим появлением и последующим широким распространением *виртуальные локальные сети — VLAN* (Virtual Local Area Network) обязаны внедрению в локальные сети многопортовых прозрачных мостов-коммутаторов.

Ранее было показано, что если сегменты локальной сети объединяются при помощи устройств типа "мост", коллизионный домен разделяется на столько частей, сколько портов имеет данный мост. В этом случае пропускная способность сети существенно увеличивается, поскольку N-станций (число портов моста) могут одновременно участвовать в информационном обмене. Следует также отметить, что пропускная способность в данном случае увеличивается за счет того, что мост, в отличие от репитера, реализует функцию фильтрации — трафик занимает только те сегменты локальной сети, в которые он непосредственно адресован. Применение мостов, таким образом, позволяет сегментировать ЛВС в части передачи *одноадресного трафика* — Unicast-трафика ЛВС.

Однако существует тип трафика, который мост обрабатывает так же, как и репитер. Этот тип трафика называется *широковещательный* или Broadcast-трафик. Если на вход моста поступает кадр, адрес назначения которого принадлежит к типу BROADCAST, мост должен передать этот кадр через все свои порты. Таким образом, локальная сеть, независимо от того, построена она на мостах или репитерах, представляет собой единый широковещательный или Broadcast-домен. Если принять во внимание то, что некоторые приложения способны формировать довольно большой объем Broadcast-трафика, становится понятно, что с ростом числа пользователей этот фактор может оказать заметное влияние на уменьшение общей пропускной способности сети. Снижения этого влияния можно было бы добиться при помощи изоляции группы активных формирователей Broadcast-трафика от остальных абонентов ЛВС. В этом случае Broadcast-трафик распространяется только в пределах этой изолированной группы абонентов, которые и образуют виртуальную сеть. Взаимная изоляция абонентов таких виртуальных сетей выполняется на канальном уровне OSI (ISO 7498) и ограничивает распространение ненужного трафика по сети, что повышает эффективность ее использования. Кроме того, для обеспечения безопасности информационного взаимодействия разделение единой ЛВС на несколько независимых сетей также становится целесообразным.

Принципы построения виртуальных сетей

Разделение ЛВС на не связанные на канальном уровне сегменты может быть реализовано физическим и логическим способами. Физический способ разделения сетей предполагает, что абоненты, находящиеся в различных сегментах

ЛВС, используют независимые устройства для обеспечения информационного обмена. Очевидно, что такой способ сегментации обеспечивает разделение широковещательного домена, однако образованная по этому принципу ЛВС наверняка потребует больших вложений при построении. Кроме того, такую сеть будет не слишком удобно эксплуатировать и трудно развивать. В этом смысле гораздо более перспективным представляется логический способ разделения ЛВС, при использовании которого абоненты различных сегментов используют единое оборудование ЛВС, а разделение формируемого ими трафика обеспечивается путем модификации процедуры обработки кадров соединяющего их моста. Действительно, для разделения широковещательного домена совсем не обязательно использовать независимые устройства канального уровня. Для этого вполне достаточно определить критерий принадлежности абонентов к тому или другому сегменту с тем, чтобы обеспечить на данном устройстве разделение передаваемого трафика, например, путем создания независимых таблиц фильтрации. Каждой такой таблице будет соответствовать логическая сеть, информационный обмен в пределах которой может выполняться независимо от обменов, выполняемых в других логических сетях. Образованные при помощи этой или подобной операции логические сети принято называть *виртуальными*.

Определение

Виртуальной сетью (Virtual LAN, VLAN) называется образованная в пределах ЛВС логическая группа абонентов, взаимодействие между которыми на канальном уровне OSI выполняется независимо от абонентов основной ЛВС и других виртуальных сетей.

По способу установления принадлежности абонента к виртуальной сети различаются статические и динамические *VLAN*. Членство абонента в *статической виртуальной сети* определяется номером порта коммутатора (моста), к которому он подключен. Использование номера порта, к которому подключено данное устройство, в качестве критерия принадлежности к виртуальной сети является наиболее простым для реализации принципом организации VLAN. На рис. 7.1 представлен вариант организации статических виртуальных сетей. В данном случае абоненты, подключенные к портам 11—13, образуют VLAN10, абоненты, подключенные к портам 21—23, образуют VLAN20. Поскольку каждая из виртуальных сетей имеет собственный сервер, обе они функционируют совершенно независимо друг от друга.

Использование этого принципа при организации виртуальной сети имеет как свои преимущества, так и недостатки. Наибольшими достоинствами данного метода организации VLAN являются:

- простота администрирования;
- возможность обеспечения достаточно простой и эффективной физической защиты компонентов виртуальной сети.

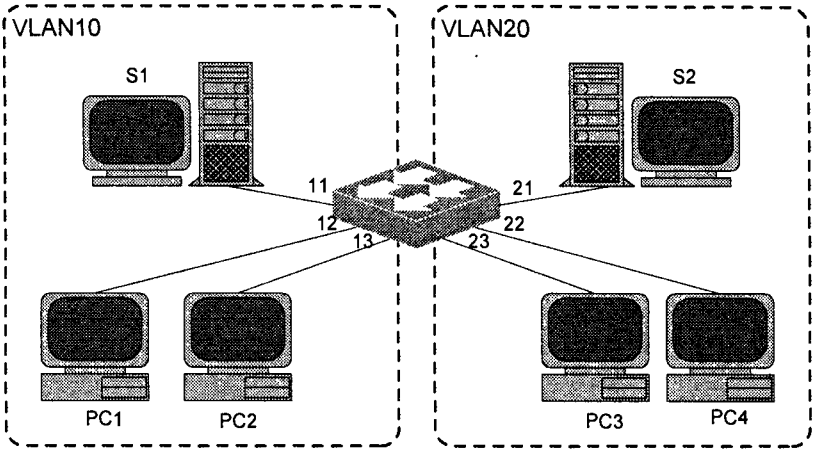


Рис. 7.1. Пример организации двух статических виртуальных сетей

Недостатком использования параметров физического подключения в качестве критерия для определения членства в виртуальной сети является отсутствие достаточной гибкости при управлении компонентами — в ряде случаев при изменении физического подключения может потребоваться изменение конфигурации виртуальной сети.

В некоторых случаях более целесообразным может оказаться использование *динамических VLAN*. Принадлежность абонента к таким виртуальным сетям определяется в процессе их функционирования, в качестве критерия при этом используется уникальный параметр, присущий абоненту, например, MAC-адрес. Поскольку MAC-адрес является глобально уникальным идентификатором, который однозначно связан с пользовательским компьютером, определение членства является в данном случае однозначным и обеспечивает достаточную гибкость. В табл. 7.1 приведен пример построения двух виртуальных сетей, членство в которых определяется по MAC-адресу.

Таблица 7.1. *Использование MAC-адреса для определения принадлежности абонента к VLAN*

MAC-адрес	Номер VLAN
00d0.b7a7.a000	1
0050.8bca.3623	1
0004.aca2.6ef7	2
0004.ac18.0e33	2
0060.08c4.7c17	1

В данном случае к виртуальной сети номер 2 принадлежат станции, которые имеют одинаковое значение Vendor Code = 0004.ac.

Примечание

Обычно для определения принадлежности к виртуальной сети используются все 48 бит MAC-адреса абонента.

Основным недостатком использования MAC-адреса в качестве критерия принадлежности к VLAN является трудоемкость администрирования, поскольку эти адреса являются длинными и трудно запоминаются. Кроме того, существуют группы пользователей, которые используют мобильные компьютеры с выносной NIC-картой, для которых установление членства в виртуальной сети по значению MAC-адреса может оказаться неоднозначным.

Преимущества использования VLAN в МСС

Главным преимуществом, которое обеспечивается при использовании виртуальных сетей, является не столько сама возможность ограничения Broadcast-трафика, сколько возможность создания изолированных групп пользователей в пределах локальной сети. Наиболее удобно, с точки зрения администратора сети, объединение пользователей по функционально производственному признаку.

Повышение производительности ЛВС

Увеличение производительности при использовании VLAN достигается за счет уменьшения доли Broadcast-трафика в пределах каждой виртуальной сети. Еще большего эффекта от использования виртуальных сетей можно добиться в том случае, если выделить в отдельную VLAN пользователей, которые формируют основной объем этого трафика. В обычных сетях соотношение объемов данных, передаваемых в одноадресном режиме (Unicast) и многоадресных режимах (Non-Unicast, Broadcast, Multicast), не должно быть менее 5. В мультисервисных сетях это значение может быть меньше вследствие увеличения объема данных передаваемых в режиме Multicast. Увеличение производительности при использовании виртуальных сетей обеспечивается из-за сокращения объема широковещательного трафика, подаваемого на серверное оборудование и станции пользователей рабочей группы.

Примечание

Определить реальные объемы данных, передаваемых в одноадресном режиме (Unicast) и многоадресных режимах (Non-Unicast, Broadcast, Multicast), для конкретной рабочей станции или сервера можно используя *утилиту NETSTAT* (MS WINDOWS) с ключом "– e".

Каждый абонент ЛВС должен анализировать содержимое поля полезной нагрузки всех кадров с адресом назначения FF-FF-FF-FF-FF-FF, которые поступают на Ethernet-порт сетевой карты. Следовательно, чем больше подобных кадров поступает на сетевую карту рабочей станции, тем меньше времени центральный процессор сможет уделить для выполнения на ней действительно полезных приложений. На рис. 7.2 приведен пример использования утилиты NETSTAT для определения объемов данных, передаваемых в различных режимах.

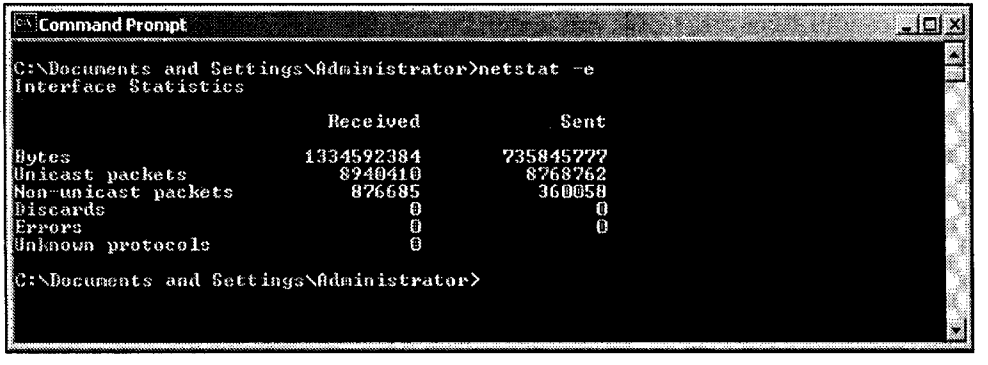


Рис. 7.2. Пример использования утилиты NETSTAT для определения объемов данных, передаваемых в различных режимах

Анализ данных, представленных на рис. 7.2, показывает, что соотношение объемов данных, передаваемых в одноадресном режиме (Unicast) и многоадресных режимах (Non-Unicast, Broadcast, Multicast), для представленной сети находится в пределах рекомендованного диапазона.

Создание виртуальных рабочих групп

Локальные сети в настоящее время объединяют в каждой организации разнообразные группы пользователей. Эти группы могут сильно отличаться друг от друга требованиями, которые предъявляются к параметрам информационного обмена. Члены этих групп могут быть в то же время территориально рассредоточены в пределах офиса, что делает невозможным их объединение при помощи чисто аппаратных средств. Использование механизма виртуальных сетей в данном случае представляется идеальным способом решения проблемы, поскольку VLAN обеспечивает возможность создания виртуальных рабочих групп по самым разнообразным признакам.

При построении мультисервисных сетей в качестве критерия формирования виртуальной группы пользователей целесообразно применять тип представляемой услуги. В отдельные виртуальные сети, например, могут быть выде-

лены абоненты, получающие услугу VoIP или пакетного телевидения. Такое решение позволит защитить указанных абонентов от широковещательного трафика, создаваемого при доступе обычных пользователей в сети Интернет, и обеспечит начальный уровень защиты от несанкционированного доступа к этим услугам.

Таким образом, больший уровень безопасности при использовании виртуальных сетей обеспечивается за счет того, что трафик различных групп не пересекается. Разделение различных групп пользователей в данном случае осуществляется на канальном уровне. Следовательно, для того чтобы нарушить установленные правила информационного обмена, преднамеренному или непреднамеренному нарушителю нужно будет приложить в данном случае значительно больше средств и усилий.

Снижение затрат на эксплуатацию

С точки зрения администратора использование VLAN является чрезвычайно удобным, поскольку при создании и реорганизации виртуальных сетей не требуется изменений в схемах подключения аппаратуры. Все изменения производятся программным путем, и, кроме того, некоторые из этих изменений могут быть выполнены автоматически.

Логическое разделение ЛВС на виртуалвные подсети упрощает администрирование сети, поскольку обеспечивает возможность независимого управления трафиком различных групп абонентов. Это, в свою очередь, делает возможным реализацию разнообразных политик распределения ресурсов ЛВС между ними, что в конечном счете может привести к повышению доходов.

Физическое разделение ЛВС на независимые сети, разумеется, обеспечивает максимально возможный уровень информационной безопасности, однако при построении мультисервисных сетей применение такого метода вряд ли можно считать оправданным, поскольку в этом случае резко увеличиваются затраты на построение ЛВС и ее эксплуатацию.

Использование виртуальных сетей для разделения Broadcast-домена обеспечивает снижение затрат на эксплуатацию и повышение эффективности использования пропускной способности сети, а поскольку это не требует приобретения дополнительного оборудования, следовательно, достигается значительная экономия средств.

Распределенные виртуальные сети

Как было показано ранее, построение виртуальной сети позволяет успешно решить ряд задач, стоящих перед создателем ЛВС. Однако применение VLAN может привести к появлению новых проблем. Дело в том, что в совре-

менных сетях лишь относительно небольшая доля сетевого трафика (до 20%) замыкается внутри локального сегмента. Подавляющая часть трафика, как правило, выходит за пределы сегмента (обмен с общим сервером, сетью Интернет и т. д.). Кроме того, при создании больших виртуальных сетей появляется необходимость использования более одного коммутатора для подключения компонентов этой сети. В этом случае компоненты одной виртуальной сети оказываются физически подключенными к различным коммутаторам, вследствие чего возникает необходимость обмена информацией о принадлежности абонентов к VLAN между коммутаторами. На рис. 7.3 приведен пример ЛВС, в которой организованы две распределенные виртуальные сети — VLAN10 и VLAN20.

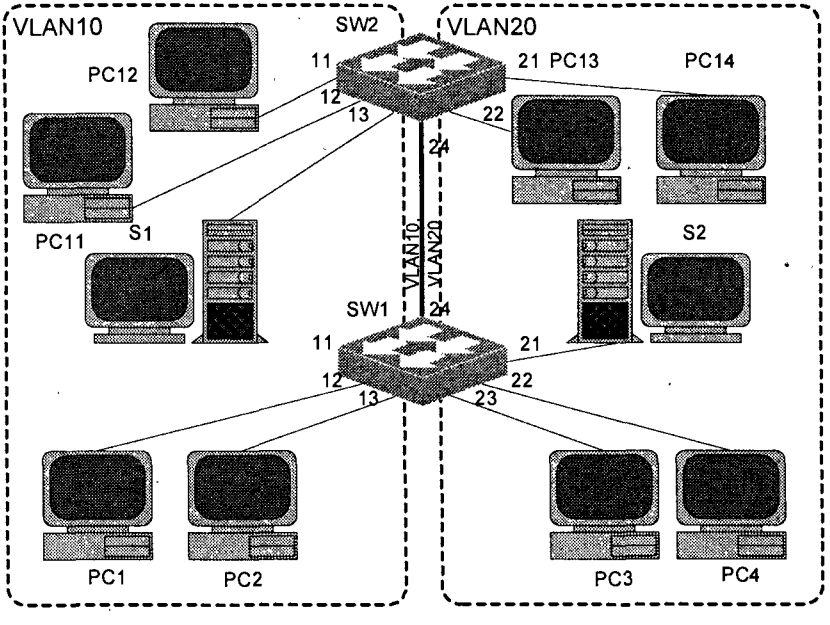


Рис. 7.3. Пример организации распределенных виртуальных сетей

Поскольку абоненты этих VLAN равномерно распределены между коммутаторами SW1 и SW2, эти коммутаторы должны обмениваться информацией о принадлежности кадра передаваемого через порт 24 к VLAN10 или VLAN20. Для обеспечения такого обмена принято использовать специальные метки, вставляемые в кадры, которые передаются между коммутаторами (frame tagging). Наличие этих меток обеспечивает возможность разделения совокупного трафика на потоки, которые относятся к различным виртуальным сетям.

В зависимости от того, где в кадре размещается метка, различаются два способа маркирования кадра:

- внешнее маркирование (Технология маркирования ISL);
- внутреннее маркирование (Технология IEEE 802.1Q).

Технология маркирования ISL

При использовании внешнего метода маркирования помечаемый кадр помещается внутрь другого кадра, который предназначен для переноса данного кадра через сеть коммутаторов и содержит в себе всю необходимую для этого информацию, в том числе и метку VLAN. Достоинствами данного метода являются сохранение исходного вида передаваемого кадра и возможность передавать в одном канале трафик разнородных сетей (Ethernet, Token Ring, FDDI). Метод внешнего маркирования для организации многокомпонентных вычислительных сетей был предложен компанией Cisco под наименованием — *ISL* (Inter Switch Link). Очевидным недостатком метода внешнего маркирования кадра является повышение накладных расходов. Так, например, при передаче с помощью этой технологии кадра длиной 64 байта, его длина увеличится практически на 50%.

При использовании этой технологии стандартный кадр канального уровня помещается внутрь специального транспортного кадра ISL, который состоял из заголовка ISL, инкапсулированного кадра и проверочной контрольной суммы.

Структура кадра ISL приведена в табл. 7.2.

Таблица 7.2. *Структура кадра ISL*

Номер поля	Наименование и содержание поля	Длина поля (байт)
1	ISL HEADER — заголовок кадра ISL	26
2	USER FRAME — инкапсулируемый кадр	1—24500
3	FCS — контрольная сумма кадра ISL	4

Заголовок ISL имел примерно такую же структуру, как и заголовок обычного кадра. В нем, в частности, размещался адрес станции назначения и адрес источника. В качестве адреса станции назначения в данном случае используется значение 01-0c-00-00-00, которое дополнялось байтом, содержащим признак данного кадра и идентификатор пользователя. В заголовке ISL размещался также идентификатор виртуальной сети (10 бит).

Появление технологии ISL (Inter Switch Link) у компании Cisco Systems позволило успешно решить как минимум три задачи:

- обеспечение маркирования кадра меткой номера виртуальной сети без изменения его первоначальной структуры;
- обеспечение возможности объединения сетей, построенных с использованием различных технологий (FDDI, Token Ring);
- обеспечение возможности построения независимых активных топологий для каждой из виртуальных сетей.

До последнего времени технология ISL активно использовалась на оборудовании компании Cisco Systems, однако в настоящее время, в связи с появлением и повсеместным внедрением спецификаций IEEE 802.1Q и, впоследствии, IEEE 802.1S (MSTP), она имеет ограниченное применение.

Технология IEEE 802.1Q

Гораздо большее распространение имеет в настоящее время технология, которая для явного указания членства VLAN предполагает размещение дополнительного поля внутри кадра. При использовании метода внутреннего маркирования метка помещается непосредственно в тело передаваемого по сети кадра. Именно такой способ маркирования кадров положен в основу спецификации IEEE 802.1Q, которая имеет название *"Virtual Bridged Local Area Networks"*. Достоинством данного метода является компактность формируемого кадра — его первоначальная длина увеличивается только на 4 байта. Однако использование данного метода приводит к тому, что в сети могут появиться кадры большей длины, чем это было предусмотрено в первоначальном варианте спецификации IEEE 802.3 — 1518 байт.

В таблице приведена структура кадра IEEE 802.3 с добавленным полем TAG. Размер максимального кадра в данном случае увеличивается со значения 1518 до 1522 байтов. Следствием этого изменения может быть неверное функционирование мостов, не поддерживающих взаимодействие по спецификации IEEE 802.1Q, которые эти кадры будут считать ошибочными и уничтожать. Таким образом, использование технологии не обеспечивает совместимость по принципу "снизу вверх". Комитетом IEEE 802.3 была подготовлена дополнительная спецификация IEEE 802.3ac, которая узаконила увеличение максимального размера кадра. Другим способом решения данной проблемы является уменьшение максимального размера поля полезной нагрузки при формировании кадра.

В табл. 7.3 приведена структура кадра Ethernet IEEE 802.1Q.

Метка кадра состоит из двух частей:

- поля TPID — идентификатора протокола;
- поля TCI — управляющей информации метки.

Таблица 7.3. Структура кадра Ethernet IEEE 802.1Q

Номер поля	Наименование и содержание поля	Значение	Длина поля (байт)
1	DESTINATION ADDRESS — адрес назначения кадра	01-80-c2-00-00-00	6
2	SOURCE ADDRESS — адрес источника кадра		6
3	TAG — метка кадра	81-00-XX-XX	4
4	TYPE LENGTH — тип или длина полезной нагрузки кадра		2
5	LLC PDU — полезная нагрузка кадра		46—1500
6	FCS — контрольная сумма		4

Поле TPID предназначено для того, чтобы указать на принадлежность данного кадра к числу тегированных (помеченных меткой) кадров IEEE 802.1Q. Размер этого поля отличается в зависимости от того, какой формат (Ethernet или SNAP) имел исходный файл. В первом случае поле TPID имеет длину 2 байта и включает в себя только указатель метки протокола 802.1Q (802.1QTagType "81-00"). В кадре SNAP поле TPID имеет длину 8 байтов и включает в себя следующие поля:

- стандартный заголовок SNAP AA-AA-03;
- идентификатор протокола SNAP 00-00-00;
- указатель метки протокола 802.1Q (802.1QTagType "81-00").

Поле TCI предназначается для того, чтобы разместить не только данные, определяющие принадлежность данного кадра к той или иной VLAN, но и для того, чтобы указать приоритет данного кадра по отношению к другим. Структура поля TCI приведена в табл. 7.4.

Таблица 7.4. Структура поля TCI

Номер поля	Наименование и содержание поля	Длина поля (бит)
1	PRIORITY — относительный приоритет кадра	3
2	CFI — признак канонического формата MAC-адресов в полезной нагрузке кадра	1
3	VID — идентификатор виртуальной сети	12

В поле PRIORITY (приоритет) размещается три бита, которые определяют относительный приоритет данного кадра. Максимальному приоритету соот-

ветствует значение 7, т. е. когда в этом поле содержатся все единицы. В данном случае используется тот же принцип управления трафиком, какой применяется в сетях FDDI и Token Ring, только число уровней приоритета существенно больше. Для каждого порта создаются очереди, в которые помещаются кадры, имеющие одинаковый уровень приоритета. В первую очередь обслуживаются очереди кадров с более высоким уровнем приоритета. Кадры меньшего приоритета обычно поступают на обработку в том случае, если все очереди для кадров большего приоритета пусты.

В поле CFI (Canonical Format Identifier — признак канонического формата) размещается признак, который интерпретируется в зависимости от того, какой формат (Ethernet, SNAP или FDDI) имел исходный кадр. Ноль в данном поле для кадров Ethernet или SNAP указывает на то, что коды MAC-адресов, которые могут быть размещены в поле полезной нагрузки, представлены в классическом (каноническом) формате.

В поле VID (VLAN Identifier) размещается идентификатор, определяющий принадлежность данного кадра к одной из 4095 возможных виртуальных сетей.

Значение VID = 0 не используется для обозначения номера виртуальной сети и указывает на то, что данный кадр принадлежит к группе кадров priority-tagged. Значение VID = FFF также не используется для обозначения номера виртуальной сети и зарезервировано для возможного применения в будущем.

Типы портов VLAN

В зависимости от предписанного способа обработки маркированных и немаркированных кадров порты коммутатора (моста) делятся на две категории:

- *маркирующие порты* — Tagged Ports;
- *демаркирующие порты* — Untagged Ports.

Демаркирующие порты используются для подключения оконечных абонентов к активному оборудованию ЛВС. Каждому из таких портов соответствует значение идентификатора PVID (Port VLAN ID — идентификатор VLAN порта). Все кадры, поступающие на порт этого типа от абонента, снабжаются меткой соответствующей VLAN и в дальнейшем обрабатываются так же, как и другие маркированные данной меткой кадры. Несколько портов коммутатора могут иметь одинаковое значение PVID, подключенные к ним оконечные абоненты становятся членами одной VLAN. В том случае, если из соответствующей виртуальной сети поступает кадр, который нужно передать подключенному абоненту, метка VLAN из кадра извлекается, а значение FCS — пересчитывается. Таким образом, демаркирующие порты применяются для обработки трафика только одной VLAN, номер которой совпадает со значением PVID, определенным для данного порта.

Примечание

Порт прозрачного моста может исполнять функцию Untagged только для одной VLAN. Обычно, по умолчанию, все порты коммутатора устанавливаются Untagged со значением PVID = 1 (Default VNAN).

Маркирующие порты используются для организации магистральных соединений между коммутаторами и могут передавать и принимать трафик нескольких виртуальных сетей одновременно. Порт этого типа обрабатывает маркированные кадры, не подвергая их при этом никаким дополнительным изменениям. Только в том случае, если идентификатор VLAN у кадра находится в списке виртуальных сетей, для которых порт коммутатора выполняет функцию Tagged, этот кадр будет передан через данный порт.

Ранее уже было отмечено, что маркирующие порты, как правило, используются для организации соединений между коммутаторами. Взаимодействие с ЛВС конечного пользователя, подключенного к такому порту, невозможно, поскольку абонент ЛВС не сможет обработать маркированные IEEE 802.1Q кадры, которые будет принимать от коммутатора. Однако в некоторых случаях, например для настройки и контроля функционирования коммутатора, это взаимодействие бывает необходимо обеспечить. Такой режим можно организовать, если определить для порта, выполняющего функцию Tagged, номер VLAN-U, для которой он будет выполнять функцию Untagged. Таким образом, кадры этой виртуальной сети будут обрабатываться этими портами без меток IEEE 802.1Q.

Примечание

У коммутаторов Catalyst компании Cisco Systems виртуальная сеть VLAN1 по умолчанию считается "местной" (Native) и обладает вышеописанными свойствами. Администратор, впрочем, может при желании определить в качестве "местной" любую другую виртуальную сеть. Следует, однако, отметить, что необходимо избегать соединения коммутаторов с различными значениями местных VLAN, поскольку в этом случае трафик, как минимум, двух VLAN будет потерян.

Туннели IEEE 802.1Q

При организации распределенных сетей передачи данных может появиться необходимость в передаче трафика нескольких независимых VLAN через активное оборудование сторонних организаций. Такая потребность может появиться при объединении через сеть Ethernet — провайдера ЛВС нескольких филиалов независимых организаций, в каждой из которых, в свою очередь, используются виртуальные сети для разделения трафика административных подразделений. Для обеспечения подобных требований может быть использован IEEE 802.1Q-туннель, соединяющий коммутаторы провайдера, через

который будут передаваться кадры, помеченные двумя метками — меткой организации и меткой подразделения. Метка организации при этом помещается на том порту активного оборудования, к которому подключен соответствующий филиал, в кадр уже помеченный меткой подразделения данной организации. Туннельный порт коммутатора провайдера при этом выполняет функцию Untagged по отношению к внешней метке. Для обеспечения корректного функционирования системы передачи данных при этом следует исключить возможность смешивания непомеченных кадров, которые могут поступать на туннельный порт коммутатора от клиентской организации и получают при этом одиночную метку, и кадров аналогичной VLAN, определенной на коммутаторе. Кроме того, следует учитывать, что общая длина передаваемого через туннель кадра увеличится еще, как минимум, на 4 байта.

Управление виртуальными сетями

Большинство современных виртуальных сетей имеют статическую архитектуру.

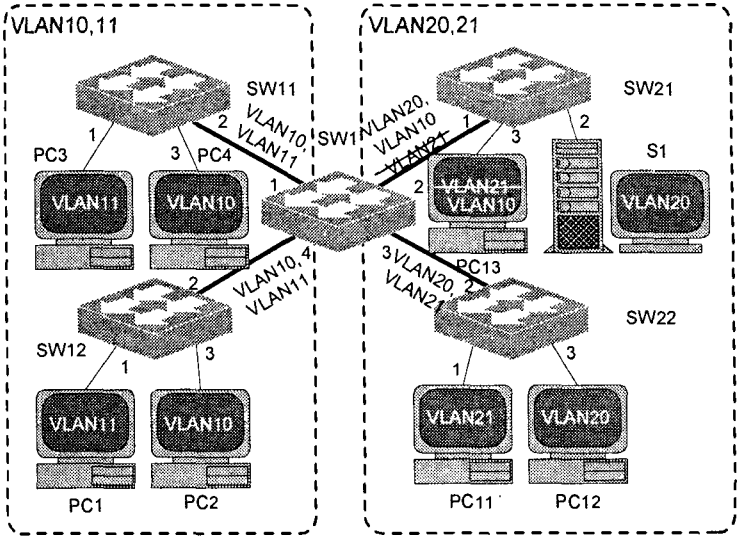
Архитектура VLAN в таких сетях определяется конфигурацией той области активной топологии сети, в которой размещаются участники (абоненты) данной VLAN.

Эта архитектура, как правило, создается и поддерживается системным администратором, который определяет и переопределяет принадлежность порта коммутатора к той или другой виртуальной сети. При появлении нового абонента имеющейся VLAN или при создании новой виртуальной сети существующая архитектура одной или всех имеющихся VLAN должна подвергаться изменениям. В некоторых случаях при этом нужно будет выполнить изменение настроек всех коммутаторов сети. Очевидно, что с увеличением количества VLAN и по мере роста самой ЛВС задача администрирования VLAN будет все более и более усложняться. На рис. 7.4 приведен пример ЛВС с четырьмя виртуальными сетями. В том случае, если PC13, подключенный к коммутатору SW21, потребуется перевести в VLAN10, кроме перенастройки порта доступа на SW21, нужно будет изменять настройки магистральных портов коммутаторов SW1 и SW21. (В данном случае следует добавить функцию Tagged для VLAN10 на обоих портах, связывающих эти коммутаторы.) В таблице на рис. 7.4 более темным выделены номера портов коммутатора, для которых необходимо произвести ручное изменение настроек VLAN.

Сократить объем выполняемых при изменении конфигурации VLAN работ можно, если автоматически разрешить прохождение через магистральные (маркирующие) порты коммутаторов трафика всех активных виртуальных сетей. В этом случае для выполнения описанного ранее изменения конфигурации сети достаточно будет просто изменить настройки порта доступа на

коммутаторе SW21. На первый взгляд такое решение кажется обоснованным, целесообразным и, главное, — простым для реализации. Действительно, нет ничего плохого в том, чтобы разрешить прохождение на прозрачный мост (коммутатор) трафика тех виртуальных сетей, абоненты которых к нему не подключены. Учитывая, что поступать на коммутатор может только трафик, прошедший фильтрацию по адресу назначения на порту отправителя, можно предположить, что этого трафика не будет совсем. Однако, в действительности, существуют, как минимум, три разновидности адресов назначения и соответствующие категории трафика, которые будут свободно распространяться по ЛВС:

- широковещательный (Broadcast);
- групповой (Multicast);
- неизвестный одноадресный (Unknown Unicast).



Комм/порт	VLAN			
	10	11	20	21
SW11/1		U		
SW11/2	T	T		
SW11/3	U			
SW12/1		U		
SW12/2	T	T		
SW12/3	U			
SW21/1			T	T
SW21/2			U	
SW21/3				U
SW22/1				U
SW22/2			T	T
SW22/3			U	
SW1/1	T	T		
SW1/2			T	T
SW1/3			T	T
SW1/4	T	T		

Рис. 7.4. Пример изменения конфигурации VLAN

Можно ожидать, что в мультисервисных сетях уровень группового и широковещательного трафика будет достаточно высоким и, следовательно, общая загрузка сети существенно возрастет, поскольку через каждое из магистральных соединений теперь будет передаваться совокупный трафик всех указанных ранее категорий для всех VLAN сети. Помимо загрузки магистральных каналов, этот трафик может вызвать повышенную нагрузку на центральные процессоры принимающих его коммутаторов, которые будут вынуждены его обрабатывать.

Учитывая приведенные ранее соображения, оптимальным кажется решение, которое обеспечивает автоматическое изменение конфигурации коммутаторов при изменении — добавлении новых или удалении старых — абонентов виртуальных сетей. Такой способ реализации подобного решения представляет использование протокола *GVRP* (Generic VLAN Registration Protocol), который в свою очередь является частным случаем универсального протокола *GARP* (Generic Attribute Registration Protocol) или собственного протокола *VTP* (VLAN Trunk Protocol) компании Cisco Systems.

Протокол GARP

Протокол GARP (Generic Attribute Registration Protocol) определен в IEEE 802.1D и содержит совокупность процедур, которые могут быть использованы для формирования и распространения по сетям прозрачных мостов дополнительных параметров (атрибутов), определяющих особенности информационного обмена в этой сети. Протокол GARP является полностью симметричным и позволяет каждому из участников декларировать или дезавуировать значение некоторого атрибута. Для того чтобы поддерживать информационный обмен по протоколу GARP, каждый из участников (GARP participant) должен иметь следующие компоненты:

- *компонент-приложение* — GARP application component;
- *компонент-заявитель* — GARP declaration component.

Компонент-приложение является центральным и предназначен для выполнения участником GARP комплекса действий, соответствующих текущему состоянию системы (изменение внутренних настроек устройства, передача сообщений и т. д.).

Назначение заявителя состоит в том, чтобы поддерживать связь с другими участниками протокола, принимая от них сообщения протокола GARP. Кроме того, при необходимости, заявитель формирует собственные сообщения этого протокола, обеспечивая, таким образом, установку требуемых значений необходимых ему параметров. В том случае, если участником протокола GARP является многопортовый мост — коммутатор, каждому из его портов ставятся в соответствие отдельные независимые компоненты — приложение и заявитель. В дополнение к этому многопортовый мост должен содержать специальный компонент протокола — *распространитель* — GARP propagation component. Задачей этого компонента является обеспечение информационного обмена между участниками протокола GARP, размещенными в том же мосту, что и данный участник.

Примечание

Для портов, которые используются для подключения оконечных пользователей, наличие компонента GIP не требуется.

Особенностью протокола GARP является его симметричность: каждый из участников имеет одинаковые с остальными права, все участники, число которых не ограничено, действуют по одним правилам. Следует отметить, что в современных ЛВС, которые практически не используют разделяемые среды для передачи данных, невозможно наличие более двух участников GARP. Более того, в подавляющем большинстве случаев одним из участников наверняка будет порт коммутатора.

В настоящее время известно два варианта практической реализации протокола GARP — протоколы GVRP (Generic VLAN Registration Protocol) и GMRP(GARP Multicast Registration Protocol).

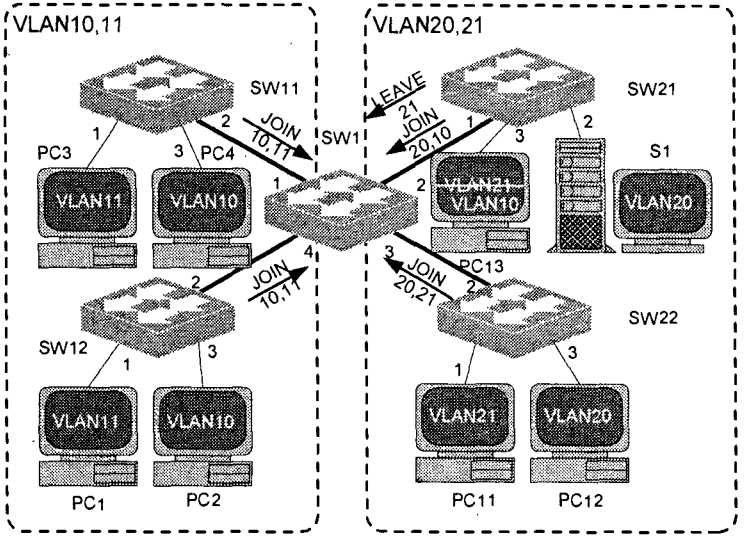
Динамические VLAN. Протокол GVRP

Протокол GVRP (Generic VLAN Registration Protocol), как уже было отмечено ранее, является частным приложением протокола GARP и предназначен для автоматического создания и обслуживания таблицы активных виртуальных сетей, что позволяет обеспечить передачу только необходимого трафика через каждый из сегментов ЛВС. Участниками протокола GVRP являются многопортовые мосты (коммутаторы ЛВС) и оконечные рабочие станции, имеющие специальное программное обеспечение для обработки и создания помеченных кадров IEEE 802.3/Ethernet.

При выполнении протокола GVRP прозрачный мост передает в подключенный сегмент ЛВС декларации, в которых указывает идентификаторы тех виртуальных сетей, трафик которых он желает принимать. Также мост принимает и обрабатывает GVRP-декларации других мостов, подключенных к данному сегменту, с тем, чтобы избежать повторного декларирования одной VLAN или отказаться от приема в сегмент трафика некоторой виртуальной сети, для которой в нем не осталось приемников. В дополнение к описанным ранее функциям мост, который участвует в выполнении протокола GVRP, должен обеспечить распространение информации о потребности в трафике виртуальных сетей между своими портами и другими мостами, образующими активную топологию данной ЛВС.

Для выполнения этих функций все участники протокола GVRP обмениваются сообщениями из стандартного набора GARP (`Join`, `Leave`, `Leave All`), передаваемыми через ЛВС в виде кадров IEEE 802.3/Ethernet с адресом назначения 01-80-C2-00-00-21. В поле полезной нагрузки такого кадра помещается PDU протокола GVRP, структура которого соответствует рекомендованной IEEE 802.1D для протокола GARP. Поскольку в протоколе GVRP используется только один тип атрибута — идентификатор VLAN, то единственным используемым значением соответствующего поля PDU является 1. Для кодирования идентификатора декларируемой VLAN в данном случае используется

поле значения атрибута (два байта). На рис. 7.5 приведен пример автоматического изменения конфигурации ЛВС при использовании протокола GVRP.



Комм/порт	VLAN			
	10	11	20	21
SW11/1		U		
SW11/2	D	D		
SW11/3	U			
SW12/1		U		
SW12/2	D	D		
SW12/3	U			
SW21/1	D		D	
SW21/2			U	
SW21/3	U			
SW22/1				U
SW22/2			D	D
SW22/3			U	
SW1/1	D	D		
SW1/2	D		D	
SW1/3			D	D
SW1/4	D	D		

Рис. 7.5. Пример автоматического изменения конфигурации ЛВС с использованием динамических VLAN

Предполагается, что все прозрачные мосты — коммутаторы в ЛВС, схема которой приведена на рис. 7.5, поддерживают протокол GVRP. В этом случае на магистральных портах этих коммутаторов автоматически будут сконфигурированы только необходимые динамические VLAN (в таблице на рисунке они помечены буквой "D"), поскольку сообщение JOIN по протоколу GVRP формируется только для активных виртуальных сетей. В том случае если на коммутаторе изменяется номенклатура активных VLAN, то он формирует сообщения JOIN и LEAVE в соответствии с произведенными изменениями. На примере, приведенном на рис. 7.5, коммутатор SW21 при изменении конфигурации VLAN на порту № 3 автоматически формирует сообщения GVRP LEAVE VLAN21 и GVRP JOIN VLAN10. Получив эти сообщения, коммутатор SW1 также автоматически меняет настройки динамических VLAN на своем порту № 2.

Применение протокола GVRP, таким образом, обеспечивает согласованное и автоматическое изменение настроек всех прозрачных мостов (коммутаторов) ЛВС при изменении конфигурации VLAN на одном из них, что существенно облегчает их администрирование. Однако при использовании этого протокола следует учитывать некоторые важные особенности его практической реализации. Дело в том, что конфигурация динамических виртуальных сетей,

сформированных протоколом GVRP, обычно не сохраняется автоматически в энергонезависимом запоминающем устройстве коммутатора. Вследствие этого, после рестарта на коммутаторе SW1, работоспособность ЛВС, схема которой приведена на рис. 7.5, будет полностью нарушена. Кроме того, использование протокола GVRP может привести к снижению уровня информационной безопасности ЛВС. Очевидно, что в этом случае конфигурация виртуальных сетей ЛВС может быть изменена в любой момент времени без участия администратора. Следует также учитывать, что этот протокол не имеет встроенных процедур установления подлинности (аутентификации) источника сообщения об изменении конфигурации VLAN, вследствие чего злоумышленник, использующий протокол GVRP, легко может получить доступ к защищаемой части ЛВС.

Протокол VTP Cisco Systems

На коммутаторах Catalyst Cisco Systems для динамического управления виртуальными сетями может быть использован протокол *VTP* (VLAN Trunk Protocol). Этот протокол обеспечивает тот же набор функций управления VLAN, что и описанный ранее протокол GVRP, однако использует другой принцип их реализации. Основными отличиями протокола VTP по отношению к GVRP являются следующие:

- участники могут быть не равноправны по отношению к выполняемым функциям администрирования VLAN;
- протокол VTP обеспечивает возможность построения административных доменов;
- в протоколе VTP предусмотрена возможность аутентификации отправителя и шифрования содержимого передаваемых сообщений.

Сообщения протокола VTP передаются только через маркирующие порты коммутаторов в виде PDU-инкапсулированных в поле полезной нагрузки кадров IEEE 802.3/Ethernet. В качестве адреса назначения для таких кадров используется кодировка 01-00-0C-CC-CC-CC. В том случае, если PDU инкапсулируется в кадр IEEE 802.3, поле SNAP (Subnetwork Access Protocol) устанавливается значением "AAAA", а поле "type" (SNAP header) — значением "2003".

Как уже было отмечено, одной из главных особенностей протокола VTP является централизация управления и ограничение области администрирования VLAN.

Определение

Доменом VTP называется область ЛВС, объединяющая в себя группу прозрачных мостов (коммутаторов), имеющих согласованную конфигурацию VLAN и находящихся под единым управлением.

Для идентификации VTP-домена используется уникальное имя (VTP Domain Name), которое должно быть одинаковым для всех коммутаторов данного домена. Обязательными условиями при построении VTP-домена являются следующие:

- каждый коммутатор может принадлежать только одному VTP-домену;
- коммутаторы домена должны быть непосредственно связаны;
- между коммутаторами домена должно быть установлено соединение с использованием протокола ISL или IEEE 802.1Q.

Каждый коммутатор, входящий в VTP-домен, создает и обслуживает индивидуальную копию базы данных виртуальных сетей (VTP Data Base). В построении базы данных могут принимать участие только те коммутаторы, которые входят в VTP-домен. Каждой из последовательных версий этой базы данных соответствует увеличивающееся на единицу значение идентификатора версии базы данных VLAN — Configuration Revision Number. Таким образом, более новым версиям базы соответствуют большие значения идентификатора.

В табл. 7.5 приведены некоторые из атрибутов виртуальных сетей, которые содержатся в базе данных VTP (VTP Data Base).

***Таблица 7.5.** Атрибуты виртуальных сетей в базе данных VTP*

Имя атрибута	Назначение атрибута
Vlan-ID	Идентификатор (номер) виртуальной сети
Vlan-Status	Состояние виртуальной сети
Vlan-Type	Тип виртуальной сети (IEEE 802.3/802.5)
Vlan-Name	VID — идентификатор виртуальной сети
MTU-Size	Максимальный размер передаваемого блока данных

Для того чтобы поддерживать актуальное состояние базы данных виртуальных сетей домена, коммутаторы используют следующие сообщения протокола VTP:

- *"Общее объявление"* (Summary advertisements);
- *"Частичное объявление"* (Subset advertisement);
- *"Запрос объявления"* (Advertisement requests).

Сообщение "Общее объявление" формируется периодически и содержит обобщенную информацию о текущем состоянии базы данных на том коммутаторе, который сформировал данное сообщение. В том случае, если конфи-

гурация базы данных на коммутаторе изменилась со времени передачи последнего общего объявления, в дополнение к общему объявлению он передает частичные объявления для всех виртуальных сетей, конфигурации которых изменились. Сообщение "Частичное объявление" содержит полную информацию о конфигурации одной VLAN. Сообщение "Запрос объявления" используется в том случае, если на коммутаторе отсутствует информация о какой-либо из виртуальных сетей. Это сообщение содержит идентификаторы тех VLAN, полную информацию о которых желает получить отправивший его прозрачный мост (коммутатор).

В зависимости от своего положения в локальной сети, коммутатор может выполнять одну из следующих функций протокола VTP:

- VTP-сервер;
- VTP-клиент;
- VTP-прозрачный агент.

Коммутаторы, выполняющие роли VTP-сервер и VTP-клиент, формируют и обрабатывают сообщения протокола VTP, прозрачный агент не принимает активного участия в построении и обслуживании базы данных виртуальных сетей домена, однако может обеспечивать ретрансляцию сообщений VTP, поступающих на его порты.

Коммутатор, выполняющий функцию сервера, является полноправным участником протокола VTP. Имена и номера виртуальных сетей, создаваемых на этом коммутаторе заносятся в его локальную базу, после чего она синхронизируется с локальными копиями базы VLAN на других коммутаторах. Для этого коммутатор, выполняющий функцию VTP-сервера, на котором произошло изменение конфигурации, рассылает своим соседям сообщение "Общее объявление" (Summary advertisement), в котором указывается версия новой редакции базы. В том случае, если сосед располагает более старой версией базы, он направляет сообщение "Запрос объявления", в ответ на которое получает сообщение "Частичное объявление", содержащее необходимые данные об измененных VLAN.

Примечание

Сообщение "Общее объявление" рассылается каждым VTP-сервером раз в 300 сек даже в том случае, если изменений базы данных не проводилось.

Коммутатор, выполняющий функцию VTP-клиент, действует по аналогичному алгоритму. Единственное отличие клиента заключается в том, что на нем невозможно автономно выполнять изменения существующей базы данных (добавлять или удалять VLAN). В отличие от сервера, VTP-клиент не хранит копию базы данных в энергонезависимом запоминающем устройстве, поэто-

му каждый раз после включения электропитания он обязательно формирует сообщение "Запрос объявления".

Таким образом, благодаря постоянному обмену сообщениями протокола VTP, поддерживается актуальное состояние локальных копий базы данных VLAN на всех коммутаторах VTP-домена. Обладая информацией об активных VLAN, каждый коммутатор может выполнять процедуру вытеснения (pruning) пассивных виртуальных сетей со своих магистральных портов.

Применение протокола VTP так же, как и GVRP, обеспечивает согласованное и автоматическое изменение настроек всех прозрачных мостов (коммутаторов) ЛВС при изменении конфигурации VLAN на одном из них, что существенно облегчает их администрирование. В отличие от GVRP, протокол VTP обеспечивает требуемый уровень информационной безопасности, благодаря использованию встроенной процедуры аутентификации и возможности шифрования передаваемых сообщений при необходимости. К недостаткам этого протокола следует отнести то, что он поддерживается только на оборудовании одного производителя — Cisco Systems. В дополнение к этому следует отметить, что протокол VTP достаточно сложен для администрирования и его неаккуратное использование также может привести к нарушению информационного обмена в ЛВС.

Примечание

Появление в VTP-домене сервера с пустой базой данных и с большим значением идентификатора версии базы данных VLAN — Configuration Revision Number — приведет к обнулению локальных копий базы данных на всех коммутаторах домена.

Управление доступом абонентов к ресурсам МСС

Организация аутентификации — установление подлинности абонентов и управление их доступом к сетевым ресурсам принадлежит к числу наиболее важных задач, решаемых при построении мультисервисных сетей. Достоверное и надежное установление подлинности абонентов не только защищает сетевые ресурсы от несанкционированного доступа, но и способствует повышению авторитета провайдера и снижению себестоимости предоставляемых им услуг. Следует иметь в виду, что с задачей аутентификации обычно тесно связана еще одна важная задача — калькуляция стоимости предоставленной услуги — *(биллинг)*. Следовательно, неудачные технические решения, использованные для аутентификации и управления доступом абонентов, могут не только явиться причиной большого экономического ущерба для провайдера, но и существенно подорвать доверие его клиентов. Поэтому такое

большое внимание уделялось и уделяется разработке протоколов и технических решений для установления подлинности абонентов и управления доступом к сетевым ресурсам.

Для установления подлинности наиболее часто используются универсальные протоколы TACACS и RADIUS. Использование этих протоколов предполагает наличие сервера, который содержит базу данных абонентов. В этой базе данных в закодированном виде хранятся имена и пароли доступа абонентов. Процесс регистрации абонента при этом состоит из нескольких этапов.

1. Получение от абонента данных, необходимых для его регистрации.
2. Передача имени и кода доступа от абонента TACACS или RADIUS серверу.
3. Принятие решения об аутентичности абонента.
4. Подключение или отключение абонента от сетевых ресурсов.

Действия второго и третьего этапа обычно выполняются на TACACS- или RADIUS-сервере базы данных абонентов. Как правило, в этом случае в качестве сервера используется надежная вычислительная машина, на которой запущено соответствующее приложение (например, приложение RADIUS FreeBSD). Первый и последний этапы управления доступом абонентов к ресурсам сети выполняются на рабочей станции абонента и на сетевом устройстве управления доступом, которое расположено у провайдера. По сути, это устройство играет роль переключателя, который подключает абонента к сетевому ресурсу по команде сервера-аутентификации. Это же устройство получает от абонента данные, необходимые для его аутентификации, но лишь затем, чтобы передать их серверу. В качестве примера подобного устройства можно привести модемный пул, который взаимодействует с внешним RADIUS-сервером.

Примечание

В некоторых случаях устройство управления доступом может сочетать в себе функции сервера-аутентификации абонентов (например, при реализации функции RADIUS-сервера на модемном пуле). Несмотря на возможность создания при этом более компактных систем, такие схемы используются существенно реже из-за трудности их администрирования.

Особенность реализации решений управления доступом абонентов в мультисервисных сетях заключается в том, что эти сети, как правило, используют общие и разделяемые каналы передачи данных. В этих каналах трафик абонентов, прошедших процедуру аутентификации, может свободно соседствовать с трафиком абонентов, которые такую процедуру не проходили. Поэтому в мультисервисных сетях техническое решение управления доступом абонентов должно обеспечивать также изоляцию трафика аутентифицированных абонентов.

К протоколам, выполняющим подобные функции в мультисервисных сетях, можно отнести:

- *протокол PPPoE* (PPP over Ethernet IETF RFC 2516);
- *протокол PPTP* (Point-to-Point Tunneling Protocol IETF RFC 2637);
- *протокол IEEE 802.1X.*

Первые два из перечисленных протоколов являются разновидностями классического *протокола PPP* (Point-to-Point Protocol — IETF STD 51, RFC 1661), который используется для управления подключением абонентов по коммутируемым и выделенным каналам "точка-точка". Привлекательность идеи использования разновидностей протокола PPP состоит в том, что основанные на этом протоколе технические решения используются уже достаточно давно, поэтому соответствующие клиентские приложения и драйверы существуют в подавляющем большинстве современных операционных систем. В отличие от классического протокола PPP, протоколы PPPoE и PPTP разработаны для использования в современных вычислительных сетях, построенных на основе технологии Ethernet/IEEE 802.3. Протокол IEEE 802.1X построен с использованием модели клиент-сервер и также может применяться для ограничения доступа в локальных вычислительных сетях, построенных на прозрачных мостах (коммутаторах).

Протокол PPP

Протокол PPP (Point-to-Point Protocol) является универсальным протоколом канального уровня, который обеспечивает инкапсуляцию блоков данных протокола сетевого уровня в блоки данных канального уровня — кадры для их последующей передачи через каналы передачи данных.

Универсальность структуры кадра PPP, тщательно проработанной для сохранения совместимости с наиболее часто используемыми аппаратными средствами, обеспечивает возможность мультиплексирования различных протоколов сетевого уровня в одном физическом канале.

В то же время этот протокол является достаточно экономичным: всего 8 дополнительных байтов требуется для оформления инкапсулированного пакета, в том случае, когда используется заданный по умолчанию формат HDLC. При применении приложений, для которых важно наиболее полное использование пропускной способности канала, оформление пакета может быть сокращено до 2 или 4 байтов.

Функциями протокола PPP являются:

- управление адресами протокола сетевого уровня (IP);
- асинхронное и синхронное формирование пакета данных;

- мультиплексирование протоколов сетевого уровня;
- конфигурирование канала связи;
- проверка качества канала связи;
- обнаружение ошибок при передаче данных и согласование параметров сжатия информации.

Для обеспечения эффективного выполнения этих функций в протоколе PPP применяются экономичный алгоритм формирования кадра на основе протокола HDLC и два типа вспомогательных протоколов: протокол управления каналом — *LCP* (Link Control Protocol) и семейство протоколов управления сетью — *NCP* (Network Control Protocols).

Служебные протоколы PPP

Протокол LCP (Link Control Protocol) используется для автоматического согласования формата инкапсуляции, управления размерами кадров, установления подлинности партнера по соединению, обнаружения замыкания канала, иными словами, обеспечивает непосредственное управление функционированием канала.

Протоколы NCP (Network Control Protocols) предназначены для организации и выбора конфигурации PPP для взаимодействия с различными протоколами сетевого уровня. Для взаимодействия с протоколом IP, в частности, используются протоколы *IPCP* (IP Control Protocol) и *NCP* (Network Control Protocol) протокола PPP. Протокол IPCP обеспечивает настройку, активизацию и блокирование IP-модулей на обоих концах PPP-соединения, присвоение и управление IP-адресами, что является особенно актуальной и сложной задачей при использовании коммутируемых каналов.

При разработке протокола PPP предполагалось, что этот протокол должен быть максимально прост для конфигурирования. В соответствии с проектом, задаваемые по умолчанию значения изменяемых параметров этого протокола соответствуют его наиболее часто встречающейся конфигурации. Пользователь может переопределять заданную по умолчанию конфигурацию, причем изменения автоматически будут сообщены ответной части без его вмешательства. Это автоматическое конфигурирование реализовано с использованием дополнительного механизма согласования опций, в котором каждый конец канала сообщает свои возможности и требования. Примечательно, что в протоколе PPP один и тот же механизм согласования опций используется для протокола LCP и для семейства протоколов NCP.

Процедура информационного взаимодействия с использованием протокола PPP реализуется следующим образом:

1. Для того чтобы организовать взаимодействие через канал связи с непосредственным соединением, инициирующий абонент PPP отправляет LCP-

пакеты для выбора конфигурации и проверки качества канала передачи данных.

2. После того, как соединение в канале установлено и LCP-пакетом проведено необходимое согласование параметров канала, инициирующий узел протокола PPP отправляет NCP-пакеты для того, чтобы выбрать и определить конфигурацию одного или более протоколов сетевого уровня.
3. Как только конфигурация каждого выбранного протокола определена, дейтаграммы из каждого протокола сетевого уровня могут быть отправлены через данный канал.
4. Канал сохраняет свою конфигурацию для связи до тех пор, пока соответствующие сообщения LCP или NCP не закроют этот канал, или пока не произойдет какое-нибудь внешнее событие, например, истечет "срок допустимого бездействия" таймера или вмешается администратор системы.

Прежде чем по установленному соединению между узлами сети начнут передаваться IP-пакеты, протоколы LCP и IPCP должны, каждый на своем уровне, открыть канал. В информационное поле PPP-протокола инкапсулируется только одна IP-дейтаграмма, а максимальная длина IP-пакета, который можно передавать через PPP-соединение, равна максимальной длине информационного поля PPP-пакета. Если длина IP-дейтаграммы превышает эту величину, то она должна быть подвергнута фрагментации. Структура кадра протокола PPP приведена в табл. 7.6.

Таблица 7.6. *Структура кадра протокола PPP*

Номер поля	Наименование и содержание поля	Значение	Длина поля (байт)
1	FLAG — признак начала кадра	7E	1
2	ADDRESS — адрес абонента	FF	1
3	CONTROL — управление	03	1
4	PROTOCOL — тип протокола, использованного для формирования полезной нагрузки PPP-кадра	—	2
5	INFORMATION — полезная нагрузка кадра	—	>0
6	FCS — контрольная сумма	—	2
7	FLAG — признак завершения кадра	7E	1

- FLAG (1 байт)

  Поле флага. Это поле указывает на начало или конец блока данных. Это поле всегда содержит бинарную последовательность 01111110 (0x7E) и

служит в качестве разделителя пакетов. Пакет, состоящий из двух последовательно идущих байт 01111110, — игнорируется.

Примечание

Для обеспечения кодовой прозрачности протокола PPP все комбинации из шести последовательных единиц, встречающиеся в управляющих и информационных полях передаваемого PPP-кадра, заменяются на комбинацию бит — 01111101. Восстановление исходного вида кода производится после приема кадра при помощи процедуры обратной замены.

- ADDRESS

  Поле адреса (1 байт). Это поле является рудиментом, доставшимся протоколу PPP в наследство от протокола HDLC. Поле содержит бинарную последовательность 11111111, представляющую собой стандартный широковещательный адрес. Поскольку протокол PPP используется исключительно на линиях с двумя абонентами, присвоение им индивидуальных адресов канального уровня просто не имеет смысла.

- CONTROL

  Поле управления (1 байт). Это поле содержит бинарную последовательность 00000011, которая требует от пользователя передачи ответной информации. Пакеты с другим значением поля не обрабатываются.

- PROTOCOL

  Поле протокола (2 байта). Его значение идентифицирует протокол, заключенный в информационном поле блока данных. Например, для протокола IP значение этого поля равно 0x0021 (33).

- INFORMATION

  Поле данных. Длина поля — от нуля и больше; оно содержит дейтаграмму для протокола, заданного в поле протокола. Конец информационного поля определяется локализацией замыкающей последовательности "флаг" и предоставлением двух байтов полю FCS. Максимальная длина информационного поля по умолчанию равна 1500 байтам. В соответствии с соглашением, разрешающие реализации PPP могут использовать другие значения максимальной длины информационного поля.

- FCS

  Поле контрольной суммы (2 байта). Это поле содержит значение контрольной суммы всех полей пакета. В соответствии с априорным соглашением, разрешающие реализации PPP могут использовать 32-битовое (четырехбайтное) поле FCS, чтобы улучшить процесс контроля ошибок.

Протокол LCP предназначен для обеспечения динамического согласования параметров канала для протокола PPP. Протокол LCP представляет собой

внутренний протокол PPP, поэтому блоки данных протокола LCP передаются в информационном поле полезной нагрузки PPP-кадра. Только один блок данных протокола LCP (LCP PDU) одновременно может быть инкапсулирован в информационное поле PPP-кадра, при этом поле "Тип протокола" должно иметь значение 0xc021, что соответствует номеру протокола управления каналом — LCP. В табл. 7.7 приведена структура PDU протокола LCP.

Таблица 7.7. *Структура PDU протокола LCP*

Номер поля	Наименование и содержание поля	Длина поля (байт)
1	CODE — тип сообщения LCP	1
2	IDENTIFIER — идентификатор сообщения	1
3	LENGTH — длина LCP PDU, выраженная в байтах	2
4	DATA — полезная нагрузка PDU	>0

- CODE (код)

  Поле занимает один байт в заголовке блока данных протокола LCP. Код, размещенный в данном поле, определяет тип сообщения LCP. В том случае, если партнер PPP принимает блок данных с неизвестным ему значением поля CODE, он передает сообщение `Code-Reject` (код не принят). Перечень кодов сообщений протокола LCP и их назначения приведены в табл. 7.8.

Таблица 7.8. *Сообщения протокола LCP*

Код	Сообщение	Назначение
1	`CONFREQ` (Configure Request)	Запрос выбора конфигурации
2	`CONFACK` (Configure Ack)	Выбор конфигурации подтвержден
3	`Configure Nak`	Выбор конфигурации не подтвержден
4	`CONFREJ` (Configure Reject)	Конфигурация отклонена
5	`TERMREQ` (Terminate Request)	Запрос завершения
6	`TERMACK` (Terminate Ack)	Подтверждение завершения
7	`Code Reject`	Код отклонен
8	`Protocol Reject`	Протокол отклонен
9	`Echo Request`	Эхо-запрос
10	`Echo Reply`	Эхо-ответ
11	`Discard Request`	Запрос отброшен

- IDENTIFIER (идентификатор)

  Поле занимает один байт в заголовке блока данных протокола LCP. В этом поле размещается уникальный идентификатор, формируемый источником PPP-сообщения. Анализ значения этого идентификатора помогает установить соответствие переданных запросов и полученных ответов. В том случае, если PPP-партнер принимает блок данных с недопустимым значением данного поля, он должен игнорировать этот блок данных.

- LENGTH (длина)

  Поле занимает два байта в заголовке блока данных протокола LCP. Значение этого поля определяет длину блока данных протокола LCP, включая поля CODE, IDENTIFIER, LENGTH и DATA. Значение поля LENGTH не должно превышать величину MRU, установленную для данного канала. Байты, выходящие за диапазон, определенный полем LENGTH, обрабатываются как дополнение и игнорируются на приеме. Если получен блок данных с недопустимым значением поля LENGTH, то этот блок данных игнорируется.

- DATA (данные)

  Поле занимает нуль или более байтов, в строгом соответствии со значением поля длины. Формат и содержание поля DATA определяется типом передаваемого сообщения.

Использование протокола PPP для управления абонентом

Протокол PPP традиционно широко используется для управления подключением абонентов по выделенной и коммутируемой линиям. Возможности этого протокола позволяют успешно решать две основные задачи организации и обслуживания модемного соединения с удаленным абонентом:

- установление подлинности абонента;
- установка параметров протокола IP на рабочей станции абонента.

Для решения первой задачи используются служебный протокол PPP LCP, а также протоколы PAP или CHAP — для передачи данных между абонентом и сервером доступа, и протоколы RADIUS или TACACS+ для организации базы данных абонентов и обмена с ней сервера доступа. Листинг 7.1 содержит пример последовательности сообщений протокола PPP при попытке аутентификации нелегального пользователя. В качестве сервера доступа был использован маршрутизатор Cisco 2610, на котором включена отладочная печать командами `debug ppp negotiation` и `debug ppp authentication`.

Листинг 7.1. Протокол PPP. Отключение нелегального пользователя

```
   1. Сервер доступа получает запрос на аутентификацию нелегального
      абонента
   ...
Jul 31 13:12:35: As40 PAP: I AUTH-REQ id 3 len 20 from "baduser"
Jul 31 13:12:35: As40 PAP: Authenticating peer baduser
   2. Сервер доступа формирует сообщение об отказе в аутентификации
Jul 31 13:12:35: As40 PAP: O AUTH-NAK id 3 len 19 msg is "Request Denied"
Jul 31 13:12:35: As40 PPP: Phase is TERMINATING
   3. Сервер доступа формирует запрос на отключение абонента
Jul 31 13:12:35: As40 LCP: O TERMREQ [Open] id 174 len 4
   4. Абонент подтверждает отключение
Jul 31 13:12:35: As40 LCP: I TERMACK [TERMsent] id 174 len 4
   5. Сессия разрывается
Jul 31 13:12:35: As40 LCP: State is Closed
Jul 31 13:12:35: As40 PPP: Phase is DOWN
...
```

Далее приведен пример последовательности сообщений (листинг 7.2), используемых для присвоения собственного IP-адреса и адреса первичного DNS-сервера удаленному абоненту.

Листинг 7.2. Протокол PPP. Присвоение IP-адреса удаленному абоненту

```
   1. Абонент передал запрос с несформированными IP-адресами
Jul 31 13:11:07: As39 IPCP: I CONFREQ [ACKrcvd] id 6 len 22
Jul 31 13:11:07: As39 IPCP:  Address 0.0.0.0 (0x030600000000)
Jul 31 13:11:07: As39 IPCP:  PrimaryDNS 0.0.0.0 (0x810600000000)
   2. Сервер доступа не согласовал использование несформированных
      IP-адресов и передал абоненту их корректные значения
Jul 31 13:11:07: As39 IPCP: O CONFNAK [ACKrcvd] id 6 len 16
Jul 31 13:11:07: As39 IPCP:  Address 99.99.99.229 (0x03063E2163E5)
Jul 31 13:11:07: As39 IPCP:  PrimaryDNS 99.99.99.241 (0x81063E2163F1)
   3. Абонент установил IP-адреса, предложенные сервером доступа,
      и запрашивает возможность их использования
Jul 31 13:11:07: As39 IPCP: I CONFREQ [ACKrcvd] id 7 len 22
Jul 31 13:11:07: As39 IPCP:  Address 99.99.99.229 (0x03063E2163E5)
Jul 31 13:11:07: As39 IPCP:  PrimaryDNS 99.99.99.241 (0x81063E2163F1)
   4. Сервер доступа подтверждает возможность использования выданных
      IP-адресов абонентом
Jul 31 13:11:07: As39 IPCP: O CONFACK [ACKrcvd] id 7 len 22
Jul 31 13:11:07: As39 IPCP:  Address 99.99.99.229 (0x03063E2163E5)
```

```
Jul 31 13:11:07: As39 IPCP:  PrimaryDNS 99.99.99.241 (0x81063E2163F1)
```

5. Абонент начинает взаимодействие на сетевом уровне с использованием полученных от сервера доступа настроек

```
Jul 31 13:11:07: As39 IPCP: State is Open
Jul 31 13:11:07: As39 IPCP: Install route to 99.99.99.229
```

Протокол PPPoE

Протокол PPPoE (Point-to-Point Protocol over Ethernet) представляет собой стандартный метод организации сессии и инкапсуляции PPP-дейтаграмм при передаче их по сети Ethernet/IEEE 802.3. Основные принципы протокола изложены в документе IETF RFC 2516 (A Method for Transmitting PPP Over Ethernet February 1999 Category: Informational).

Применение этого протокола обеспечивает построение и обслуживание соединения "точка-точка" между абонентом и сервером доступа провайдера по сети с множественным доступом к среде передачи данных. Поскольку построенное таким образом соединение обладает всеми признаками соединения по выделенной линии, то для управления доступом по нему легко могут быть применены стандартные процедуры, используемые для аналогичных целей в протоколе PPP.

Основные принципы PPPoE

Процесс организации PPPoE-соединения состоит из двух этапов. В ходе первого этапа ("Поиск" — Discovery) клиент производит поиск сервера доступа, через который впоследствии будет организовано PPP-соединение. Если в сети используется одновременно несколько PPPoE-серверов доступа, на первом этапе также производится выбор одного из них в качестве кандидата для установления соединения. По завершению первого этапа клиент и сервер доступа получают все необходимые данные для организации PPP-соединения между собой. Поскольку PPPoE-соединение организуется на канальном уровне, то для его установления участникам достаточно знать MAC-адрес удаленного партнера. Этап поиска включает в себя четыре шага:

1. Клиент передает инициирующее (`Initiation`) сообщение по широковещательному адресу канального уровня (FF-FF-FF-FF-FF-FF).
2. Один или несколько серверов доступа передают сообщение — предложение (Offer) по MAC-адресу клиента.
3. Клиент передает сообщение о запросе сеанса (`Session Request`) по MAC-адресу выбранного сервера доступа.
4. Выбранный сервер доступа передает сообщение о подтверждении (`Confirmation`) установления сеанса.

Все сообщения, формируемые участниками на первом этапе PPPoE-сеанса, передаются в поле полезной нагрузки кадров Ethernet с установленным значением поля ETHER_TYPE = 88-63, что является отличительным признаком этапа Discovery протокола PPPoE. В табл. 7.9 приведена структура сообщения протокола PPPoE.

Таблица 7.9. *Структура сообщения протокола PPPoE*

Номер поля	Наименование и содержание поля	Значение	Длина поля (бит)
1	VER — номер версии спецификации PPPoE	1	4
2	TYPE — тип спецификации PPPoE	1	4
3	CODE — тип сообщения PPPoE		8
4	SESSION_ID — идентификатор сессии PPPoE		16
5	LENGTH — длина поля данных сообщения		16
6	PAYLOAD — поле данных сообщения PPPoE		

Содержимое полей VER и TYPE при использовании текущей версии протокола формируются значением 1.

Поле LENGTH сообщения PPPoE используется для размещения выраженной в байтах длины поля данных этого сообщения.

Поле PAYLOAD сообщения PPPoE используется для непосредственного размещения значений аргументов сообщения. Поскольку различные сообщения имеют разное количество аргументов, то это поле имеет переменную длину и формируется по схеме TLV с использованием специальных меток (TAG).

В поле SESSION_ID некоторых сообщений PPPoE помещается идентификатор установленной сессии.

Поле CODE используется для указания типа передаваемого сообщения PPPoE. В табл. 7.10 приведены значения полей CODE и SESSION_ID для сообщений PPPoE.

Таблица 7.10. *Значения полей CODE и SESSION_ID для сообщений PPPoE*

Сообщение PPPoE	Значение поля $CODE_{16}$	Значение поля $SESSION\_ID_{16}$
Active Discovery Initiation (PADI)	09	00-00
Active Discovery Offer (PADO)	07	00-00

Таблица 7.10 (окончание)

Сообщение PPPoE	Значение поля $CODE_{16}$	Значение поля $SESSION\_ID_{16}$
Active Discovery Request (PADR)	19	00-00
Active Discovery Session-confirmation (PADS)	65	00-00
Active Discovery Terminate (PADT)	a7	Номер разрываемого сеанса

После выполнения четвертого шага первый этап заканчивается и начинается второй этап, который представляет собой сеанс, выполняемый по правилам протокола PPP. Отличие сеанса PPPoE от обычного сеанса PPP заключается лишь в том, что блоки данных протокола PPP передаются не по выделенной или коммутируемой линии, а по сети Ethernet. Следствием этого является ограничение на максимальную величину передаваемого блока данных, которая в протоколе PPPoE не должна превышать 1492 байтов = 1500 байтов (Ethernet MTU) — 8 байтов (заголовок PPPoE).

Для организации информационного обмена с использованием протокола PPPoE на сервере доступа и клиентской рабочей станции создаются последовательные виртуальные интерфейсы. Обмен между абонентом и сервером доступа при этом выполняется только на канальном уровне. Однако если сервер доступа выполняет функцию маршрутизатора или прокси-сервера, то он может обеспечить доступ клиентской рабочей станции в сеть Интернет.

Особенности применения PPPoE в мультисервисных сетях

В мультисервисных сетях протокол PPPoE может быть использован для управления доступом абонентов к сетевому ресурсу. На рис. 7.6 приведен пример использования протокола PPPoE для управления доступом клиентов к серверу S1.

На приведенной схеме для аутентификации абонентов используется отдельный сервер RADIUS. Для организации доступа к сетевому ресурсу на абонентских рабочих станциях должно быть установлено программное обеспечение PPPoE-клиента. В качестве сервера доступа в данном случае используется многоуровневый коммутатор MSW1. Передача данных аутентификации между абонентом и сервером доступа выполняется по протоколу PAP. Для подключения к сетевому ресурсу S1 абонент должен пройти процедуру регистрации. В данном случае для абонента она ничем не отличается от обычной

процедуры коммутируемого доступа в Интернет, только вместо модемного соединения организуется виртуальное соединение между рабочей станцией абонента и сервером доступа. С абонентской рабочей станции данные, необходимые для аутентификации абонента, сервер доступа передает на RADIUS-сервер. В том случае, если имя и пароль абонента совпадают с записями базы данных сервера, регистрация абонента разрешается. Тогда сервер доступа передает рабочей станции абонента параметры IP-соединения, которые обеспечивают доступ к требуемому сетевому ресурсу. Если процесс регистрации абонента завершен неудачно, то абонент не получает от сервера доступа необходимых настроек и его сеанс PPPoE завершается. Для разделения легальных и нелегальных абонентов в данном случае используются виртуальные сети (см. *главу 8*) и списки доступа. Например, в данном случае системный администратор может сконфигурировать сервер доступа таким образом, что абонент, прошедший аутентификацию, получает IP-адрес из специального диапазона (например, 10.7.7.128/25). Специально сконфигурированный список доступа (access-list) при этом используется для предотвращения доступа к сетевому ресурсу остальных абонентов. В листинге 7.3 приведен пример конфигурационного файла сервера управления доступом с использованием протокола PPPoE для сети, схема которой приведена на рис. 7.6.

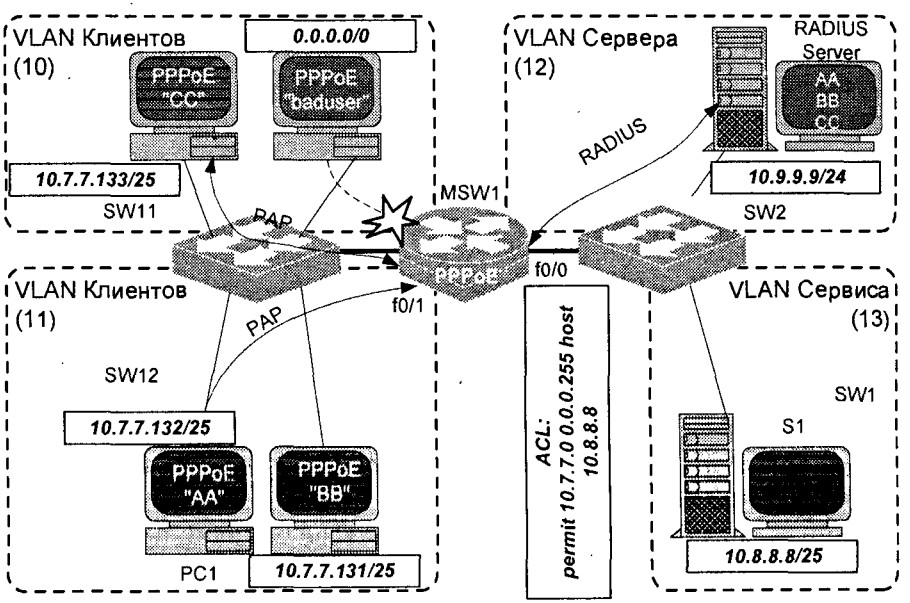


Рис. 7.6. Пример использования протокола PPPoE для управления доступом к ресурсам сервера S1

Листинг 7.3. Протокол PPPoE. Конфигурационный файл сервера управления доступом

1. На сервере доступа инициируется шаблон виртуального интерфейса для управления доступом по протоколу PPPoE

```
vpdn enable
vpdn-group 1
accept-dialin
protocol pppoe
virtual-template 1
```

2. На интерфейсах, к которым подключены потенциальные абоненты, включается протокол PPPoE

```
interface FastEthernet0/1.10
encapsulation dot1Q 10
no ip address pppoe enable
interface FastEthernet0/1.11
encapsulation dot1Q 11
no ip address
pppoe enable
```

3. На сервере доступа создается шаблон виртуального интерфейса и пул адресов для подключения абонентов PPPoE

```
interface Virtual-Template1
ip address 10.7.7.129 255.255.255.128
peer default ip address pool pool77
ppp authentication pap
ip local pool pool77 10.7.7.130 10.7.7.254
```

4. Для интерфейса, к которому подключен защищаемый ресурс, создается список разрешения доступа

```
interface FastEthernet0/1.13
ip address 10.8.8.1 255.255.255.128
ip access-group 111 out
access-list 111 permit ip 10.7.7.0 0.0.0.255 host 10.8.8.8
```

5. К серверу доступа для аутентификации абонентов PPPoE подключается внешний сервер RADIUS

```
aaa new-model
aaa authentication ppp RADIUS if-needed group radius local
radius-server host 10.9.9.9 auth-port 1812 acct-port 1813 key 7 XXXXX
```

В мультисервисных сетях Ethernet/IEEE 802.3, таким образом, протокол PPPoE достаточно успешно может быть использован для управления доступом абонентов к защищаемым сетевым ресурсам. Его основными преимуществами в этом случае являются:

- высокая эффективность использования полосы пропускания канала (заголовок PPPoE имеет длину всего 8 байтов);
- относительная простота настройки сервера доступа.

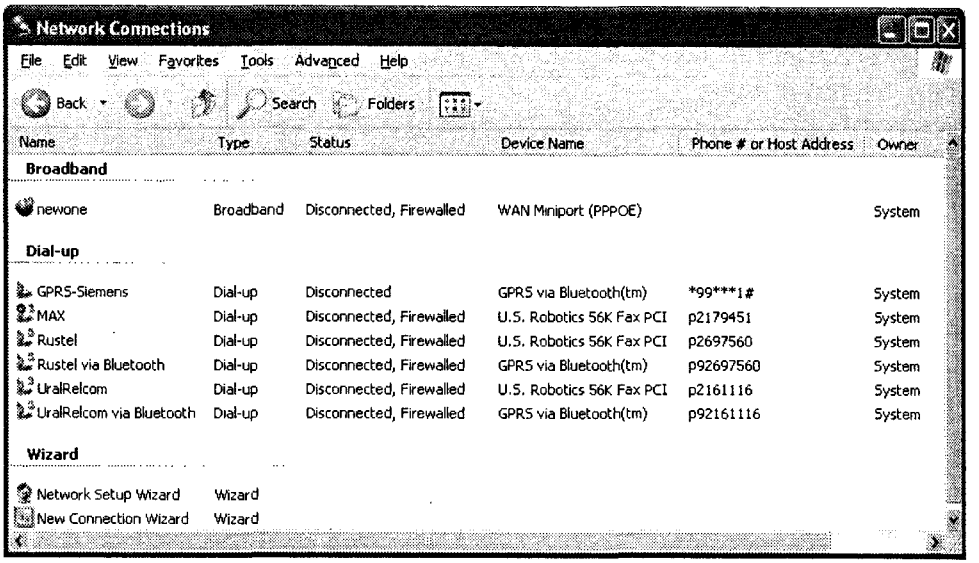


Рис. 7.7. Пример отображения PPPoE-соединения, созданного на PC под управлением MS Windows XP

Вместе с тем, протокол PPPoE имеет ряд достаточно существенных недостатков, которые проявляются при его использовании для управления доступом в мультисервисных сетях. Основным недостатком протокола PPPoE является требование подключения абонентов к серверу доступа по протоколу канального уровня. Это требование существенно ограничивает область применения протокола в современных сетях, в которых для подключения абонентов широко применяются такие технологии, как VLAN, NAT и Proxy. Еще одним существенным недостатком протокола PPPoE является его недостаточная поддержка производителями системного программного обеспечения. Базовые комплекты MS Windows 2000, например, не содержат предустановленного клиентского программного обеспечения для PPPoE. Впрочем, в операционной системе MS Windows XP такое программное обеспечение присутствует и не требует высокой квалификации для организации соединения. Это особенно важно, поскольку установка производится на рабочей станции абонента и все технические проблемы, которые она вызовет, умноженные на количество клиентов, лягут на плечи службы технической поддержки провайдера. На рис. 7.7 приведен пример отображения PPPoE-соединения, организованного на рабочей станции, функционирующей под управлением операционной системы MS Windows XP. Представленное на рис. 7.7 соединение newone было создано с использованием стандартного мастера (Wizard) за три шага без использования дополнительных драйверов или программного обеспечения. Примечательно, что при настройке PPPoE-клиента не требуется указывать какие-либо параметры сервера, поскольку его поиск клиент производит авто-

матически. Это несомненное достоинство протокола, которое, впрочем, одновременно является и недостатком PPPoE.

Требование организации обмена между абонентом и сервером доступа на канальном уровне приводит к необходимости размещения серверов в каждом сегменте вычислительной сети, где размещены потенциальные абоненты. Другим решением может быть размещение всех потенциальных абонентов PPPoE в одном сегменте ЛВС, но реализация как первого, так и второго решения в современных вычислительных сетях может быть сопряжена со значительными трудностями. Недостатками протокола PPPoE также являются ограничение на максимальный размер передаваемого блока данных и отсутствие функций управления потоком передаваемых данных, что в некоторых случаях может привести к неустойчивой работе и нарушению функционирования соединения.

Протоколы L2TP и PPTP

Протоколы *L2TP* (Layer Two Tunneling Protocol) и *PPTP* (Point-to-Point Tunneling Protocol) предназначены для обеспечения подключения пользователя к защищенным ресурсам частной сети (Private Network). Эти протоколы были созданы примерно одновременно, основные принципы их построения и использования описаны в следующих документах IETF (Internet Engineering Task Force):

- Point-to-Point Tunneling Protocol (PPTP) IETF RFC 2637 July 1999 Category: Informational;
- Layer Two Tunneling Protocol "L2TP" IETF RFC 2661 August 1999 Category: Standards Track.

Оба из вышеуказанных протоколов описывают способы и механизмы передачи блоков данных протокола PPP через сеть TCP/IP (Интернет) при взаимодействии удаленного пользователя с виртуальными частными сетями (Virtual Private Networks).

Хотя эти протоколы имеют очень много общего и отличия между ними не кажутся существенными, следует иметь в виду, что на статус официального стандарта в настоящее время претендует только протокол L2TP.

Протокол PPTP

В разработке спецификации протокола *PPTP* (Point to Point Tunneling Protocol — туннельный протокол "точка-точка") принимали участие представители компаний Ascend Communications, Microsoft Corporation, 3Com, Copper Mountain Networks, ECI Telematics. Протокол PPTP описывает способы и ме-

ханизмы передачи блоков данных протокола PPP через сеть TCP/IP (Интернет). Протокол PPTP может быть использован при создании защищенных каналов для организации информационного обмена с использованием сетевых протоколов IP, IPX или NetBEUI. Данные этих протоколов инкапсулируются в пакеты протокола IP по правилам протокола PPTP, после чего они могут в зашифрованном виде быть доставлены по открытой сети TCP/IP. Для аутентификации пользователя на сервере доступа предполагается использование протокола *MS-CHAP* (Microsoft Challenge Handshake Authentication Protocol). Для шифрования данных, передаваемых через открытые каналы, может быть использован протокол *MMPE* (Microsoft Point-To-Point Encryption Protocol).

Протокол PPTP предполагает разделение функций, которые обычно выполняются сервером доступа, между двумя независимыми устройствами:

- концентратором доступа PPTP — *PAC* (PPTP Access Concentrator);
- сетевым сервером PPTP — *PNS* (PPTP Network Server).

В табл. 7.11 приведено распределение функций стандартного сервера доступа между PAC и PNS.

Таблица 7.11. *Распределение функций стандартного сервера доступа между PAC и PNS*

Функция сервера доступа	Выполняется на PAC	Выполняется на PNS
Управление физическим подключением абонентов	Да	Нет
Терминирование сеансов PPP LCP	Да	Нет
Участие в аутентификации абонента	Да/Нет	Да
Объединение каналов Multilink PPP	Нет	Да
Терминирование сеансов PPP NCP	Нет	Да
Передача блоков данных между абонентами доступа	Нет	Да

Стандартным назначением протокола PPTP является обеспечение передачи данных между PAC и PNS. Кроме того, как уже было отмечено, этот протокол может быть использован для организации PPP-соединения между двумя станциями через сеть TCP/IP, при этом вызывающая станция должна выполнять функции PNS. В протоколе PPTP применяются расширенные функции управления потоками передаваемых данных и защиты от перегрузки, что позволяет наиболее эффективно использовать его пропускную способность для передачи данных.

Процесс организации защищенного соединения PPTP включает в себя три этапа:

- организация PPP-соединения между PPTP-клиентом и концентратором доступа PAC;
- создание управляющего соединения (Control Connection) между PPTP-клиентом и сетевым сервером PNS;
- построение PPTP-туннеля для передачи данных между PPTP-клиентом и сетевым сервером PNS.

Создаваемое на первом этапе между PPTP-клиентом и сетевым сервером PNS PPP-соединение используется для того, чтобы обеспечить возможность построения двух действующих постоянно соединений между PPTP-клиентом и сетевым сервером PNS. Соединение PPP в данном случае строится по обычным правилам с использованием стандартных технических решений и предназначено для решения следующих задач:

- организации и завершения физического соединения между PPTP-клиентом и концентратором доступа PAC;
- установления подлинности (аутентификации) абонента;
- инкапсуляции в PPP PDU-блоков данных протоколов для последующей передачи их через туннель.

Управляющее соединение используется для создания, управления и обслуживания PPTP-туннеля. Для этих целей в протоколе PPTP используются сообщения, которые передаются между PAC и PNS с использованием транспортного протокола TCP (порт назначения = 1723) по установленному соединению PPP. В табл. 7.12 приведен список управляющих сообщений протокола PPTP.

Таблица 7.12. *Управляющие сообщения протокола PPTP*

Имя сообщения	Назначение сообщения	Код
Start-Control-Connection-Request	Запрос создания управляющего соединения (УС)	1
Start-Control-Connection-Reply	Подтверждение создания УС	2
Stop-Control-Connection-Request	Запрос на закрытие УС	3
Stop-Control-Connection-Reply	Подтверждение закрытия УС	4
Echo-Request	Запрос контрольного эхо-сообщения	5
Echo-Reply	Ответ контрольного эхо-сообщения	6
Outgoing-Call-Request	Запрос исходящего вызова от PNS	7

Таблица 7.12 (окончание)

Имя сообщения	Назначение сообщения	Код
Outgoing-Call-Reply	Подтверждение исходящего вызова от PAC	8
Incoming-Call-Request	Запрос входящего вызова от PAC	9
Incoming-Call-Reply	Подтверждение входящего вызова от PNS	10
Incoming-Call-Connected	Соединение входящего вызова от PAC	11
Call-Clear-Request	Запрос отключения вызова от PNS	12
Call-Disconnect-Notify	Уведомление об отключении вызова от PNS	13
WAN-Error-Notify	Уведомление об ошибке подключения от PAC	14
Set-Link-Info	Информация о параметрах канала от PNS	15

Инкапсуляция данных абонента, передаваемых по туннельному соединению между PPTP-клиентом и сетевым сервером PPTP, производится по правилам интернет-протокола *GRE* (Generic Routing Encapsulation) (IETF RFC 1701, 1702 GRE). Блоки данных, передаваемые через туннельное соединение, при этом имеют следующую структуру:

1. Заголовок протокола канального уровня.
2. Заголовок протокола IP.
3. Заголовок протокола TCP.
4. Заголовок протокола GRE.
5. Блок данных протокола PPP.

Протокол PPTP сам по себе не обеспечивает информационную защиту устанавливаемых соединений. Поэтому для обеспечения должного уровня информационной безопасности должны быть использованы дополнительные средства. Рекомендованным для протокола PPTP является использование протокола *MS-CHAP* (Microsoft Challenge Handshake Authentication Protocol) на этапе аутентификации абонента и протоколов *MS-CCP* (Microsoft Compression Control Protocol) и *MPPE* (Microsoft Point-to-Point Encryption) для сжатия и шифрования передаваемых через туннель данных.

Протокол L2TP

В разработке спецификации протокола *L2TP* (Layer Two Tunneling Protocol — туннельный протокол второго уровня) принимали участие представители компаний Ascend Communications, Microsoft Corporation и Cisco Systems. Протокол L2TP представляет собой дальнейшее развитие протокола PPTP и

протокола *L2P* — Cisco Layer Two Forwarding Protocol (IETF RFC 2637 July 1999 Category-Informational).

Так же, как и протокол PPTP, протокол L2TP описывает способы и механизмы передачи блоков данных протокола PPP через сеть TCP/IP (Интернет). Протокол L2TP также предусматривает расщепление функций сервера доступа между концентратором доступа, размещаемым на точке выхода в сеть общего пользования L2TP — *LAC* (L2TP Access Concentrator) и сетевым сервером, размещенным в защищенной сети L2TP — *LNS* (L2TP Network Server). Так же, как и протокол PPTP, протокол L2TP использует управляющее соединение между концентратором и сетевым сервером для обслуживания создаваемого между ними туннельного соединения. Но управляющие сообщения, которые при этом используются в протоколе L2TP, незначительно отличаются от сообщений, используемых в протоколе PPTP. В протоколе L2TP, например, не используются контрольные эхо-сообщения, но добавлено сообщение `Outgoing-Call-Connected`. Еще одно существенное отличие протокола L2TP от PPTP заключается в отказе от использования протокола транспортного уровня TCP для передачи данных через туннель. В протоколе L2TP данные между LAC и LNS передаются с использованием транспортного протокола UDP (порт назначения = 1701). Незначительным изменениям по отношению к протоколу PPTP подверглась также структура передаваемого через туннель блока данных. В отличие от PPTP, протокол L2TP не использует в чистом виде спецификацию GRE для инкапсуляции блоков данных PPP в дейтаграммы UDP, однако заголовок, употребляемый для этих целей в протоколе L2TP, очень похож на заголовок GRE. В табл. 7.13 приведена структура заголовка протокола L2TP.

Таблица 7.13. *Структура заголовка протокола L2TP*

Номер поля	Содержание поля	Значение в управл. сообщении	Значение в PDU данных	Длина поля (бит)
1	Type (T) — тип сообщения	1	0	1
2	Length (L) — наличие поля Length в сообщении	1		1
3	Sequence (S) — наличие полей Ns и Nr в сообщении	1		1
4	Offset (O) — наличие поля Offset в сообщении	0		1
5	Priority (P) — приоритет сообщения	0		1
6	Ver — версия протокола L2TP	2	2	3
7	Length — общая длина сообщения (байт)			16
8	Tunnel ID — идентификатор управляющего соединения			16

Таблица 7.13 (окончание)

Номер поля	Содержание поля	Значение в управл. сообщении	Значение в PDU данных	Длина поля (бит)
9	Session ID — идентификатор сеанса внутри тоннеля			16
10	Ns — номер передаваемого сообщения	Ns	Ns	16
11	Nr — номер управляющего сообщения ожидаемого к приему	Nr		16
12	Offset — поле нагрузки	—		Var

Основные отличия протокола L2TP от PPTP определяются способами обеспечения информационной безопасности туннельного соединения. Решения, используемые в протоколе L2TP, обеспечивают более высокий уровень защиты по следующим причинам:

- шифрование данных в сеансе PPTP начинается только после установления PPP-соединения. При использовании L2TP/IPSec шифрование начинается до установления PPP-соединения;
- для шифрования данных, передаваемых через соединение PPTP, применяется протокол MPPE, основанный на алгоритме Rivest-Shamir-Aldeman RC-4, который обеспечивает возможность использования 40-, 56- и 128-битных ключей. Соединения L2TP/IPSec применяют стандартный *алгоритм кодирования DES* (Data Encryption Standard), который использует 56-битный ключ для DES или три 56-битных ключа для 3-DES;
- для установления подлинности абонента в протоколе PPTP используется только один уровень аутентификации — клиент-сервер по стандартным правилам PPP. L2TP/IPSec обеспечивает возможность реализации дополнительного этапа аутентификации с использованием сертификатов рабочих станций (computer certificate).

В остальных аспектах применение протокола L2TP обеспечивает такие же возможности по организации защищенного соединения через открытую сеть TCP/IP, как и протокол PPTP.

Применение туннельных протоколов в мультисервисных сетях

Как уже отмечалось, основным назначением туннельных протоколов PPTP и L2TP является обеспечение доступа удаленного абонента к ресурсам защищенных частных сетей. В мультисервисных сетях эти протоколы, также как и протокол PPPoE, могут быть использованы для управления доступом абонен-

тов к сетевым ресурсам. Специфика мультисервисных сетей в данном случае состоит в том, что в них все подключения абонентов выполняются, как правило, по технологии Ethernet/IEEE 802.3, поэтому отпадает необходимость использования концентратора доступа (LAC или PAC) для организации туннельного соединения. В этих случаях рабочая станция абонента выполняет те функции по организации и обслуживанию PPP-соединения, которые обычно возлагаются на концентратор доступа.

Кроме того, использование туннельных протоколов (в отличие от PPPoE) для управления доступом избавляет от необходимости подключения абонента к серверу на канальном уровне в пределах широковещательного домена. Все это существенно упрощает настройку и обслуживание аппаратуры, обеспечивающей управление доступом абонентов, поскольку в данном случае она может быть размещена там, где ее удобно администрировать.

Следует, однако, отметить, что при использовании туннельных протоколов для управления доступом абонентов несколько усложняется настройка клиентского программного обеспечения. В частности, для подключения к серверу по протоколу PPTP на рабочей станции потенциального абонента должны быть сконфигурированы:

- стартовый IP-адрес — на сетевой карте Ethernet;
- маска сети — на сетевой карте Ethernet;
- адрес шлюза — на сетевой карте Ethernet;
- IP-адрес сервера доступа (PAS) — на клиенте PPTP.

Поскольку стартовый адрес клиента нужен только для организации туннельного соединения, то его обычно назначают из диапазона предназначенного для абонентов частных сетей (Address Allocation for Private Internets — IETF RFC 1918 Category — Best Current Practice). При успешной аутентификации на рабочей станции абонента появится виртуальный интерфейс, которому и будет назначен адрес из пула сервера доступа. Процедура настройки собственно сервера доступа при использовании туннельных протоколов по отношению к процедуре, описанной для PPPoE (см. листинг 7.3), практически не изменяется. Изменения в данном случае касаются лишь типа протокола, который используется для построения туннельного соединения.

Протокол IEEE 802.1X

Протокол *IEEE 802.1X* определяет основные компоненты и алгоритмы, используемые в сетях Ethernet/IEEE 802.3 для ограничения несанкционированного подключения абонента к сетевым устройствам с применением процедуры аутентификации.

Отличия протокола IEEE 802.1X от описанных ранее спецификаций PPPoE, PPTP и L2TP объясняются тем, что он был изначально разработан для использования в обычных и беспроводных сетях с множественным доступом к среде передачи данных. Далее перечислены основные преимущества использования протокола IEEE 802.1X для ограничения несанкционированного доступа в сетях Ethernet/IEEE 802.3:

- протокол IEEE 802.1X представляет собой стандартное решение, которое поддерживается всеми производителями коммуникационного оборудования;
- в качестве узла ограничения доступа IEEE 802.1X используется коммутатор Ethernet;
- при отрицательном результате аутентификации или отказе от нее абонента автоматически происходит его отключение от сетевого устройства IEEE 802.1X.

Основные компоненты IEEE 802.1X

В протоколе IEEE 802.1X для организации установления подлинности абонента используется модель клиент-сервер. Основными компонентами IEEE 802.1X являются:

- *сервер аутентификации* (Authentication Server);
- *клиент-соискатель*, проходящий процедуру аутентификации (Supplicant);
- *узел ограничения доступа* (Access Point).

В качестве сервера аутентификации может быть использована одна или несколько рабочих станций, находящихся в защищенной зоне ЛВС, на которых выполняется приложение RADIUS-server. Функции, которые выполняет сервер аутентификации IEEE 802.1X, ничем не отличаются от функций, выполняемых аналогичными серверами при использовании протоколов PPPoE, PPTP и L2TP.

Абонентом IEEE 802.1X является клиентская рабочая станция, на которой установлено программное обеспечение для аутентификации по этому протоколу.

Узел ограничения доступа предназначен для подключения или отключения абонента от сети в зависимости от результатов выполнения его аутентификации на сервере. Порты узла доступа IEEE 802.1X могут находиться в одном из двух возможных состояний, соответствующих статусу авторизации подключенных к ним абонентов:

- *абонент авторизован* (Authorized) — нормальное состояние после успешной аутентификации абонента. Порт принимает от абонента все кадры;

- *абонент не авторизован* (Unauthorized) — нормальное состояние перед началом аутентификации абонента. Порт принимает от абонента только кадры с сообщениями расширяемого протокола аутентификации *EAPOL* (Extensible Authentication Protocol Over LAN).

По сути, узел доступа IEEE 802.1X играет роль ключа, управляемого сервером аутентификации.

Примечание

Коммутаторы некоторых производителей (например, Allied Telesyn или D-Link) могут одновременно выполнять функции узла ограничения доступа и сервера аутентификации IEEE 802.1X, что обеспечивает возможность их использования в автономном режиме.

Сообщения протокола IEEE 802.1X

Особенность протокола IEEE 802.1X состоит в том, что для установления подлинности абонента используется стандартный протокол *EAPOL* (Extensible Authentication Protocol Over LAN — расширяемый протокол аутентификации, предназначенный для использования в ЛВС). В сообщениях EAPOL размещаются данные, необходимые для установления подлинности абонента, а также управляющие команды. При выполнении процедуры аутентификации сообщения EAPOL передаются между узлом доступа и соискателем, а также между сервером аутентификации и узлом доступа. В табл. 7.14 приведен список сообщений EAPOL, используемых в протоколе IEEE 802.1X.

Таблица 7.14. *Сообщения EAPOL, используемые в протоколе IEEE 802.1X*

Имя сообщения	Назначение сообщения	Источник
EAP-Start	Запрос аутентификации абонентом	Клиент
EAP-Logoff	Завершение сеанса абонентом	Клиент
EAP-Packet	Данные для аутентификации абонента	Клиент
EAP-Success	Подтверждение аутентификации абонента	Узел доступа

Процедура аутентификации IEEE 802.1X может быть начата по инициативе или абонента, или узла доступа. Для того чтобы начать эту процедуру, абонент должен передать сообщение EAP-Start. В ответ на это сообщение клиент получает от узла доступа запрос параметров аутентификации, после чего начинается обычная процедура установления подлинности абонента. Узел доступа сам может начать эту процедуру, например, при обнаружении подключения нового абонента. Информацию для аутентификации, полученную от

абонента, узел управления доступом передает на сервер, который сравнивает их с записями клиентской базы данных и принимает решение об аутентификации данного абонента. Решение об успешном завершении процедуры аутентификации передается на узел доступа для подключения абонента к ресурсам сети. Узел доступа использует сообщение `EAP-Success`, для того чтобы проинформировать абонента об успешном завершении процедуры.

Особенности применения протокола IEEE 802.1X

Тот факт, что протокол IEEE 802.1X представляет собой стандартное решение, существенно облегчает его внедрение в мультисервисных сетях. Следует, однако, учитывать, что реализации этого протокола могут оказаться несовместимыми с фирменными решениями различных производителей коммуникационного оборудования. Например, на коммутаторах Cisco Systems протокол IEEE 802.1X не может быть применен на тех портах, где используется Port Security и наоборот. Не допускается на коммутаторах Cisco Systems также использование протокола IEEE 802.1X на портах магистрального, агрегированного и некоторых других типов. Поэтому перед внедрением протокола IEEE 802.1X в мультисервисную ЛВС администратор должен внимательно ознакомиться с документацией производителя об особенностях применения этого протокола на данном оборудовании.

Настройка протокола IEEE 802.1X на коммутаторе обычно выполняется по стандартной схеме (см. протокол PPPoE) и включает в себя настройку портов для управления подключением абонентов и определение параметров взаимодействия узла доступа с сервером аутентификации. Некоторые производители коммуникационного оборудования позволяют использовать дополнительные функции, облегчающие администрирование сети и управление абонентами IEEE 802.1X. К таким функциям можно отнести, например, аутентификацию абонента по инициативе администратора (команда `dot1x re-authenticate` Cisco Systems) или дополнительный контроль параметров подключаемого абонента (команда `dot1x port method` 3COM).

Управление доступом групп абонентов

В некоторых случаях при построении мультисервисных сетей целесообразно организовать управление доступом к сетевому ресурсу для нескольких групп абонентов. При этом в качестве критерия принадлежности к группе могут быть использованы:

- *номер виртуальной сети* (VLAN ID);
- *адрес канального уровня* (MAC-адрес);
- *адрес сети* (IP-адрес).

Если некоторым группам разрешен доступ к ресурсу, то все абоненты, принадлежащие к этим группам, имеют одинаковые возможности доступа к нему. Очень важно, однако, при этом не только исключить доступ к сетевому ресурсу абонентов других групп, но и обеспечить взаимную изоляцию трафика различных групп абонентов, для которых разрешен доступ к этому ресурсу. Отсутствие взаимной изоляции трафика различных групп абонентов приводит к существенному понижению уровня информационной безопасности мультисервисной ЛВС. Часто системы изоляции используются в сочетании с системами управления доступом. В этом случае индивидуальные системы управления доступом организуют подключение к сетевому ресурсу выбранных абонентов, в то время как системы изоляции трафика обеспечивают недоступность этого ресурса для остальных абонентов. Системы изоляции могут также использоваться в мультисервисных сетях и в виде самостоятельного решения, например, для предотвращения взаимного доступа к данным, передаваемым различными группами абонентов.

Среди решений, которые наиболее часто используются в мультисервисных сетях для изоляции трафика различных групп абонентов, в первую очередь, следует выделить асимметричные виртуальные сети и списки управления доступом.

Списки управления доступом — *ACL* (Access Control Lists) позволяют разделять трафик групп пользователей по атрибутам канального, сетевого и транспортного уровней эталонной модели OSI-7 (ISO 7498) и обеспечивают тем самым возможность независимого управления доступом для этих групп.

Применение асимметричных и частных виртуальных сетей (Asymmetric VLAN, Private VLAN) позволяет обеспечить взаимную изоляцию трафика нескольких групп абонентов, имеющих доступ к одному ресурсу.

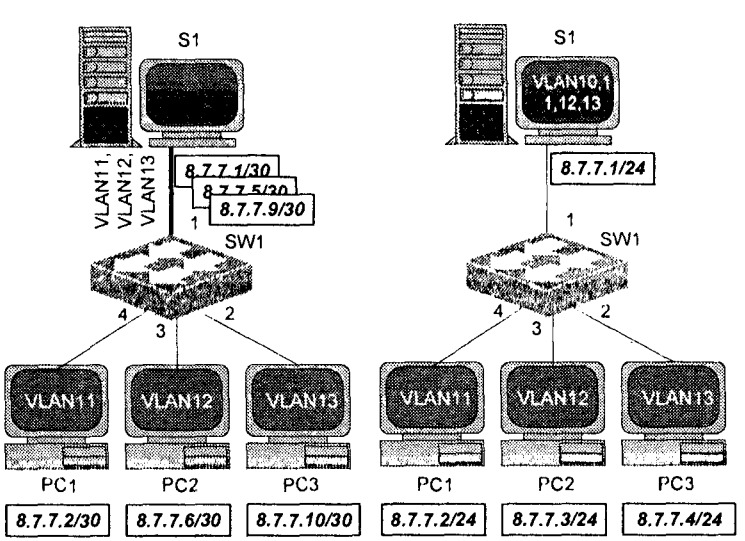
Для повышения общего уровня информационной безопасности в дополнение к системам группового и индивидуального управления доступом абонентов могут быть использованы специальные решения, обеспечивающие ограничение доступа абонентов к порту многопортового моста-коммутатора (Port Security).

Асимметричные VLAN

Как было отмечено ранее, виртуальные сети используются для разделения трафика различных групп абонентов. Важно отметить, что разделение выполняется на канальном уровне уровней эталонной модели OSI-7 (ISO 7498), и, следовательно, взаимодействие между разделенными при помощи виртуальных сетей группами абонентов может осуществляться только на сетевом или более высоких уровнях эталонной модели. Поэтому для организации

доступа различных групп таких абонентов к общему ресурсу бывает необходимо обеспечить его присутствие в нескольких виртуальных сетях одновременно. Обычно это реализуется путем подключения этого ресурса (например, медиасервера) к маркирующему порту многопортового коммутатора с использованием протокола IEEE 802.1Q. При этом на сервере, разумеется, должна быть установлена соответствующая сетевая карта и сконфигурированы виртуальные интерфейсы для каждой из используемых виртуальных сетей.

В качестве примера рассмотрим представленную на рис. 7.8, *а* сеть, в которой в качестве общего ресурса выступает почтовый сервер, а доступ трех групп абонентов, имеющих легальные IP-адреса, к этому серверу обеспечивается с использованием тегированного порта коммутатора. Такое решение нельзя, однако, считать универсальным и оптимальным. Подключение общего ресурса с использованием протокола IEEE 802.1Q обеспечивает изоляцию трафика подключаемых к нему различных групп абонентов, но такое решение зачастую бывает слишком дорогим для реализации и неудобным в обслуживании. Так в примере, представленном на рис. 7.8, *а*, для подключения абонентов необходимо использовать три (по числу групп подключаемых абонентов) различных IP-подсети и соответственным образом настраивать три виртуальных интерфейса на сервере.



Комм/порт	VLAN			
	10	11	12	13
Вариант а) Симметричные VLAN				
SW1/1		T	T	T
SW1/2				U
SW1/3			U	
SW1/4		U		
Вариант б) Асимметричные VLAN				
SW1/1	U	U	U	U
SW1/2	U			U
SW1/3	U		U	
SW1/4	U	U		

а) *б)*

Рис. 7.8. Организация доступа групп абонентов к общему ресурсу с использованием симметричных и асимметричных VLAN

Некоторые производители телекоммуникационного оборудования, среди которых можно выделить компании Cisco Systems и D-Link, предлагают оригинальные способы для решения сходных проблем. В дополнение к обычным (симметричным) виртуальным сетям, на коммутаторах этих производителей могут быть организованы специальные — асимметричные или частные VLAN.

Определение

Асимметричная виртуальная сеть представляет собой разновидность VLAN, прием и передача трафика между абонентами которой выполняется по различным правилам.

Таким образом, применение асимметричных VLAN позволяет организовать разделение трафика абонентов внутри одной виртуальной сети.

Различные производители предлагают разные способы для построения асимметричных виртуальных сетей. Например, асимметричные VLAN на оборудовании D-Link создаются путем включения порта коммутатора, к которому подключен общий сетевой ресурс, одновременно в несколько виртуальных сетей с признаком Untagged. На рис. 7.8, *б* приведен пример организации асимметричной виртуальной сети для разделения трафика абонентов, имеющих доступ к общему ресурсу. Поскольку абоненты находятся в различных виртуальных сетях, они взаимно изолированы. Отличие от первого примера заключается в том, что для подключения сервера используется специально настроенный демаркирующий порт коммутатора. В отличие от обычных VLAN, порт асимметричной виртуальной сети может быть демаркирующим для нескольких номеров виртуальных сетей. В этом случае сервер по-прежнему связан со всеми абонентами, причем для его подключения к коммутатору может быть использована обычная сетевая карта. Отпадает также необходимость в организации на нем виртуальных интерфейсов и присвоения им отдельных IP-адресов, что особенно важно при использовании адресов из диапазона открытых сетей Интернет. Существенным недостатком асимметричных виртуальных систем, организованных по описанному ранее принципу, является трудность их масштабирования. Действительно, в том случае, если абоненты ЛВС подключаются к различным коммутаторам, организовать асимметричную виртуальную сеть на оборудовании D-Link становится невозможно, поскольку при использовании асимметричных VLAN не происходит изучение, а также добавление в таблицы фильтрации MAC-адресов с тегированных портов. Тем самым применение асимметричных VLAN на оборудовании D-Link ограничивается одним коммутатором. В листинге 7.4 приведен пример конфигурационного файла, обеспечивающего построение асимметричных VLAN для сети, схема которой приведена на рис. 7.8, *б*.

Листинг 7.4. Построение асимметричных виртуальных сетей на коммутаторах D-Link

```
   1. Включение режима асимметричных виртуальных сетей на коммутаторе
enable asymmetric_vlan
   2. Создание виртуальных сетей
create vlan VLAN10 tag 10
create vlan VLAN11 tag 11
create vlan VLAN12 tag 12
create vlan VLAN13 tag 13
   3. Настройка виртуальных сетей для абонентов
config vlan VLAN11 add untagged 1,4
config vlan VLAN12 add untagged 1,3
config vlan VLAN13 add untagged 1,2
   4. Настройка виртуальной сети для сервера и сохранение конфигурации
config vlan VLAN10 add untagged 1-4
save
```

Решения, по организации асимметричных виртуальных сетей, предлагаемые компанией Cisco Systems, свободны от указанного недостатка. Асимметричные виртуальные сети, организуемые на коммутаторах этой компании, имеют название "частные виртуальные сети" (Private VLAN) и допускают возможность масштабирования. Такая возможность обеспечивается благодаря иерархической структуре частных VLAN, которые имеют следующие составляющие:

- основная виртуальная сеть (Primary VLAN);
- одна или несколько вторичных виртуальных сетей (Secondary VLAN).

Основная виртуальная сеть используется для переноса трафика вторичных виртуальных сетей через маркирующие порты при каскадном соединении коммутаторов. Для подключения компонентов частных виртуальных сетей могут быть использованы порты трех типов:

- *общедоступные* (Promiscuous Port);
- *клиентские* (Host Port);
- *магистральные* (Trunk Port).

Как понятно из названий, общедоступные порты частных виртуальных сетей используются для подключения общих сетевых ресурсов, для подключения изолированных абонентов нужно использовать клиентские порты. Магистральные порты используются в том случае, если частная виртуальная сеть распространяется за пределы одного коммутатора.

Таким образом, описанные выше асимметричные виртуальные сети позволяют обеспечить изоляцию трафика групп абонентов, имеющих доступ к единому ресурсу в ЛВС, которые построены на оборудовании компаний D-Link или Cisco Systems.

Примечание

Необходимо отметить, что решения, которые предлагаются различными производителями для организации асимметричных виртуальных сетей, не опираются на общий стандарт и являются взаимно несовместимыми. Более того, асимметричные VLAN могут поддерживаться не на всех моделях коммутаторов, поэтому к выбору этого решения нужно отнестись особенно внимательно.

Списки управления доступом

Списки управления доступом (Access Control Lists) представляют собой универсальное решение, которое используется при разделении (классификации) трафика для его последующей обработки. При разделении с помощью списков доступа могут анализироваться следующие параметры трафика:

- адреса протокола канального уровня OSI ISO 7498;
- адреса протокола сетевого уровня OSI ISO 7498;
- номера портов протоколов транспортного уровня OSI ISO 7498.

Список управления доступом включает в себя список правил разделения трафика и управляющую директиву.

Список правил должен иметь уникальный идентификатор (имя или номер) и может содержать несколько правил классификации, которые применяются последовательно к очередному обрабатываемому блоку данных до тех пор, пока его контролируемые параметры не совпадут с требованиями одного из них. Каждое правило классификации состоит из шаблона признаков и решения о классификации — "принять" (Permit) или "отклонить" (Deny). Правило может иметь порядковый номер для удобства редактирования. Шаблон признаков может включать значения или диапазоны адресов источника и (или) приемника данных. В листинге 7.5 приведен пример определения на коммутаторе Cisco Systems правила, которое выделяет из общего потока пакетов протокола IP только те, у которых адрес назначения равен 10.8.8.8, а IP-адрес источника находится в диапазоне 10:7.7.1—10.7.7.254.

Листинг 7.5. Создание расширенного списка доступа на коммутаторе Cisco Systems

```
1. Переход в режим создания расширенных //проверяющих адрес
   назначения и адрес источника пакета//,списков доступа
Ip access-list extended 111
```

```
   2. Создание нумерованного правила — используются два шаблона —
      "0.0.0.255" — //проверяются только три старших байта адреса
      источника// и "host" //проверяются все разряды адреса назначения//
access-list 111 permit ip 10.7.7.0 0.0.0.255 host 10.8.8.8
   3. Переход в режим настройки интерфейса
Interface f0/1
   4. Пропускать на выход интерфейса только пакеты, параметры которых
      удовлетворяют правилу 111
ip access-group 111 out
```

Основным назначением списка правил, таким образом, является выбор той части трафика, к которой будет применяться управляющая директива. Современные коммутаторы позволяют также создавать правила для классификации трафика по параметрам канального и транспортного уровней. В первом случае могут быть использованы MAC-адреса источника и приемника кадров, во втором — номера портов протоколов UDP и TCP.

Примечание

Определения правил классификации могут быть использованы не только для управления доступом. В современных коммутаторах подобные определения применяются, например, для управления полосой пропускания интерфейсов и организации политики маршрутизации.

Управляющая директива содержит идентификатор списка применяемых правил и определяет направление (входящий или исходящий), номер интерфейса, а также действие, которое выполняется с классифицированным трафиком. Смысл управляющей директивы может меняться в зависимости от того, для какой цели классифицируется трафик. Например, специальная управляющая директива может использоваться для ограничения доступа в коммутатор по протоколу Telnet ("ip access-class" в коммутаторах Cisco Systems). Один список правил классификации может быть использован несколькими различными управляющими директивами. Обычно имя управляющей директивы задает тип операции, которая будет выполняться с классифицированным трафиком, для правил транспортного и сетевого уровня используются одинаковые директивы управления (в приведенном листинге — это команда `ip access group`). Для правил канального уровня обычно используются отдельные управляющие директивы, например, для коммутаторов Cisco Systems для ограничения трафика на канальном уровне используется команда `mac access group`.

Далее перечислены основные ограничения и рекомендации, которые необходимо учитывать при использовании списков управления доступом на коммутаторах Catalyst компании Cisco Systems:

- на интерфейсе может быть определено только по одной управляющей директиве каждого типа для каждого направления трафика;
- в том случае, когда управляющая директива применяется к интерфейсу виртуальной сети, соответствующий список правил применяется ко всем интерфейсам, входящим в эту VLAN;
- если на одном интерфейсе определены управляющие директивы для списков управления доступом сетевого и канального уровня, в первую очередь будет выполняться директива сетевого уровня. Если этот порт к тому же принадлежит к некоторой VLAN, то преимущество получит управляющая директива, определенная на этой виртуальной сети.

Таким образом, списки управления доступом представляют собой универсальный и мощный инструмент, который может быть использован как для ограничения доступа к сетевым ресурсам, так и для различных манипуляций с трафиком, проходящим через коммутатор. Следует, однако, отметить, что для настройки и правильного применения на коммутаторе списков управления доступом необходимы твердые знания основных принципов организации сетевого взаимодействия. Нужно также учитывать, что использование многочисленных списков доступа сетевого и транспортного уровня может в некоторых случаях стать причиной недопустимого увеличения нагрузки на центральный процессор коммутатора, что, в свою очередь, может привести к резкому понижению скорости обработки кадров.

Функция Port Security

Функция Port Security обеспечивает повышение информационной безопасности ЛВС, благодаря незначительной модификации алгоритма функционирования прозрачного моста. Это простой и надежный аппарат, который обеспечивает реализацию базовых функций защиты портов на коммутаторах уровня доступа от несанкционированных подключений без увеличения нагрузки на центральный процессор коммутатора.

Основная идея Port Security заключается в управлении процессом обучения, который выполняется на порту каждого коммутатора. Обычно (см. *главу 6*) коммутатор автоматически определяет MAC-адреса подключенных абонентов, анализируя адреса источников принимаемых на порт кадров. При этом для каждого нового источника формируется динамическая запись, которая сохраняется в таблице фильтрации. Для того чтобы общее количество записей в таблице фильтрации не превысило размера выделенной для ее хранения области ОЗУ, время хранения динамических записей ограничено. Если в течение определенного интервала времени от источника не будет получено новых кадров, то соответствующая ему запись будет удалена из таблицы

фильтрации. Таким образом, стандартный режим обучения порта прозрачного моста-коммутатора характеризуется тем, что:

- при подключении нового абонента к порту его MAC-адрес автоматически заносится в таблицу фильтрации для данного порта;
- количество подключаемых абонентов практически не ограничено.

Следовательно, если потенциальный нарушитель имеет возможность непосредственного подключения к порту коммутатора, закрепленному за некоторой VLAN, то он автоматически получит доступ ко всем ресурсам этой виртуальной сети. Очевидно, что для повышения уровня информационной безопасности в сети было бы целесообразно ограничить возможность несанкционированных подключений к ресурсам ЛВС. Особенно актуально это для мультисервисных сетей, которые построены на статических виртуальных сетях и не используют процедуры установления подлинности абонента. В таких сетях подключение нелегального абонента может быть выполнено параллельно действующему абоненту и незаметно для него, например, через сетевой повторитель или неуправляемый коммутатор.

Повышение информационной безопасности при использовании функции Port Security достигается путем внесения следующих двух дополнительных функций в алгоритм работы прозрачного моста:

- функции отказа от режима обучения (формирования динамических записей в таблице фильтрации коммутатора) для выделенного порта коммутатора или ограничения количества обучаемых адресов;
- функции удаления всех поступающих на порт кадров, адрес источника которых отсутствует в таблице фильтрации и (или) формирование диагностического сообщения.

Таким образом, первая функция обеспечивает четкое разделение всех подключенных к порту абонентов на легальные и нелегальные. В случае отказа от режима обучения для легальных абонентов этого порта в таблице фильтрации формируются статические записи. При этом значительно повышается уровень информационной безопасности, поскольку адреса легальных абонентов хранятся на коммутаторе. Очевидно, что этот вариант по той же причине существенно более сложен для администрирования.

Для реализации функции Port Security в мультисервисных сетях более целесообразным представляется применение ограничений на общее количество легальных абонентов для выделенного порта. Этот вариант значительно упрощает администрирование и, вместе с тем, его применение может повысить уровень информационной безопасности ЛВС. К его недостаткам следует отнести трудность определения максимального количества легальных абонентов для каждого из портов. Если это количество будет слишком большим, то

нелегальный абонент может подменить собой одного из пассивных легальных абонентов, MAC-адрес которого был удален из таблицы фильтрации по тайм-ауту. Для предотвращения подобных ситуаций рекомендуется запрещать обновление по тайм-ауту таблицы фильтрации для данного порта.

Примечание

Следует учитывать, что использование функции Port Security с ограничением максимального количества подключаемых к порту абонентов даже при наличии запрета на обновление таблицы фильтрации по тайм-ауту не может обеспечить защиты от подключения нелегального абонента сразу после рестарта коммутатора. Эта проблема может быть решена путем настройки Port Security с использованием "клейких" (Sticky) MAC-адресов. В этом случае адреса легальных абонентов определяются коммутатором автоматически и хранятся в его конфигурационном файле.

При настройке функции Port Security следует также обратить внимание на тип реакции при обнаружении трафика нелегального абонента. В подобных ситуациях крайне желательным следует признать формирование диагностических сообщений администратору ЛВС. Это особенно важно при эксплуатации сложных сетей с большим количеством подключаемых абонентов. Дело в том, что "тихое" удаление трафика нелегальных абонентов лишает администратора информации о факте и времени нарушения и не дает ему возможности локализовать нарушителя, которым может оказаться и легальный абонент, поменявший сетевую карту на своей рабочей станции.

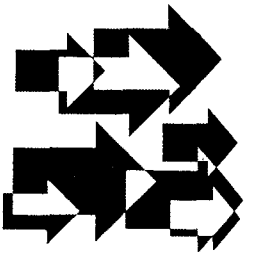
В листинге 7.6 приведен пример настройки функции Port Security на коммутаторе Allied Telesyn.

Листинг 7.6. Пример настройки функции Port Security на коммутаторе Allied Telesyn

```
Установка максимального количества обучаемых адресов на порту коммутатора
1:1 равным 1 и определение функции блокирования нелегальных MAC-адресов
до перезагрузки коммутатора.

AT-9724TS:4# config port_security ports 1:1 admin_state
enable max_learning_addr 1 lock_address_mode DeleteOnReset
Command:config port_security ports 5:1-5:5 admin_state
enable max_learning_addr 5 lock_address_mode DeleteOnReset
Success.
AT-9724TS:4#
```

ГЛАВА 8



Повышение надежности магистралей мультисервисных ЛВС

Основным способом повышения надежности является резервирование. Общеизвестно, что правильное использование этого способа позволяет строить достаточно надежные системы из относительно менее надежных компонентов. Широко знакомы также различные методы резервирования оборудования и каналов передачи данных — холодное резервирование, горячее резервирование, активное и пассивное резервирование.

Очевидно, что при построении ЛВС значительно более целесообразным следует считать применение различных вариантов активного резервирования, поскольку именно этот способ резервирования позволяет осуществлять быструю автоматическую реконфигурацию системы при выходе из строя одного из ее компонентов. Некоторые варианты реализации активного резервирования позволяют, кроме того, обеспечить распределение нагрузки между основным и резервными компонентами сети, что повышает эффективность использования оборудования и общую пропускную способность ЛВС.

В первом разделе данной главы приведено описание классического протокола связующего дерева — протокола *STP* (Spanning Tree Protocol), который традиционно используется для обеспечения активного резервирования каналов в сетях прозрачных мостов-коммутаторов. Алгоритм Spanning Tree, выполняемый на каждом из коммутаторов сети, обеспечивает автоматическое преобразование топологии.

Во втором разделе рассматриваются особенности построения и применения современного "быстрого" варианта протокола STP, а именно протокола *RSTP* (Rapid Spanning Tree Protocol). Применение этого протокола позволяет существенно сократить время переходного процесса при отказе одного из компонентов ЛВС.

Третий раздел посвящен рассмотрению многопланового протокола STP — протокола *MSTP* (Multiple Spanning Tree Protocol), использование которого

позволяет обеспечить распределение нагрузки между основными и резервными каналами и коммутаторами.

В заключительных разделах главы приведены рекомендации по использованию способов повышения надежности в мультисервисных сетях различных конфигураций.

Алгоритм Spanning Tree

В *главе 6* было показано, что использование прозрачных мостов для объединения компонентов обеспечивает целый ряд неоспоримых преимуществ при построении ЛВС. Однако при каскадном подключении таких мостов может возникнуть топология, в которой кадры будут циклически перемещаться по группе мостов, нарушая при этом нормальный информационный обмен в ЛВС. К сожалению, возможность возникновения такой проблемы заложена в самом алгоритме, в соответствии с которым функционирует прозрачный мост. Для возникновения этой ситуации достаточно, чтобы существовали как минимум два альтернативных маршрута, образующих кольцевую топологию локальной сети. Эти альтернативные маршруты могут появиться в сети в любой момент времени и по различным причинам, но, в любом случае, это приведет к полному отказу ЛВС. Для того чтобы предотвратить возможность возникновения подобных ситуаций, правила функционирования прозрачного моста должны быть дополнены алгоритмом Spanning Tree.

Возникновение "шторма" в ЛВС с кольцевой топологией

В качестве иллюстрации ЛВС с кольцевой топологией рассмотрим сеть, которая представлена на рис. 8.1. Мосты SW1 и SW2 соединяют два сегмента локальной сети, собранных на повторителях H1 и H2, в которых находятся рабочие станции PC1 и PC2. Предположим, что станция PC1 отправляет кадр, адрес назначения которого соответствует коду Broadcast канального уровня (FF-FF-FF-FF-FF-FF). Такая ситуация может произойти, например, в том случае, если станция PC1 сформирует запрос протокола ARP для того, чтобы определить значение MAC-адреса станции PC2.

В представленной структуре ЛВС это приведет к тому, что оба моста получат на свои порты № 1 кадр, адресованный в FFFF FFFF FFFF и, естественно, передадут его на свои порты № 2. После этого два Broadcast-кадра появятся в повторителе H2 и поступят через него не только на станцию PC2, но и обратно на порты № 2 мостов SW1 и SW2. В дальнейшем оба моста отправят эти кадры через свои порты № 1 обратно на повторитель H1, через который эти

кадры опять будут переданы на мосты SW1 и SW2 ... и т. д. — до бесконечности. Этот процесс действительно может продолжаться бесконечно долго, поскольку в кадре Ethernet отсутствует поле, ограничивающее время жизни кадра в сети. Поэтому прозрачный мост не имеет возможности отличить только что обработанные им кадры от кадров, поступивших на его порты извне. Чем быстрее прозрачный мост будет обрабатывать кадры, поступающие на его порт по циклическому маршруту, тем быстрее они к нему будут возвращаться вновь и вновь.

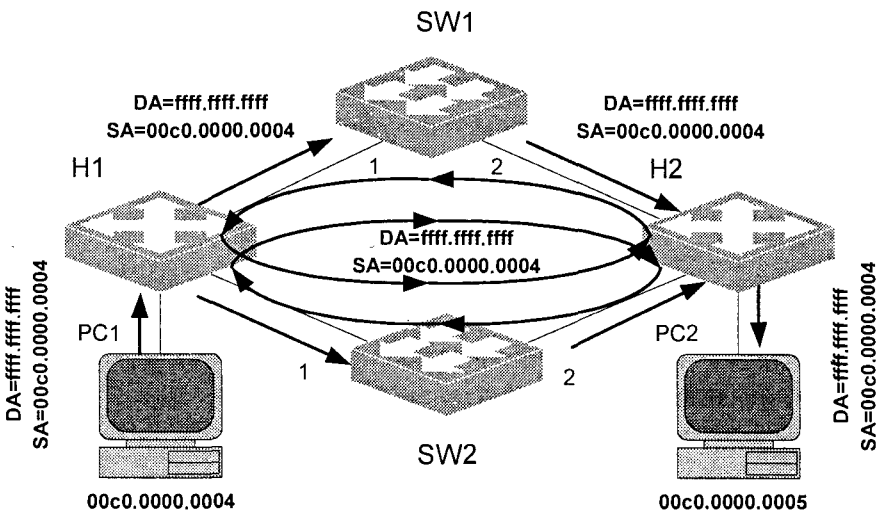


Рис. 8.1. Возникновение циклических маршрутов в сети прозрачных мостов

Определение

Broadcast-штормом называется процесс бесконечной передачи Broadcast-кадров в сетях прозрачных мостов.

При возникновении такого шторма ресурсы вычислительной сети оказываются заблокированными, поскольку все мосты данной ЛВС будут с предельно высокой скоростью циклически обрабатывать "штормовой" Broadcast-трафик.

Примечание

Следует отметить, что вследствие специфики обработки Broadcast-кадров в сети Ethernet, шторм окажет воздействие не только на мосты, образующие кольцевой маршрут, но и на рабочие станции, а также другие мосты, находящиеся с ними в одном Broadcast-домене. Аналогичные штормы могут возникнуть в такой сети также в случае появления в ней кадра с адресом назначения, для которого

не выполняются стандартные процедуры обучения и фильтрации. Примером таких кадров могут быть кадры с адресом назначения из Multicast-диапазона канального уровня.

Не вызывает сомнений, что Broadcast-шторм представляет довольно серьезную угрозу для функционирования сети. Рабочие станции при возникновении шторма в подключенной сети не только теряют доступ к общим сетевым ресурсам ЛВС, но и могут даже "зависнуть" из-за высокого уровня поступающего на них трафика. Удаленное управление мостами, вовлеченными в Broadcast-шторм, как правило, становится невозможным из-за крайне высокой нагрузки на центральный процессор. В некоторых случаях единственным средством для прекращения подобного шторма после его возникновения может быть только физический разрыв кольцевого соединения мостов.

Примечание

Некоторые производители коммуникационного оборудования предоставляют администратору ЛВС возможность использования специальных механизмов и функций для обнаружения и ограничения последствий возникновения Broadcast-штормов в сетях прозрачных мостов.

Применение альтернативных маршрутов в сети прозрачных мостов

В отличие от мостов, функционирующих по алгоритму Source Route, прозрачные мосты не могут использовать более одного маршрута одновременно для доставки кадров абонентам ЛВС. Поэтому появление в такой сети альтернативных маршрутов может быть вызвано двумя основными причинами:

- ошибкой администратора, выполняющего изменение топологии сети;
- пассивным резервированием каналов или компонентов ЛВС.

Первый из приведенных случаев особенно часто является причиной возникновения разнообразных штормов в ЛВС, поскольку при этом аварийная ситуация возникает совершенно неожиданно и плохо поддается как диагностированию, так и локализации. В больших и плохо документированных сетях достаточно неправильно выполнить всего лишь одно соединение, чтобы обеспечить возникновение в ЛВС несанкционированного альтернативного маршрута и, как следствие, Broadcast-шторма. Интервал времени, в течение которого после внесения некорректных изменений в топологию ЛВС возникает шторм, определяется особенностями информационного обмена в сети, а именно, частотой возникновения в ней Broadcast-кадров. Излишне говорить о том, что это свойство шторма еще более затрудняет обнаружение причины его появления. Возможность возникновения подобных ситуаций, однако, мо-

жет быть в достаточной мере ограничена благодаря применению административных методов, например, использованию специальных актов и отчетов при выполнении работ по изменению конфигурации сети.

Зачастую, однако, появление резервных маршрутов в ЛВС объясняется необходимостью обеспечить требуемый уровень надежности ее функционирования. Особенно это справедливо для локальных сетей крупных организаций. Такие сети, как правило, объединяют от 500 до 1 000 абонентов и имеют сложную многоуровневую архитектуру. К подобным сетям предъявляются повышенные требования в части безотказного функционирования, поэтому для обеспечения должного уровня надежности такие сети обычно имеют дублирующие каналы и резервные устройства. Действительно, в крупных сетях подобные решения кажутся вполне оправданными и целесообразными. Наиболее ответственные вычислительные сети строятся с максимальным использованием резервирования. В этом случае дублируются каналы передачи данных, оборудование центральных узлов ЛВС и источники электропитания. Как уже было отмечено в начале данной главы, особенно целесообразным при построении локальных сетей представляется использование горячего резервирования. Вместе с тем, очевидно, что построение дублированных сетей на прозрачных мостах неминуемо приведет к возникновению альтернативных маршрутов распространения кадров со всеми вытекающими в виде штормов последствиями.

Основные принципы алгоритма Spanning Tree

Очевидно, что для предотвращения подобных ситуаций достаточно изменить структуру сети таким образом, чтобы в ней не осталось циклов — и до любого компонента этой сети можно было дойти только по одному пути. Кроме того, очень важно, чтобы помимо исключения из сети циклических маршрутов, в сети существовал механизм, обеспечивающий мониторинг состояния и автоматическое изменение ее конфигурации при возникновении неисправности. Для выполнения всех этих функций в сетях прозрачных мостов и применяется Spanning Tree Algorithm — сокращенно *STA* (алгоритм связующего дерева).

Основные принципы построения сетей на основе прозрачных мостов были заложены компанией Digital Equipment Corporation (DEC) в начале 1980 годов. Идея алгоритма Spanning Tree также принадлежит компании DEC. Алгоритм Spanning Tree предназначен для изменения структуры построенной на мостах вычислительной сети таким образом, чтобы в ней отсутствовали циклы, и чтобы при этом сеть сохранила связность. Впоследствии этот алгоритм был взят за основу при разработке комитетом IEEE спецификации 802.1d, в соответствии с которой обеспечивалось автоматическое из-

менение структуры сети, построенной на устройствах типа прозрачного моста (transparent bridge).

В основу алгоритма STA положена теорема из теории графов.

Теорема

Структура любого связного графа, который содержит петли, может быть изменена путем удаления ребер таким образом, что он сохранит прежнюю связность, но не будет содержать петель.

Преобразование структуры ЛВС по алгоритму STA выполняется путем перевода в пассивное состояние тех портов прозрачных мостов, которые образуют петлевые маршруты передачи кадров. При этом, в первую очередь, блокированию подлежат порты, которые обеспечивают меньшую скорость передачи данных. Для того чтобы определить, какие порты образуют петлевые маршруты и подлежат блокированию, прозрачные мосты должны обмениваться специальными управляющими сообщениями.

В алгоритме используется термин *"Активная топология ЛВС"*.

Определение

Активной топологией называется образованная активными портами прозрачных коммутаторов совокупность путей, по которым в текущий момент времени обеспечивается передача кадров между абонентами ЛВС.

По замыслу разработчиков алгоритм STA должен решать следующие задачи:

- в реальном масштабе времени определять активную топологию ЛВС, таким образом, чтобы в ней отсутствовали альтернативные пути трансляции кадров между любыми из ее абонентов;
- обеспечивать устойчивость коммутационной структуры ЛВС путем автоматического изменения активной топологии при выходе из строя или изменении состояния имеющихся, а также при появлении новых компонентов ЛВС;
- активная топология, сформированная при выполнении алгоритма STA, должна быть стабильной в сетях любого размера, ее формирование должно осуществляться в течение коротких интервалов времени, величина которых должна быть заранее известна;
- активная топология, сформированная при выполнении алгоритма STA, должна быть предсказуемой и воспроизводимой, выполнение алгоритма не должно затрагивать пользовательские станции, подключенные к ЛВС;
- доля пропускной способности ЛВС, используемой для выполнения служебного обмена по протоколу STP, должна быть незначительной и не должна существенно зависеть от размера вычислительной сети.

Для корректного выполнения алгоритма STA необходимо, чтобы в сети мостов были выполнены следующие предварительные установки:

- должен быть определен групповой или иначе Multicast-адрес канального уровня, распознаваемый всеми прозрачными мостами в сети в качестве собственного адреса при рассылке управляющих сообщений;
- каждый мост должен иметь уникальный идентификатор (Bridge Identifier). Обычно в качестве этого идентификатора используется 8-байтовое число, старшие 2 байта которого соответствуют относительному приоритету моста, младшие 6 байтов соответствуют MAC-адресу моста. При сравнении альтернативных вариантов предпочтение отдается мосту, имеющему меньшее значение идентификатора. Значение относительного приоритета моста обычно устанавливается администратором сети;
- каждый порт моста тоже должен иметь уникальный идентификатор (Port Identifier). В качестве этого идентификатора используется двухбайтовое число, состоящее из приоритета порта и номера порта;
- для каждого порта моста должно быть определено значение относительной стоимости отправки кадров через данный порт, которое зависит от пропускной способности подключенного к нему канала (Path Cost).

Алгоритм STA включает в себя следующие процедуры:

- *выбор (определение) корневого моста;*
- *построение активной топологии ЛВС;*
- *изменение активной топологии ЛВС.*

Процедуры алгоритма STA выполняются независимо на всех мостах ЛВС. Для обеспечения согласованности выполнения этих процедур мосты обмениваются управляющими сообщениями протокола *STP* (Spanning Tree Protocol).

Определение

Протокол STP (Spanning Tree Protocol) определяет номенклатуру, правила формирования и формат сообщений, которыми обмениваются прозрачные мосты в локальной сети для выполнения алгоритма STA (Spanning Tree Algorithm).

Назначение корневого моста

Корневой мост в алгоритме Spanning Tree является точкой, с которой начинается построение связующего дерева ЛВС, поэтому справедливо следующее определение.

Определение

Корневым мостом в алгоритме STA (Spanning Tree Algorithm) называется мост, расположенный в вершине дерева активной топологии сети.

Теоретически любой мост связной сети может быть выбран в качестве корневого моста. Важно, однако, чтобы этот мост был только один и, чтобы все мосты вычислительной сети имели одинаковое представление о том, какой именно мост выполняет функции корневого при построении связующего дерева. Для обеспечения уникальности корневого моста алгоритм STA предписывает использование в качестве критерия его выбора значение идентификатора моста. В соответствии с этим алгоритмом корневым становится мост с наименьшим значением *идентификатора моста — Bridge Identifier* (Bridge ID). Как уже было отмечено, этот идентификатор состоит из двух компонентов: MAC-адреса моста и его индивидуального приоритета. По умолчанию значение индивидуального приоритета у всех прозрачных мостов устанавливается равным 32768. Поле приоритета включено в идентификатор для того, чтобы системный администратор мог управлять процессом выбора корневого моста. О том, насколько важен правильный выбор корневого моста, можно получить представление по приводимому далее примеру. На рис. 8.2 представлена схема сети, которая предназначена для передачи потокового трафика от сервера S1 группам абонентов G0...G6. Сеть построена с использованием резервирования каналов, имеет петлевые маршруты. В качестве корневого моста в этой сети при равных значениях индивидуальных приоритетов будет выбран мост SW0, поскольку он имеет наименьший MAC-адрес. Значения индивидуальных приоритетов у всех мостов равны (число в скобках).

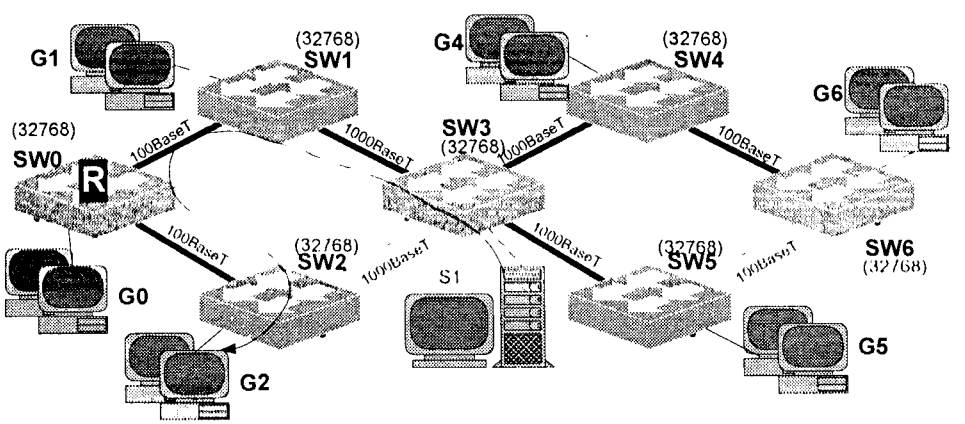


Рис. 8.2. Нарушение информационного обмена при некорректном выборе корневого моста

Заблокированные в результате выполнения алгоритма STA каналы на рисунке представлены тонкими линиями. Корневой мост отмечен буквой "R" (root).

Очевидно, однако, что такое расположение корневого моста существенно изменит схему информационного обмена в представленной на рисунке сети.

Действительно, в данном случае высокоскоростной канал между мостами SW3 и SW2 окажется заблокированным, вследствие чего абоненты группы G2 вынуждены будут получать потоковый трафик от сервера S1 по транзитному маршруту SW3-SW1-SW0-SW2. Понятно, что сформированная подобным образом активная топология не обеспечивает эффективную передачу клиентского трафика. Мало того, что трафик группы G2 передается по более длинному низкоскоростному маршруту, он еще мешает распространению трафика групп G1 и G0, поскольку отнимает часть полосы пропускания соответствующих каналов и вычислительных ресурсов мостов, через которые он не должен был проходить. Для восстановления планируемой схемы информационного обмена в приведенной на рисунке сети вполне достаточно правильно разместить в ней корневой мост. На рис. 8.3 показана схема той же сети, что была представлена на рис. 8.2, однако с другим расположением корневого моста.

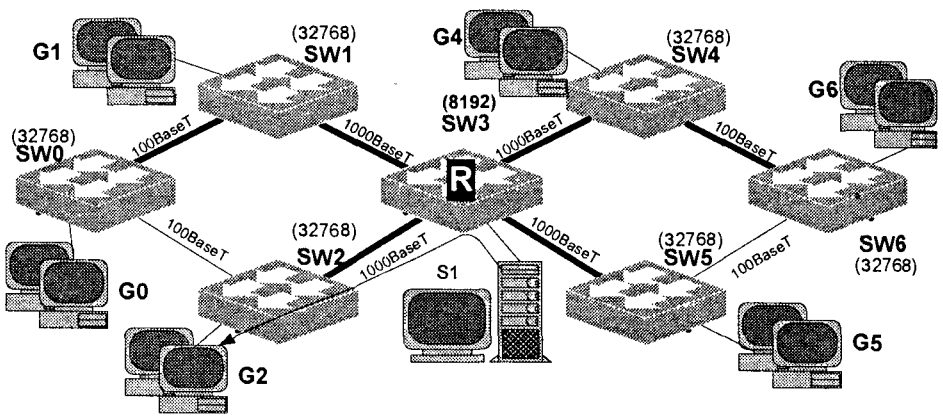


Рис. 8.3. Восстановление схемы информационного обмена при корректном выборе корневого моста

Для восстановления планируемой схемы информационного обмена в представленной сети было достаточно уменьшить значение индивидуального приоритета у моста SW3. Активная топология, представленная на рис. 8.3, обеспечивает максимально симметричную загрузку высокоскоростных каналов и кратчайшие маршруты для доставки потокового трафика от сервера групповым абонентам. Показанные примеры лишний раз подтверждают, насколько важно правильное расположение корневого моста в сети. Дело в том, что алгоритм автоматического выбора корневого моста не может учитывать ни расположение моста в сети, ни скорость передачи данных по каналам, которыми он включен в эту сеть. Поэтому в сложных сетях с резервированными каналами вмешательство администратора в процесс выбора корневого моста становится просто неизбежным.

Примечание

Некоторые производители коммуникационного оборудования (например, Cisco Systems) представляют администратору сети возможность использования специальных макрокоманд для управления процедурой назначения корневого моста. При выполнении таких команд коммутатор анализирует значения индивидуальных приоритетов у активных коммутаторов сети и автоматически определяет требуемое значение собственного приоритета для того, чтобы стать корневым.

Определение корневого и назначенных портов

В соответствии с выполняемой функцией все порты корневого моста находятся во включенном состоянии и передают полезный трафик. Порты остальных коммутаторов сети либо остаются во включенном состоянии, либо блокируются — в зависимости от расположения данного моста по отношению к корневому. При этом один из портов таких коммутаторов обязательно получает статус корневого порта (Root Port).

Определение

Корневым портом (Root Port) считается тот из портов моста, который связан наиболее дешевым путем с корневым мостом.

Для определения корневого порта используются понятия стоимости передачи трафика через порт (Port Cost) и стоимости корневого маршрута (Root Path Cost). В соответствии с установленными для алгоритма STA правилами, стоимость передачи трафика через порт прозрачного моста обратно пропорциональна скорости передачи данных через него. В табл. 8.1 приведены значения стоимости передачи трафика через порт для наиболее популярных технологий и скоростей передачи данных в современных вычислительных сетях.

Таблица 8.1. *Стоимость передачи трафика через порт для различных технологий*

Тип технологии	IEEE 802.5	IEEE 802.3	IEEE 802.5	PDH/ SDH	IEEE 802.3	SDH	SDH	IEEE 802.3	IEEE 802.3
Скорость передачи данных (Мбит/сек)	4	10	16	45	100	155	622	1	10
Стоимость передачи трафика	250	100	62	39	19	14	6	4	2

Корневым маршрутом принято называть последовательность каналов и портов коммутаторов, которые связывают конкретный порт данного коммутатора с корневым мостом.

Определение

Стоимостью корневого маршрута называется арифметическая сумма стоимостей передачи трафика тех портов, через которые этот маршрут проходит.

Следует отметить, что в соответствии с правилами, установленными для алгоритма STA, стоимость передачи трафика через порты корневого моста установлена равной 0. В качестве иллюстрации определения стоимости корневого пути рассмотрим сеть, схема которой приведена на рис. 8.4. Представленная сеть образована шестью мостами SW0—SW5. В качестве корневого моста этой сети выбран SW0 (он помечен буквой "R"). Повторители H1 и H2 в этой сети используются для подключения к ней абонентских рабочих станций (PC1—PC5). Цифрами на этом рисунке отмечены номера портов мостов, число в прямоугольнике указывает стоимость передачи данных через соответствующий порт прозрачного моста, корневые порты мостов отмечены белой точкой.

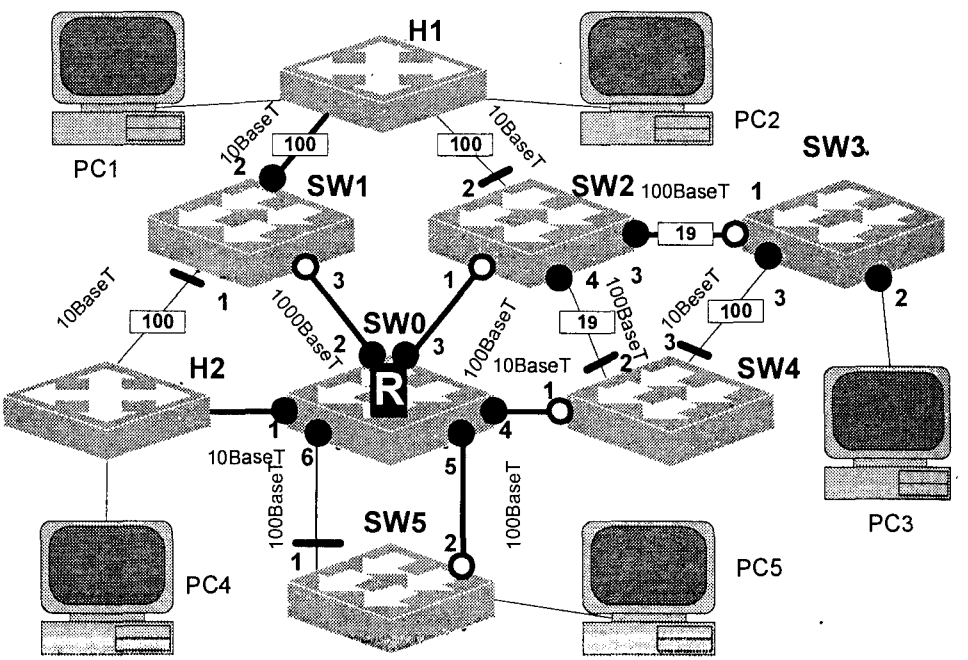


Рис. 8.4. Определение стоимости корневого маршрута

На приведенной схеме видно, что при выборе корневого порта преимущество получает тот из портов прозрачного моста, который связан с корневым мостом наиболее дешевым маршрутом. Например, корневым у моста SW3 выбран порт 1, поскольку стоимость его корневого маршрута (19) меньше, чем

стоимость маршрута для порта 3 (100). В том случае, если несколько портов моста имеют одинаковое значение величины корневого маршрута, предпочтение при выборе корневого порта отдается порту, к которому подключен мост с меньшим значением идентификатора (Bridge ID). В том случае, если конкурирующие порты подключены к одному мосту (порты 1 и 2 моста SW5), предпочтение отдается порту, к которому подключен порт с меньшим значением идентификатора (Port ID) другого моста. В том случае, когда конкурирующие порты подключены к одному порту одного моста (например, через повторитель), корневым становится тот из них, который имеет наименьшее значение идентификатора.

После определения корневых портов выполняется процедура определения выбранных (или иначе назначенных) портов (designated port) и мостов (designated bridge). Порты, получившие статус назначенных, остаются включенными и так же, как и корневые порты, участвуют в передаче данных.

Определение

Назначенным мостом для некоторого сегмента сети считается мост, который связывает этот сегмент с корневым мостом наиболее дешевым маршрутом. Порт, через который назначенный мост подключен к этому сегменту, называется *назначенным портом*.

В том случае, если несколько мостов будут иметь одинаковое значение стоимости корневого маршрута, в качестве назначенного будет выбран мост, который имеет минимальное значение идентификатора. В частности, для рассматриваемого варианта сети, назначенным мостом для сегмента, образованного повторителем H1, будет выбран мост SW1, через который проходит маршрут с тем же значением стоимости, что и через мост SW2. Аналогичным образом мост SW2 будет выбран назначенным мостом для сегмента, в котором находятся всего два абонента — порт 4 моста SW2 и порт 2 моста SW4. Порт назначенного моста, который используется для подключения к выбранному сегменту сети, называется *назначенным портом*. На представленном рисунке назначенные порты отмечены черными кружками. В том случае, когда несколько портов одного моста претендуют на статус назначенного порта, предпочтение отдается порту с наименьшим идентификатором.

После того, как были определены корневые и назначенные порты, может быть выполнена процедура формирования активной топологии. В соответствии с этой процедурой, порты всех мостов, которые не получили статус корневых или назначенных, должны быть переведены в *заблокированное* состояние. На приведенном рисунке при выполнении этой процедуры окажутся заблокированными, например, порты 2 и 3 моста SW4. Заблокированные порты на рисунке помечены пересекающей линией. После блокирования "лишних" портов формирование активной топологии считается завершенным, поскольку

ку теперь в сети остался только один маршрут доставки данных до любого из подключенных к ней абонентов.

Практическая реализация алгоритма Spanning Tree

На практике алгоритм Spanning Tree реализуется распределенным образом каждым мостом в отдельности. Для обеспечения информационного обмена в процессе выполнения этого алгоритма мосты посылают друг другу специальные сообщения, которые называются *BPDU* (Bridge Protocol Data Units). Сообщения BPDU размещаются в поле полезной нагрузки блоков данных канального уровня — кадров Ethernet. Структура кадра Ethernet, который используется для переноса сообщения BPDU, приведена в табл. 8.2.

Таблица 8.2. *Структура кадра Ethernet, который используется для переноса сообщения BPDU*

Номер поля	Содержание поля	Значение	Длина поля (байт)
1	Destination Address — адрес назначения кадра	01-80-c2-00-00-00	6
2	Source Address — адрес источника кадра		6
3	Type Length — тип или длина полезной нагрузки кадра		2
4	Заголовок LLC (DSAP-SSAP-CONTROL)	66-66-3	3
5	BPDU — тело сообщения BPDU		—

В качестве адреса станции назначения для передачи BPDU-сообщений используется специальный адрес канального уровня из Multicast-диапазона Bridge Group Address 0180-c200-0000. Кадры с таким адресом назначения должны приниматься и обрабатываться всеми прозрачными мостами сети.

При выполнении процедуры Spanning Tree используются два типа BPDU-сообщений:

- сообщения Configuration (BPDU-C);
- сообщения Topology Change Notification (BPDU-TCN).

Сообщения первого типа формируются корневым мостом и используются для формирования и оперативного изменения структуры ЛВС в соответствии с правилами алгоритма Spanning Tree. Сообщения второго типа могут быть сформированы любым мостом из числа входящих в систему и предназначены

для уведомления корневого моста о произошедшем изменении активной топологии сети прозрачных мостов.

Формирование сообщений Spanning Tree

Сообщения BPDU-C, рассылаемые корневым мостом, как раз и являются тем инструментом, с помощью которого формируется активная топология ЛВС. Именно эти сообщения несут в себе информацию о стоимости пройденного ими маршрута, что дает возможность принимающим их мостам получить представление о конфигурации сети. При помощи этих сообщений также формируются согласованные для всех мостов данной сети единые значения общих переменных, которые используются для реализации протокола STP (Spanning Tree Protocol). Эти же сообщения, в конечном счете, используются и для выбора, мониторинга состояния и перевыборов (в случае необходимости) корневого моста. Дело в том, что обычно корневой мост формирует сообщения BPDU-C с постоянным периодом, помещая в них значение своего идентификатора. До тех пор, пока остальные мосты данной сети получают такие сообщения, структура сети считается стабильной. Потеря нескольких последовательных сообщений BPDU-C может быть вызвана неисправностью одного из каналов сети или корневого моста. В последнем случае сообщения BPDU-C будут использованы при организации выбора нового корневого моста.

Структура сообщений BPDU-C приведена в табл. 8.3.

Таблица 8.3. *Структура сообщения BPDU-C*

Номер поля	Содержание поля	Значение (шест.)	Номера занимаемых байтов
1	PROTOCOL IDENTIFIER — идентификатор протокола	00-00	1—2
2	VERSION — версия протокола STP	00	3
3	MESSAGE TYPE — тип сообщения STP	00	4
4	FLAGS — поле флагов STP		5
5	ROOT ID — идентификатор корневого моста		6—13
6	ROOT PATH COST — стоимость корневого пути		14—17
7	BRIDGE ID — идентификатор моста, от которого это сообщение было получено		18—25
8	PORT ID — идентификатор порта, через который это сообщение было отправлено		26—27
9	MESSAGE AGE — время существования данного сообщения		28—29

Таблица 8.3 *(окончание)*

Номер поля	Содержание поля	Значение (шест.)	Номера занимаемых байтов
10	MAXIMUM AGE — максимальное время хранения сообщения		30—31
11	HELLO TIME — период отправки сообщений HELLO		32—33
12	FORWARD DELAY — величина задержки включения порта		34—35

- Поле PROTOCOL IDENTIFIER занимает 2 байта в BPDU-сообщении и формируется значением 00000000.
- Поле VERSION занимает 1 байт в BPDU-сообщении. Существующей в настоящий момент версии алгоритма STA соответствует значение 0000 данного поля. Предполагается, что в будущем в этом поле будут размещаться идентификаторы, с помощью которых может быть определен номер версии протокола, используемого мостом, который сформировал BPDU.
- В поле MESSAGE TYPE размещается признак, с помощью которого различаются сообщения алгоритма STA. Сообщениям типа Configuration BPDU — BPDU-C — соответствует значение 0x00 поля MESSAGE TYPE. Сообщениям типа Topology Change Notification BPDU — BPDU-TCN — соответствует значение 0x80 поля MESSAGE TYPE.
- Поле FLAGS занимает один байт в BPDU-сообщении и предназначено для кодирования сигналов, которыми при необходимости могут обмениваться соседние мосты. Наличию флага в сообщении Configuration BPDU соответствует значение 1 одного из битов данного поля. Протокол STP IEEE 802.1D использует только два типа флагов. Флаг TC (Topology Change — изменение топологии) кодируется единичным значением младшего бита 5-го байта сообщения Configuration BPDU, которое передает прозрачный мост при обнаружении изменения состояния системы. Флаг TCA (Topology Change Acknowledgment — подтверждение сообщения об изменении топологии) используется для того, чтобы обеспечить гарантированную доставку информации об изменении конфигурации системы до корневого моста. Далее будет показано, как применение флагов обеспечивает существенное сокращение времени переходных процессов при изменениях активной топологии Spanning Tree.
- В поле ROOT ID (сокращенно — RID) размещается идентификатор корневого моста. Этот идентификатор занимает 8 байтов. В двух старших бай-

тах поля RID размещается значение приоритета корневого моста. Это значение, в свою очередь, подразделяется на два поля — четыре старших бита образуют значение относительного приоритета моста, а остальные 12 бит могут быть использованы для размещения расширения идентификатора системы. Установленному по умолчанию значению приоритета соответствует величина 32768. Поэтому для управления процедурой выбора корневого моста системным администратором рекомендуется использовать значения из диапазона 0—61440 назначаемые с шагом 4096. Последующие 6 байтов поля RID представляют собой MAC-адрес корневого моста.

- Поле ROOT PATH COST занимает 4 байта в кадре BPDU и представляет стоимость кратчайшего пути от того моста, который является источником сообщения, до корневого моста.
- В поле BRIDGE ID (BID) размещается идентификатор моста, который является источником данного сообщения. Этот идентификатор занимает 8 байтов в кадре BPDU и формируется по тем же правилам, что и идентификатор корневого моста.
- В поле PORT ID (PID) сообщения BPDU размещается идентификатор порта, через который последний мост передал данное сообщение. Идентификатор занимает два байта, причем четыре старших разряда старшего байта используются для указания относительного приоритета порта в пределах коммутатора. Предпочтение при выборе корневого или назначенного порта отдается порту с меньшим значением идентификатора. Установленному по умолчанию значению приоритета порта обычно соответствует величина 128, поэтому для управления процедурой выбора порта системным администратором рекомендуется использовать значения из диапазона 0—240 назначаемые с шагом 16. Младшие 12 разрядов поля PORT ID используются для указания порядкового номера порта на коммутаторе.
- Поле MESSAGE AGE (возраст сообщения) занимает два байта в BPDU-сообщении и предназначено для фиксирования времени существования сообщения в сети. Каждый мост модифицирует содержимое этого поля всех проходящих через него сообщений путем добавления значения задержки в канале, по которому оно было получено. Значение этого и всех последующих интервалов времени определяются с точностью 1/256 доли секунды в соответствии со значениями, установленными для корневого моста.
- Поле MAXIMUM AGE (Максимальный возраст сообщения) устанавливает максимальное время существования (актуальности) данных, передаваемых данным сообщением. В том случае, если значение поля MESSAGE AGE

у полученных или хранимых данных превышает значение MAXIMUM AGE, данные считаются утратившими силу и подлежат замене. Этот параметр определяет максимальную величину интервала времени, в течение которого может быть использована информация, полученная в одном сообщении BPDU.

- Значение поля HELLO TIME сообщения BPDU определяет период следования конфигурационных сообщений. Обычно это значение соответствует интервалу времени от 1 до 4 сек.
- Значение поля FORWARD DELAY определяет величину интервала времени, который должен предшествовать переходу моста в новое состояние при изменении конфигурации системы. Эта задержка предназначена для предотвращения возникновения циклических маршрутов во время переходных процессов в сети.

Построение активной топологии

Для того чтобы принимать участие в выполнении процедуры Spanning Tree, каждый мост должен для каждого из своих портов определять и сохранять значения следующих параметров системы:

- идентификатор корневого моста — RBI (Root Bridge Identifier);
- стоимость кратчайшего пути до корневого моста (Root Path Cost);
- идентификатор ближайшего моста, через который проходит этот путь;
- идентификатор порта данного моста, через который проходит этот путь.

Формирование структуры Spanning Tree производится в ходе процесса самоорганизации замкнутой системы. Во время этого процесса соседние мосты обмениваются информацией и определяют указанные выше значения, анализируя соответствующие поля сообщений BPDU-C, принимаемых на данный порт. Каждое значение снабжается меткой времени, значение которой определяется моментом приема на порт и значением поля MESSAGE AGE соответствующего сообщения. Если вновь полученное сообщение содержит аналогичные или лучшие значения параметров, старые значения заменяются новыми и переопределяются значения соответствующих меток времени. В том случае, если метка времени не будет переопределена до истечения временного интервала, установленного значением поля MAXIMUM AGE, текущее значение параметра считается утратившим силу.

Изначально, в момент включения, любой мост считает, что именно он является корневым мостом. Каждый мост, считающий себя корневым, передает с интервалом, определяемым значением поля HELLO TIME, сообщения типа BPDU-C через все свои порты.

В этих сообщениях размещается следующая информация, на основании которой производится определение активной топологии ЛВС:

- идентификатор моста, считающего себя корневым;
- идентификатор моста, передавшего данное сообщение;
- идентификатор порта, через который было отправлено данное сообщение;
- стоимость маршрута до корневого моста.

В сообщениях BPDU-C моста, который считает себя корневым, значения двух первых идентификаторов совпадают, стоимость маршрута до корневого моста и значение поля MESSAGE AGE устанавливаются равными 0. Значения полей MAXIMUM AGE, HELLO TIME и FORWARD DELAY устанавливаются в соответствии с индивидуальными настройками данного моста. Период отправки сообщений BPDU-C не должен быть меньше значения, определяемого параметром Hold Time. В табл. 8.4 приведены рекомендованные IEEE 802.1D значения и диапазоны изменения описанных выше параметров. Все интервалы времени, представленные в табл. 8.4, указаны в секундах.

Таблица 8.4. *Рекомендованные значения таймеров алгоритма Spanning Tree*

Название таймера	Рекомендованное значение (сек)	Фиксированное значение (сек)	Диапазон изменения (сек)
Hello Time	2,0	—	1,0—10,0
Max Age	20,0	—	6,0—40,0
Forward Delay	15,0	—	4,0—30,0
Hold Time	—	1,0	—

Если мост, считающий себя корневым, получает сообщение BPDU-C со значением идентификатора корневого моста меньшим, чем его собственный, то он перестает формировать собственные сообщения и начинает транслировать сообщения моста с меньшим значением идентификатора. Кроме того, он соответствующим образом изменяет содержимое внутреннего идентификатора корневого моста. Теперь мост будет транслировать только сообщения BPDU-C с аналогичным значением идентификатора корневого моста. Сообщения с большим значением будут игнорироваться, а получение сообщения с меньшим значением приведет к повторению процедуры переопределения корневого моста. Таким образом, через некоторое время в ЛВС остается только один мост, передающий сообщения BPDU-C через все свои порты, который и становится корневым мостом. Остальные мосты транслируют сообщения

BPDU-C, полученные от корневого моста, модифицируя их содержимое следующим образом:

- значения полей BID и PID устанавливаются в соответствии с установленными для данного моста и порта значениями;
- значение поля MESSAGE AGE увеличивается описанным выше образом на величину, максимальное значение которой ограничено IEEE 802.1D диапазоном 1—4 сек;
- Значение поля ROOT PATH COST передаваемого сообщения вычисляется как сумма значения аналогичного поля сообщения принятого от корневого моста, и значения PATH COST, установленного для порта, через который передается сообщение. Таким образом, в поле ROOT PATH COST накапливается значение стоимости пути до корневого моста, пропорциональной задержке при передаче сообщения.

Все сообщения BPDU-C, поступающие на порты моста со значением идентификатора корневого моста, или иначе RBI, большим, чем хранимое значение RBI, мост игнорирует. Остальные сообщения мост обрабатывает по специальному алгоритму, чтобы определить корневой порт, через который он связан с корневым мостом кратчайшим маршрутом. В качестве критерия оптимальности маршрута мост в данном случае использует значение поля ROOT PATH COST принятого сообщения. Очевидно, что в данном случае это будет тот порт, на который приходит наилучшее по значению стоимости корневого пути сообщение BPDU-C. В том случае, если несколько портов коммутатора получают сообщения с одинаковым значением поля ROOT PATH COST, предпочтение при выборе корневого моста отдается порту, на который поступают сообщения от моста с меньшими значениями полей BID и PID. После того, как порт получает статус корневого, сообщения BPDU-C через него не передаются.

Оставшиеся порты коммутатора могут получить статус назначенных портов (designated). Это происходит в том случае, если некоторый некорневой порт коммутатора находится на оптимальном маршруте между данным сегментом и корневым мостом. Этот факт определяется независимо каждым мостом для каждого некорневого порта путем сравнения содержимого передаваемых собственных сообщений BPDU-C и сообщений, принимаемых от других мостов на данный порт. Если значение собственных сообщений BPDU-C окажется лучше, порт получает статус назначенного и используется для передачи трафика ЛВС в данный сегмент. В противном случае мост переводится в выключенное состояние, в котором будет находиться до тех пор, пока на него будут поступать блокирующие сообщения BPDU-C с назначенного порта или моста. Порты, переведенные в пассивное состояние при выполнении STA, называются *резервными портами* (alternative port). Например, в сети, функциональная схема которой приведена на рис. 8.4, в качестве запасных будут выбраны

порт 1 моста SW1, порт 2 моста SW2, порты 2 и 3 моста SW4. Изменение состояния этих портов может быть вызвано изменением структуры ЛВС.

Состояния и режимы портов Spanning Tree

Таким образом, при выполнении алгоритма STA (Spanning Tree Algorithm) порт моста может получить один из трех статусов:

- *корневой* (Root);
- *выбранный* или *назначенный* (Designated);
- *резервный* (Alternative).

Следует отметить, что статус порта определяет только способ формирования и обработки сообщений BPDU. В частности, сообщения BPDU-C передаются только через назначенные порты, а описываемое ниже сообщение BPDU-TCN — только через корневой порт. Кроме того, для каждого порта моста определяется способ обработки кадров, получаемых от абонентов ЛВС. Этот способ определяется в виде режима или состояния порта. В соответствии со стандартом IEEE 802.1D порты моста могут находиться в одном из пяти фиксированных состояний (режимов):

- *режиме блокировки* (Blocking);
- *режиме прослушивания* (Listening);
- *режиме обучения* (Learning);
- *основном режиме* (Forwarding);
- *режиме, когда порт выключен* (Disabled).

Необходимость использования нескольких различных режимов обработки кадров объясняется тем, что алгоритм Spanning Tree выполняется одновременно на многих мостах. Из-за наличия временных задержек при передаче данных в процессе его выполнения могут возникать временные нестабильные конфигурации. В частности, некоторое время в сети может существовать конфигурация, в которой имеется более одного корневого моста. Поэтому процесс нормального функционирования компонентов сети не может начаться сразу после завершения выполнения процедуры Spanning Tree.

На рис. 8.5 приведена диаграмма изменения состояний порта при выполнении процедуры Spanning Tree. Белые цифры на черном фоне обозначают наступление следующих, изменяющих состояние порта, событий:

- (1) — порт переведен администратором во включенное состояние;
- (2) — на порт поступает блокирующее сообщение BPDU-C;
- (3) — порт переведен в выключенное состояние администратором или вследствие возникновения в нем неисправности.

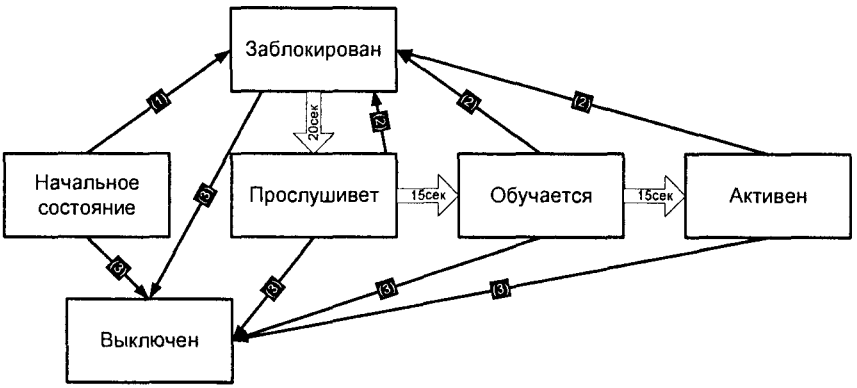


Рис. 8.5. Диаграмма изменения состояний порта при выполнении процедуры Spanning Tree

Режим блокировки

Все порты моста после включения переводятся в режим блокировки. В этом режиме для данного порта мост выполняет следующие действия:

- уничтожает информационные кадры, которые поступают на вход заблокированного порта из подключенного сегмента или от других портов данного моста;
- принимает и обрабатывает сообщения BPDU-C;
- не формирует таблицу фильтрации;
- не передает конфигурационные сообщения.

Таким образом, когда порт моста находится в режиме блокировки, поступающие на него кадры абонентов ЛВС и конфигурационные сообщения никуда не передаются. Однако мост обрабатывает поступающие на данный порт конфигурационные сообщения, и, таким образом, к моменту выхода из данного состояния мост может обладать корректными значениями основных переменных алгоритма Spanning Tree.

Режим прослушивания

В это состояние порт переводится в том случае, если его включение повлечет изменение существующей конфигурации. Порт моста, который включается в работающую сеть, необязательно должен формировать собственные сообщения BPDU для того, чтобы установить, что он не способен претендовать на звание назначенного для подключенного сегмента. Аналогичным образом можно установить, что данный порт может получить статус назначенного порта для сегмента. Именно в этом случае целесообразен перевод данного порта из состояния блокировки в состояние прослушивания. В этом режиме для данного порта мост выполняет следующие действия:

- уничтожает информационные кадры, которые поступают на вход заблокированного порта из подключенного сегмента или от других портов данного моста;
- принимает, обрабатывает и формирует конфигурационные сообщения;
- не формирует таблицу фильтрации.

Таким образом, в режиме прослушивания порт по-прежнему не пропускает через себя кадры абонентов ЛВС, однако может формировать конфигурационные сообщения и, следовательно, участвовать в изменении активной топологии ЛВС. Для того чтобы изменение активной топологии ЛВС, вызванное включением данного порта, завершилось на всех мостах системы, требуется некоторый интервал времени. Поскольку в течение этого интервала активная топология ЛВС может быть неустойчивой, нет смысла формировать записи в таблице фильтрации моста по данному порту.

Режим обучения

При переводе порта в режим прослушивания запускается счетчик времени — Forward Delay Timer. Если к моменту истечения временного интервала, определяемого данным таймером, порт по результатам выполнения процедуры Spanning Tree не будет переведен в блокированное состояние, он автоматически переходит в режим обучения.

В этом режиме для данного порта мост выполняет следующие действия:

- уничтожает информационные кадры, которые поступают на вход заблокированного порта из подключенного сегмента или от других портов данного моста;
- принимает, обрабатывает и формирует конфигурационные сообщения;
- формирует таблицу фильтрации — базу данных MAC-адресов на основании анализа адресов источников из подключенного сегмента.

В режиме обучения порт по-прежнему не пропускает через себя кадры абонентов ЛВС, однако подготавливает необходимую базу данных для того, чтобы делать это в будущем. Значение интервала времени, в течение которого порт находится в состоянии обучения и состоянии прослушивания, определяется значением поля FORWARD DELAY сообщений BPDU-C. Если в течение этих интервалов времени на порт поступит блокирующее сообщение, то он незамедлительно будет переведен в состояние "Заблокирован".

Активный режим

Завершение режима обучения производится автоматически по истечении временного интервала счетчика Forward Delay Timer. После этого порт пере-

водится в активный режим, который иначе называется Forwarding. В этом режиме для данного порта мост выполняет следующие действия:

- обрабатывает информационные кадры, которые поступают на вход данного порта от других портов данного моста;
- принимает, обрабатывает и формирует конфигурационные сообщения;
- формирует таблицу фильтрации.

Таким образом, в основном режиме порт способен выполнять весь комплекс действий по обеспечению информационного обмена.

Выключенное состояние

В этот режим порт может быть переведен по инициативе системного администратора или при обнаружении полной или частичной неработоспособности данного порта по результатам самотестирования. Порт, который находится в выключенном состоянии, не принимает участие в выполнении информационного обмена и в обмене сообщениями протокола STP.

Изменение активной топологии Spanning Tree

Причинами изменения установленной конфигурации сети могут быть:

- появление нового моста или порта;
- возникновение неисправности или выключение одного из действующих мостов или портов;
- вмешательство системного администратора, изменившего параметры STA.

Ранее было показано, как при обмене сообщениями BPDU-с производится формирование активной топологии ЛВС. Изменение активной топологии ЛВС при использовании алгоритма STA производится автоматически — порт, на который перестают поступать блокирующие сообщения от назначенного порта другого моста, будет переведен в активное состояние. Если на корневой порт моста перестанут поступать сообщения BPDU с от корневого моста, то мост будет принимать участие в выборах нового корневого моста и т. д. При переходе от одной топологии к другой некоторые из портов могут поменять свое состояние — порт, заблокированный ранее, может стать активным, и наоборот. Однако для успешного продолжения информационного обмена после изменения текущей конфигурации должно быть произведено соответствующее изменение таблицы фильтрации. Следует отметить, что алгоритм Spanning Tree не имеет специального механизма, который обеспечивает автоматическое преобразование информационных таблиц прозрачных мостов при изменении конфигурации ЛВС. Вследствие этого в течение максимального времени жизни в системе могут сохраняться "фантомные" мар-

шруты, которые проходят через несуществующие в настоящий момент соединения.

В качестве примера можно рассмотреть сеть, структура которой представлена на рис. 8.6. При разрушении маршрута, который соединял мост SW1 с мостом SW4, связность сети нарушается и прекращается информационный обмен между рабочими станциями PC1 и PC2. Соответствующее состояние сети приведено на рис. 8.6, *а*. Для восстановления связности выполняется процедура Spanning Tree. В результате выполнения этой процедуры порт, который связывает мост SW4 с мостом SW2, переводится в активное состояние. Модифицированная в соответствии с описанными выше изменениями состояний портов активная топология сети приведена на рис. 8.6, *б*.

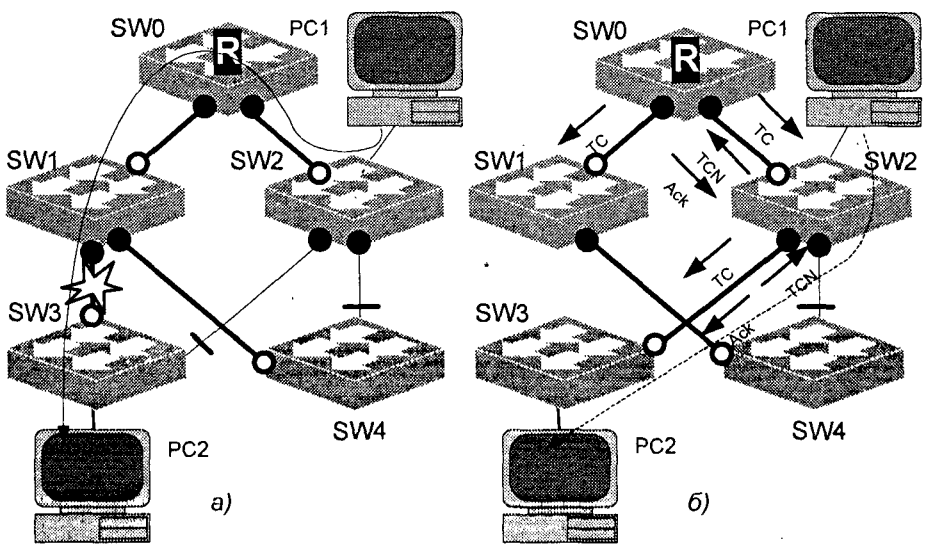


Рис. 8.6. Изменение активной топологии при выполнении процедуры Spanning Tree

Однако для того, чтобы мост SW2 начал передавать кадры, адресованные станцией PC1 станции PC2 по новому маршруту, нужно, чтобы в его таблице фильтрации была уничтожена запись, в соответствии с которой кадры, адресованные станции PC2, нужно направлять через мост SW0. При обычном развитии событий эта запись из таблицы моста SW2 исчезнет не раньше, чем истечет временной интервал Max Age (значение, установленное по умолчанию, составляет 300 сек). Для того чтобы обеспечить оперативное реагирование компонентов сети на изменение ее конфигурации, применяется специальный механизм, который называется *оповещением об изменениях топологии* — Topology Change Notification.

Суть этого механизма состоит в резком уменьшении времени сохранения записей в информационной базе моста в период изменений конфигурации системы. Мост, который фиксирует изменение конфигурации сети, по изменению состояния своих активных портов (на приведенной схеме таким мостом является SW4), формирует специальное сообщение BPDU-TCN (Topology Change Notification). Это сообщение через свой корневой порт мост направляет в назначенный порт вышестоящего коммутатора (на рис. 8.6, *б* таким коммутатором будет SW2). Передача этого сообщения производится до тех пор, пока вышестоящий мост не подтвердит получение этого сообщения передачей сообщения BPDU-C с установленным флагом Topology Change Acknowledge (подтверждение изменения топологии). Таким же образом производится гарантированная передача этого сообщения далее до тех пор, пока оно не достигнет корневого моста. Когда это сообщение достигает корневого моста, он начинает формировать свои регулярные сообщения BPDU-C с установленным флагом Topology Change. В течение интервала времени, когда такие сообщения передаются, все мосты должны использовать значение интервала Forward Delay для ограничения времени жизни динамических записей в таблице фильтрации. Поскольку установленное по умолчанию значение Forward Delay (15 сек) в 20 раз меньше значения стандартного Ageing Time (300 сек), в течение этого интервала таблица фильтрации быстро высвобождается от старых записей, что обеспечивает возможность выполнения оперативной реконфигурации системы.

Таким образом, использование алгоритма Spanning Tree и протокола STP (Spanning Tree Protocol) обеспечивает автоматическое формирование и изменение активной топологии ЛВС. Вмешательство администратора в процесс построения активной топологии обычно требуется только для определения или изменения положения корневого моста. Однако классический алгоритм Spanning Tree и протокол STP имеют ряд недостатков, к которым можно отнести:

- большое время переходных процессов при изменении конфигурации сети;
- возникновение переходных процессов при подключении и отключении отдельного абонента ЛВС.

Последний из указанных недостатков приводит к тому, что любая рабочая станция, подключенная к порту прозрачного моста, может начать информационный обмен только по истечении временного интервала 50 сек (Max Age + Forward Delay + Forward Delay). Кроме того, подключение и отключение этой станции инициирует выполнение процедуры Topology Change, что вызывает кратковременное увеличение трафика во всех сегментах сети вследствие обнуления таблиц фильтрации у всех прозрачных мостов. Наличие этих и

других недостатков объясняется тем, что спецификация Spanning Tree была разработана более 20 лет назад и оставалась с тех пор практически неизменной. В наши дни, когда требования ко всем характеристикам ЛВС радикально изменились, недостатки алгоритма и протокола существенно снижают эффективность использования сетевых ресурсов ЛВС, и в некоторых случаях могут сделать невозможным применение классической версии Spanning Tree для формирования активной топологии ЛВС.

Примечание

Некоторые производители коммуникационного оборудования модифицировали протокол путем внедрения в него дополнительных функций. К подобным решениям следует отнести функции PortFast, UplinkFast, BackboneFast, которые могут быть использованы на коммутаторах Catalyst компании Cisco Systems. Эта и подобные разработки других компаний позволили проверить технические решения и накопить необходимый опыт для создания нового варианта спецификации Spanning Tree.

Быстрый алгоритм Spanning Tree IEEE 802.1W

Ранее было показано, что алгоритм STA IEEE 802.1D, основные принципы построения которого были сформулированы в конце прошлого века, позволяет достаточно успешно решать поставленные перед ним задачи — строить не содержащие циклов структуры ЛВС. Основным и достаточно существенным недостатком этого алгоритма можно считать то, что построение новой активной топологии при изменении конфигурации ЛВС может иногда занимать достаточно много времени (до 50 сек), в течение которого сеть полностью или частично не функционирует из-за потери передаваемых кадров на портах, находящихся в промежуточных состояниях (Listening, Learning). В настоящее время, когда скорость передачи данных в ЛВС выросла в 1 000 раз, и существенно возросли требования к стабильности ее функционирования, этот недостаток становится еще более серьезным. Кроме того, классический алгоритм STA создавался в то время, когда подавляющее большинство ЛВС было построено на разделяемых средах передачи данных (общая шина технологий IEEE 10 Base 5, 10 Base 2). Современные ЛВС построены исключительно на средах, обеспечивающих передачу данных по принципу "точка-точка", что в некоторых случаях может упростить и ускорить процесс построения активной топологии STA. Для того чтобы преодолеть известные недостатки классического алгоритма STA, IEEE предложил к использованию новую спецификацию 802.1W, которая получила название протокола *RSTP* (Rapid Spanning Tree Protocol) — "быстрого" протокола Spanning Tree.

Основные принципы RSTP

По сравнению с классическим алгоритмом STA новый алгоритм *RSTA* (Rapid Spanning Tree Algorithm) обеспечивает существенное уменьшение времени построения активной топологии сети, основанной на прозрачных мостах. Ускорение обеспечивается благодаря изменениям, внесенным в процедуру обмена информационными сообщениями BPDU-C. При использовании новой процедуры обмена отпадает необходимость использования задержек для изменения состояния порта, поскольку такие изменения производятся сразу после согласования параметров между соседними мостами.

В то же время основные компоненты протокола RSTP: назначение корневого моста, используемые типы портов, структура сообщений и т. д., не претерпели существенных изменений, что обеспечивает возможность построения гибридных конфигураций, в которых мосты, поддерживающие спецификацию 802.1W, применяются вместе с мостами классической версии Spanning Tree, т. е. спецификации 802.1D.

Формирование сообщений RSTP

Одно из основных отличий протокола RSTP от его предшественника заключается в изменении способа формирования конфигурационных сообщений. Как мы помним, сообщения Configuration BPDU (BPDU-C) в протоколе STP может формировать только корневой мост. Остальные порты ЛВС при этом только транслируют полученные от корневого моста сообщения через свои назначенные порты. Использование подобной схемы оправдано в сетях, построенных на разделяемых средах передачи данных (коаксиальный кабель), когда передача производится по схеме "один-многим". Подавляющее большинство современных сетей используют схему "точка-точка" и неразделяемые среды передачи данных (витая пара, волоконно-оптический кабель). В таких сетях целесообразно использовать децентрализованную схему формирования конфигурационных сообщений, при которой каждый мост формирует эти сообщения независимо и передает их только своим непосредственным соседям. Структура этих сообщений остается при этом практически неизменной, что позволяет обеспечить совместимость с предыдущей версией протокола (Spanning Tree Protocol) и существенно сократить время построения активной топологии ЛВС.

В протоколе RSTP используются два типа управляющих сообщений — Topology Change и Configuration BPDU (BPDU-C). Назначение и структура этих сообщений в основном совпадает с параметрами аналогичных сообщений классического протокола Spanning Tree. Небольшие отличия формата сообщения BPDU-C RSTP от сообщения протокола STP (см. табл. 8.3) вызваны изменениями протокола и включают в себя:

- изменение значения поля VERSION — 02 (шест.);
- изменение значения поля MESSAGE TYPE — 02 (шест.);
- изменение структуры поля FLAGS.

Структура поля FLAGS сообщения BPDU-C протокола RSTP приведена далее в табл. 8.7 Измененное значение поля VERSION служит признаком того, что сообщение сформировано коммутатором, который поддерживает обе версии протокола STP. Значения и способ формирования остальных полей данного сообщения протокола RSTP остались неизменными по отношению к протоколу STP.

Сообщение Topology Change протокола RSTP по своему назначению совпадает с сообщением Topology Change Notification классического протокола STP, но лишь частично. Основное отличие состоит в том, что сообщение Topology Change протокола RSTP передается через все активные порты прозрачного моста, который зафиксировал переход одного из своих портов в режим передачи (Forwarding). Для сравнения напомним, что аналогичное сообщение протокола STP передается только через корневой порт при фиксировании любого изменения состояния порта. Таким образом, в классическом протоколе STP сообщение об изменении топологии, передаваемое некорневым мостом, имеет статус предварительного уведомления. Окончательное сообщение в этом случае формирует корневой мост после того, как он получит это уведомление. Поскольку в протоколе RSTP используется децентрализованная схема формирования сообщений BPDU-C, необходимость в предварительных сообщениях и обеспечении их гарантированной передачи корневому мосту отпала.

Еще одно отличие протокола RSTP состоит в том, что сообщения об изменении топологии формируются только при переходе порта в активное состояние. Выключение порта или его авария, таким образом, не могут вызвать формирование такого сообщения. На первый взгляд такое изменение не кажется вполне обоснованным, однако следует иметь в виду, что основным назначением сообщения об изменении топологии в протоколе STP (Spanning Tree Protocol) является очистка устаревших таблиц фильтрации. Очевидно, что в первую очередь менять эти таблицы нужно тогда, когда в сети появляется новый маршрут передачи данных, а не когда исчезает старый.

Значения параметров протокола RSTP

Номенклатура и значения основных параметров, которые используются в протоколе RSTP, в основном остались неизменными по отношению к протоколу STP для обеспечения их взаимной совместимости. Этим, в частности, объясняется тот парадоксальный факт, что количество таймеров, используемых протоколом RSTP, увеличилось, в то время как их применение в прото-

коле сократилось. В табл. 8.5 приведены рекомендованные значения и диапазоны изменения таймеров, которые используются в протоколе RSTP. Анализ таблицы показывает, что значения и задачи таймеров Hello Time, Forward Delay, Max Age остались неизменными.

Таблица 8.5. *Рекомендованные значения таймеров алгоритма RSTP*

Название таймера	Рекомендованное значение (сек)	Диапазон изменения (сек)
Migrate Time	3,0	—
Hello Time	2,0	1,0—2,0
Max Age	20,0	6,0—40,0
Forward Delay	15,0	4,0—30,0
Hold Time	6,0	1,0—10,0

Новый таймер Migrate Time определяет максимальный интервал времени, в течение которого ожидается поступление сообщения BPDU-C на подключенный порт. В том случае, если такое сообщение не поступит на порт в течение этого временного интервала, он получит статус граничного и, следовательно, не будет принимать участие в построении активной топологии сети.

Значение, задаваемое таймером Hold Time, используется в протоколе RSTP для ограничения максимального времени ожидания поступления очередного сообщения BPDU-C — вместо значения Max Age, которое используется для аналогичной цели в протоколе STP.

Еще одно отличие протокола RSTP заключается в изменении диапазона величины Port Path Cost. В классическом варианте протокола STP (Spanning Tree Protocol) стоимость прохождения маршрута через порт представляется целым положительным числом с диапазоном изменения значения от 0 до 65 535. Для представления общей стоимости маршрута в сообщении BPDU-C отводилось 4 байта. Следует также учесть, что величина стоимости передачи трафика через порт прозрачного моста обратно пропорциональна скорости передачи данных через него, и большим значениям скорости передачи данных соответствуют меньшие значения стоимости. Очевидно, что в современных сетях значение Path Cost в лучшем случае будет использовать только половину отведенного для ее размещения в BPDU-C диапазона. Сам по себе этот факт вряд ли мог быть причиной изменения алгоритма формирования Port Path Cost, если бы не существовала еще одна очень важная предпосылка. Дело в том, что скорости передачи данных в современных сетях неуклонно растут и, следовательно, возможность появления более высоких скоростей должна также учитываться в этом алгоритме. Для того чтобы решить обе указанные проблемы одновременно, разработчиками протокола RSTP был пред-

ложен следующий способ формирования значения Port Path Cost и его кодирования в сообщении BPDU-C:

- диапазон изменения величины Port Path Cost согласно протокола RSTP составляет 1—200000000;
- для размещения значения стоимости корневого маршрута в сообщении BPDU-C используется 4 байта.

В табл. 8.6 приведены значения Port Path Cost для существующих и перспективных скоростей передачи данных в ЛВС.

Таблица 8.6. *Рекомендованные диапазоны и значения Port Path Cost протокола RSTP*

Скорость передачи данных	Рекомендованное значение	Рекомендованный диапазон изменения
Менее 100 Кбит/сек	200 000 000	20 000 000–200 000 000
1 Мбит/сек	20 000 000	2 000 000–200 000 000
10 Мбит/сек	2 000 000	200 000–20 000 000
100 Мбит/сек	200 000	20 000–2 000 000
1 Гбит/сек	20 000	2 000–200 000
10 Гбит/сек	2 000	200–20 000
100 Гбит/сек	200	20–2 000
1 Тбит/сек	20	2–200
10 Тбит/сек	2	1–20

Очевидно, что предложенное в новой редакции спецификации решение, с одной стороны, позволяет более эффективно использовать соответствующее информационное поле в сообщении BPDU-C, а с другой — обеспечивает возможность использования алгоритма Spanning Tree в современных и перспективных ЛВС.

Построение активной топологии RSTP

В соответствии с требованиями протокола RSTP и согласно спецификации 802.1W, сообщения BPDU-C формируются каждым мостом с постоянным периодом независимо от того, получает или нет этот мост аналогичные сообщения от других мостов (в том числе от корневого моста). Следует напомнить, что в алгоритме 802.1D мосты только транслировали сообщения, получаемые от корневого моста. Кроме того, внеочередные конфигурационные сообщения формируются в том случае, если меняется состояние моста. При-

менение такой схемы обмена позволило существенно сократить значение интервала времени, в течение которого сохраняются данные, полученные в последнем сообщении BPDU-C от соседнего моста. В то время как классический протокол STP по спецификации 802.1D предписывает сохранение данных, неподтвержденных очередными сообщениями, в течение 20 сек, протокол RSTP требует замены этих данных по истечении 3-х периодов следования конфигурационных сообщений (обычно 6 сек).

Состояния портов моста RSTP

В дополнение к ролям (состояниям) портов, установленных алгоритмом STA, алгоритм RSTA (Rapid Spanning Tree Algorithm) вводит несколько новых. Таким образом, полный список ролей, которые может выполнять порт моста, теперь составляет четыре наименования:

- *корневой порт* (Root Port);
- *назначенный порт* (Designated Port);
- *альтернативный порт* (Alternative Port);
- *резервный порт* (Backup Port).

Правила получения ролей и функции, выполняемые соответствующими портами, для корневого и назначенного порта остались без изменений. Оба эти порта находятся во включенном состоянии и используются для передачи трафика ЛВС. Роли альтернативного или резервного получают порты, заблокированные вследствие получения сообщения BPDU-C лучшего, чем сообщение, которое через них можно было бы отправить. Отличие между ними состоит в том, что роль альтернативного получает порт, заблокированный сообщением, полученным от порта соседнего моста, который выполняет функцию назначенного для подключенного сегмента. Роль резервного получает порт, заблокированный сообщением от того моста, на котором он сам расположен. Порты моста, выполняющие роли альтернативного и резервного, не используются для передачи трафика ЛВС. Необходимость подобного расщепления роли объясняется тем, что при возникновении неисправности на корневом порту моста роль корневого может быть мгновенно передана лучшему среди имеющихся у него альтернативных портов. Причем этот порт может быть сразу переведен в активный режим, поскольку его включение гарантированно не приведет к образованию кольцевого маршрута.

Протокол RSTP также определяет новый статус для портов, которые используются для непосредственного подключения рабочих станций пользователей к прозрачному мосту. Такие порты называются *граничными* (Edge). Они не участвуют в выполнении алгоритма Spanning Tree — через них не передаются конфигурационные сообщения, изменения их состояния не приводят к из-

менению активной топологии. Граничные порты при включении моста сразу переводятся в активное состояние, минуя промежуточные стадии. Статус граничных автоматически получают порты, на которые не поступают сообщения BPDU-C, кроме того, этот статус может быть получен по инициативе администратора. В соответствии с правилами алгоритма RSTA граничный порт, на который поступило любое сообщение BPDU, необратимо теряет статус граничного и становится обычным портом.

Режимы портов моста RSTP

В алгоритме RSTA различается только 3 независимых, по отношению к процедурам обработки кадров абонентов ЛВС, режима, в которых может использоваться порт моста:

- *режим изоляции* (Discarding);
- *режим обучения* (Learning);
- *активный режим* (Forwarding).

Это отличие вызвано отказом от использования временных задержек при переходе порта из одного режима в другой.

Функции, выполняемые портом в режиме обучения (Learning) и активном режиме (Forwarding) алгоритма RSTA, соответствуют функциям одноименных режимов классического алгоритма STA.

Порт моста, находящийся в режиме изоляции (Discarding), уничтожает принимаемые кадры абонентов ЛВС и не формирует записи в таблице фильтрации. В этот режим переводятся порты, получившие при выполнении алгоритма RSTA роль альтернативного или резервного. Отсутствие в RSTA промежуточного состояния аналогичного состоянию прослушивания STA объясняется использованием описываемого далее нового принципа формирования активной топологии.

Согласование активной топологии

Отличие принципа построения активной топологии, используемого в алгоритме RSTA, состоит в том, что решения об изменении статуса портов принимаются по итогам согласования, выполняемого соседними мостами. Для обеспечения такого согласования алгоритм RSTA использует измененную форму конфигурационных сообщений BPDU-C. В основном структура этих сообщений совпадает со структурой аналогичных сообщений протокола STP. Отличие заключается в структуре поля FLAGS, которая приведена в табл. 8.7.

Используя новые флаги сообщений BPDU-C, соседние мосты могут обмениваться информацией о своем текущем статусе и состоянии и, при необходимости, выполнять их оперативное изменение. Например, вследствие измене-

Таблица 8.7. *Структура поля FLAGS сообщения BPDU-C протокола RSTP*

Номер поля	Содержание поля	Номера занимаемых битов
1	TOPOLOGY CHANGE FLAG — флаг изменения топологии	0
2	PROPOSAL FLAG — флаг предложения	1
3	PORT ROLE — указание роли порта	2—3
4	LEARNING FLAG — флаг режима обучения	4
5	FORWARDING FLAG — флаг активного режима	5
6	AGREEMENT FLAG — флаг соглашения	6
7	TOPOLOGY CHANGE ACKNOWLEDGEMENT (TCA) — флаг подтверждения изменения топологии (не используется в RSTP)	7

ния конфигурации сети порт некоторого моста планирует перейти в активное состояние, поскольку он исполняет роль назначенного для подключенного сегмента. Этот порт, однако, не может быть включен мгновенно, поскольку расположенная ниже него часть сети вследствие произошедших изменений может временно содержать циклические маршруты. Тем не менее этот порт может быть включен, если подключенный к нему мост каким-либо образом гарантирует отсутствие таких маршрутов на своих портах и даст соответствующий сигнал.

Практически это выполняется следующим образом: через порт, который мост планирует перевести в активное состояние, он передает сообщение BPDU-C с установленным флагом Proposal (Предложение). Получив такое сообщение, соседний мост выполняет процедуру синхронизации путем перевода всех остальных своих активных не граничных портов в состояние изоляции — Discarding. Достигнув этого состояния, соседний мост формирует ответное сообщение BPDU-C с установленным флагом Agreement (Соглашение). После получения такого сообщения первый мост переводит свой порт в активное состояние. Что касается второго моста, то указанная выше процедура выполняется заново, вследствие чего часть заблокированных ранее портов будет переведена в активное состояние, а те порты, которые не получат статус назначенных — останутся выключенными. Таким образом, "волна" предложений и соглашений прокатится по сети, оставляя после себя скорректированную активную топологию.

Следует также отметить, что указанная выше процедура может быть успешно выполнена только в том случае, если активизируемый порт подключен к сегменту с неразделяемой средой передачи ("точка-точка"). В противном случае

для перевода порта в активное состояние должна быть использована стандартная процедура классического алгоритма STA.

Изменение активной топологии RSTP

Сообщения об изменениях топологии сети в алгоритме RSTA, в отличие от классического алгоритма STA, где их может передавать только корневой мост, передаются децентрализованно. Поэтому в алгоритме RSTA не используются извещающие сообщения BPDU-TCN и флаг TCA. Сообщения об изменениях топологии сети с установленным флагом Topology Change, тот мост, на котором было зафиксировано изменение, передает через все свои назначенные порты и, при необходимости, через корневой порт. При получении такого сообщения каждый из соседних мостов должен очистить содержимое своей таблицы фильтрации для всех не граничных портов, кроме того, на который было получено сообщение BPDU-C с установленным флагом Topology Change.

На рис. 8.7, *а* приведен пример изменения активной топологии ЛВС с использованием алгоритма Rapid Spanning Tree. На рисунке буквой "А" в белом прямоугольнике отмечен порт, через который с этого моста должны направляться кадры, адресованные PC1. В данном случае мост SW3, на котором произошло изменение конфигурации, направляет мосту SW2 сообщение об изменении топологии при переходе своего порта 2 во включенное состояние. При получении этого сообщения мост SW2 очищает свою таблицу фильтрации, удаляя из нее ставшую неактуальной запись о достижимости через порт 1 станции с MAC-адресом А (рис. 8.7, *б*). Мост SW2, в свою очередь, передает аналогичное сообщение дальше, через свои порты 1 и 2, что приводит к оперативному изменению таблиц фильтрации на всех мостах системы. Следует отметить, что при получении сообщения об изменении конфигурации системы очищается только часть содержимого таблицы фильтрации, не связанная с портом, на который это сообщение было получено.

В связи с этим в ЛВС, структура которой приведена на рис. 8.7, исходное содержимое таблицы фильтрации изменится у всех мостов, за исключением SW3 и SW4. Таблица фильтрации SW3 останется неизменной потому, что именно этот мост сформировал сообщение об изменении топологии. Таблица фильтрации SW4 останется неизменной потому, что сообщение об изменении топологии поступает на SW4 именно на тот порт, через который должны доставляться кадры станции PCA.

Таким образом, использование модифицированного алгоритма формирования сообщений об изменении топологии позволяет существенно сократить время переходных процессов при изменении топологии сети и избежать временных ее перегрузок, вызванных полной очисткой таблиц фильтрации.

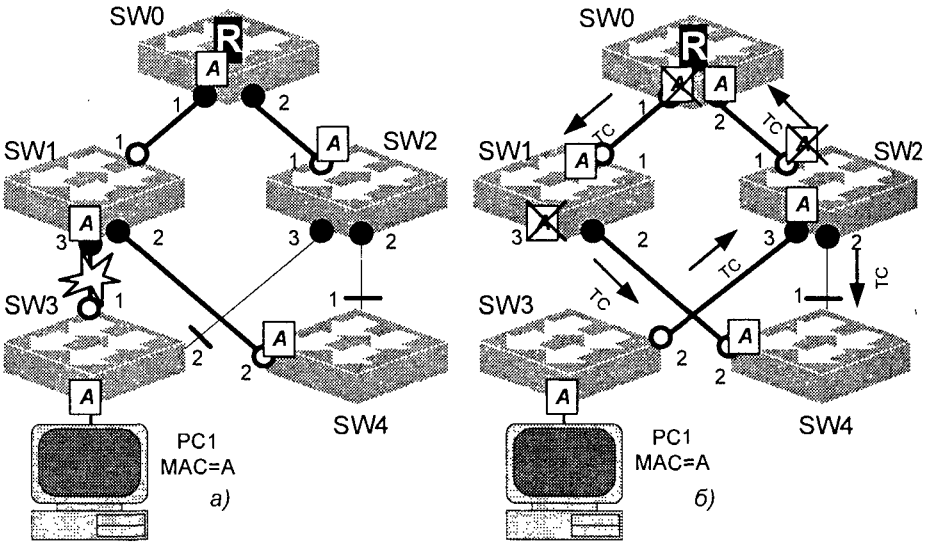


Рис. 8.7. Изменение активной топологии при выполнении процедуры RSTP

Как было показано ранее, применение протокола и алгоритма RST обеспечивает существенное повышение эксплуатационных характеристик ЛВС. Кроме того, использованные в алгоритме изменения и дополнения позволят успешно применять его не только в современных, но и в будущих ЛВС с существенно более высокими скоростями передачи данных. Новая редакция протокола STP ("быстрого" STP) — протокол RSTP — в настоящее время используется в качестве основного, и его поддержка является обязательной для выпускаемого вновь оборудования. В то же время новая версия протокола совместима с предыдущей версией, что обеспечивает возможность построения смешанных систем, в которых только часть мостов поддерживает протокол RSTP. Как и классический протокол STP, протокол RSTP практически не требует вмешательства администратора и обеспечивает автоматическое построение активной топологии ЛВС.

Многоплановые протоколы Spanning Tree

Классический протокол STP и его современная редакция — RSTP, как это было показано ранее, обеспечивают построение активной топологии ЛВС путем исключения из общего связующего дерева (Common Spanning Tree — CST) дублирующих путей передачи данных. Таким образом, если в ЛВС существуют дублирующие резервные каналы, они могут быть использованы для передачи данных только при выходе из строя основных каналов. Следовательно, эти вполне исправные и, как правило, высокоскоростные каналы

будут практически постоянно выключены из функционирования, в то время как основные каналы, может быть, не справляются с большими объемами передаваемых через них данных. Очевидно, что подобный способ резервирования нельзя считать достаточно эффективным, поскольку имеющиеся в распоряжении совокупные вычислительные ресурсы используются только наполовину своих возможностей.

Если принять во внимание то, что подавляющее большинство современных ЛВС разделены на виртуальные сети, крайне привлекательной представляется идея построения нескольких независимых связующих деревьев (Multiple Spanning Trees — MST) для различных виртуальных сетей. В этом случае можно обеспечить выравнивание нагрузки ЛВС, поскольку каналы, заблокированные для одних VLAN, могут быть использованы для передачи трафика других виртуальных сетей. В настоящее время эта идея может быть реализована путем использования следующих протоколов и технических решений:

- протоколов PVST и PVST+ компании Cisco Systems;
- протокола MSTP IEEE 802.1Q (редакция 2003 г.).

В основе всех этих протоколов лежит идея построения нескольких независимых активных топологий Spanning Tree в пределах одной ЛВС. Каждая из этих топологий не содержит циклических маршрутов и представляет собой план соединения прозрачных мостов ЛВС для передачи трафика одной или нескольких VLAN. Для создания каждого из таких планов применяется классический или модифицированный алгоритм STP, используются обычные или модифицированные сообщения BPDU-C. Именно поэтому такие протоколы могут быть названы *многоплановыми протоколами Spanning Tree*. При правильном построении этих планов можно добиться относительно равномерной загрузки основных и резервных каналов.

Однако несмотря на видимое сходство, все указанные протоколы достаточно сильно отличаются друг от друга. В первую очередь отличия между ними заключаются в способах построения независимых топологий и особенностях организации информационного обмена между прозрачными мостами при выполнении алгоритма. Дело в том, что сами сообщения BPDU-C, вследствие особенностей их формирования, обычно могут распространяться только в пределах одной виртуальной сети. Поэтому основные трудности в реализации многоплановых протоколов STP связаны как раз с организацией распространения и необходимостью модификации структуры сообщения BPDU-C.

Многоплановые протоколы STP Cisco Systems

Приоритет в разработке и внедрению многоплановых протоколов Spanning Tree принадлежит компании Cisco Systems — признанному лидеру в произ-

водстве телекоммуникационного оборудования и создании новых информационных технологий. Именно эта компания предложила первый вариант спецификации многопланового протокола *PVST* (Per-VLAN Spanning Tree Protocol) и внедрила его в свои коммутаторы Cisco Catalyst. Отличительной особенностью и обязательным требованием к реализации этого протокола является использование частной спецификации ISL (Inter Switch Link) Cisco Systems для кодирования принадлежности к VLAN. Впоследствии компания представила и в настоящее время использует доработанный вариант своего протокола, который имеет название *PVST+*. Последняя версия протокола обеспечивает возможность совместного использования коммутаторов, поддерживающих спецификации ISL и IEEE 802.1Q.

Протокол PVST

Протокол *PVST* (Per-VLAN Spanning Tree Protocol) обеспечивает построение и использование на коммутаторе независимых процессов протокола STP (Spanning Tree Protocol) для каждой из сконфигурированных на нем виртуальных сетей. Каждый из магистральных портов такого коммутатора принимает, обрабатывает и формирует стандартные конфигурационные сообщения BPDU-C отдельно для каждой из VLAN, трафик которых через него передается. В результате обмена этими сообщениями порт может перейти в активное состояние для некоторых из VLAN и остаться в заблокированном состоянии для трафика других виртуальных сетей. Поскольку протокол PVST предполагает использование внешней схемы ISL для маркирования кадров, то для его реализации в каждой из VLAN классический протокол STP может быть использован в PVST без каких-либо изменений алгоритма. При этом, естественно, остаются неизменными форматы и алгоритмы формирования всех сообщений протокола STP. Основным недостатком протокола PVST является невозможность его применения в тех локальных сетях, где используются различные схемы кодирования принадлежности кадров к VLAN (ISL и IEEE 802.1Q).

Протокол PVST+

Основной недостаток PVST устранен в более поздней версии протокола — PVST+, которая допускает построение нескольких PVST-регионов, связанных между собой коммутаторами, на которых протокол PVST не поддерживается. При этом PVST-информация передается от одного региона к другому через тоннель, поверх протокола MSTP (IEEE 802.1Q). Общим и наиболее существенным недостатком протоколов PVST и PVST+ является малая эффективность использования вычислительных ресурсов коммутатора. Дело в том, что нагрузка на центральный процессор и требования к объему используемой памяти запоминающего устройства для этих протоколов растут про-

порционально количеству активных VLAN, определенных на коммутаторе. В крупных ЛВС, где количество виртуальных сетей может достигать нескольких сотен, эта особенность может оказать негативное влияние на общую производительность и устойчивость функционирования ЛВС.

Протокол MSTP (IEEE 802.1Q)

Универсальный многоплановый протокол Spanning Tree — *MSTP* (Multiple Spanning Tree Protocol) представляет собой единый комплекс процедур, которые могут быть использованы в ЛВС, построенных на прозрачных мостах, с тем, чтобы обеспечить повышение надежности передачи данных и эффективности использования оборудования.

Алгоритм протокола MSTP объединяет в себе алгоритмы протоколов STP и RSTP, позволяет организовать смешанные вычислительные структуры, построенные на оборудовании различных производителей, благодаря использованию различных способов построения покрывающего дерева:

- Common Spanning Tree (CST) Protocol (Clause 8 of IEEE Std 802.1D, 1998 Edition);
- Rapid Spanning Tree Protocol (RSTP) (Clause 17 of IEEE Std 802.1D, 2004 Edition).

Основные понятия и определения MSTP

Так же, как и описанные ранее алгоритмы, алгоритм MST (Multiple Spanning Tree) обеспечивает возможность автоматического построения и динамической реконфигурации активной топологии ЛВС таким образом, что каждый из абонентов в любой момент времени был бы связан с любым другим абонентом этой сети только одним из возможных маршрутов.

Если в сети присутствуют один или несколько резервных каналов, то в ней может быть реализовано несколько вариантов построения активной топологии. На рис. 8.8, *а* приведена функциональная схема ЛВС с дублирующими каналами передачи данных.

В зависимости от расположения корневого моста для такой ЛВС могут быть построены несколько вариантов активной топологии. Некоторые из таких вариантов приведены на рис. 8.8, *б*, *в* и *г*. Несмотря на довольно большое количество различных вариантов, следует отметить, что целесообразными являются лишь очень немногие из них. Например, в том случае, если SW1 и SW2 являются высокоскоростными коммутаторами, связанными между собой при помощи высокоскоростного канала, вариант, помеченный на рис. 8.8, *г*, явно не будет признан целесообразным.

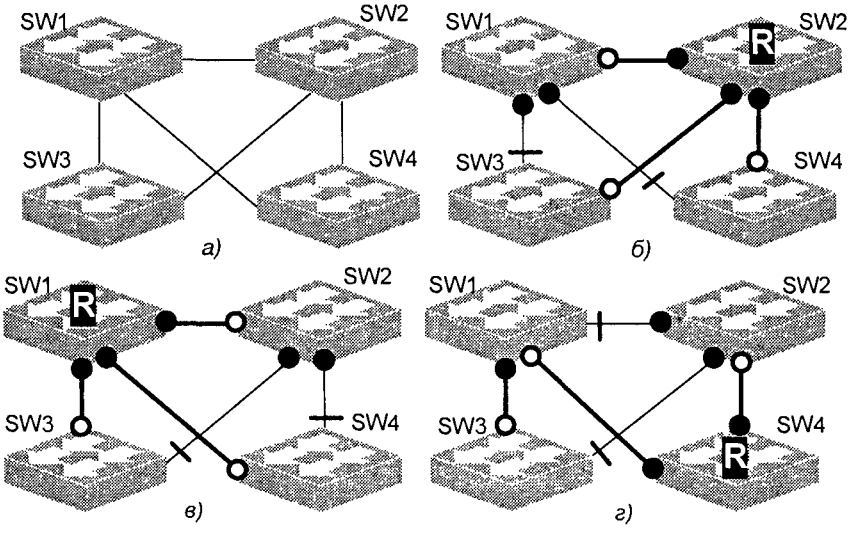


Рис. 8.8. Варианты построения активной топологии ЛВС

Определение

Инстанция (план) — это один из вариантов построения активной топологи ЛВС, предназначенный для передачи трафика одной или нескольких VLAN.

Таким образом, для каждой инстанции в соответствии с требованиями классического протокола STP или протокола RSTP определяется свой вариант построения топологии. Все виртуальные сети ЛВС распределяются между инстанциями произвольным образом, однако при этом любая виртуальная сеть может быть представлена только в одной инстанции. Например, возможен такой вариант распределения, при котором все виртуальные сети принадлежат одной инстанции — этот вариант называется *общее связующее дерево — CST* (Common Spanning Tree).

Для обеспечения взаимодействия с предыдущими версиями протокола STP и удобства администрирования, алгоритм MST предусматривает организацию в ЛВС *многоплановых регионов — MR* (Multi Instance Region) и MST-Region (Multi Spanning Tree Region). Внутри каждого из таких регионов возможно построение нескольких независимых планов Spanning Tree — *MSTI* (Multiple Spanning Tree Instance) для групп виртуальных сетей.

Определение

Регионом в протоколе MSTP называют группу прозрачных мостов, для которых выполняются единые правила распределения VLAN между инстанциями.

Для передачи управляющих сообщений протокола и обеспечения взаимодействия с классическим алгоритмом STA, протокол MSTP использует общее связующее дерево (CST). Каждый прозрачный мост MSTP должен участвовать в построении активной топологии, соответствующей общему Spanning Tree плану ЛВС — CST, т. е. формировать и обрабатывать сообщения BPDU соответствующего формата. Построенный таким образом и размещенный территориально внутри MR-региона фрагмент общего дерева называется внутренним деревом Spanning Tree — *IST* (Internal Spanning Tree). В дополнение к этому, коммутаторы, находящиеся внутри MST-регионов, дополнительно могут участвовать в построении внутренних планов региона MSTI (Multiple Spanning Tree Instance) Spanning Tree для определенных в этом регионе блоков VLAN, каждому из которых соответствует свой вариант активной топологии соответствующего фрагмента ЛВС.

С точки зрения коммутаторов, не поддерживающих протокол MSTP, каждый регион может быть представлен виртуальным коммутатором, функционирующим в полном соответствии с требованиями классического протокола STP (CST — Common Spanning Tree, общее связующее дерево).

Протокол MSTP использует единый формат конфигурационных сообщений для всех вариантов его реализации, поэтому структура начальной части сообщений BPDU одинакова для CST, RST и MST, следовательно, сообщения, обеспечивающие построение общего дерева, адекватно обрабатываются как внутри MR, так и за их пределами. Очевидно, что при этом обеспечиваются следующие возможности:

- построение не содержащих циклических маршрутов активных топологий для каждой из выделенных групп виртуальных сетей внутри региона;
- построение не содержащей циклических маршрутов активной топологии для всей ЛВС в целом;
- автоматическое распознавание границ региона и согласование типа реализуемого протокола Spanning Tree (CST/RST/MST);
- обеспечение выравнивания загрузки между группами внутри региона и оперативного изменения конфигурации при выходе из строя и изменении состояния любого компонента ЛВС.

Применение протокола MSTP не требует дополнительных по отношению к классическому протоколу STP настроек активного оборудования ЛВС, однако преимущества от его использования могут быть достигнуты только при наличии единого принципа распределения виртуальных сетей между инстанциями для всех прозрачных мостов региона и единства применяемых при этом идентификаторов.

Примечание

Следует также отметить, что алгоритм MST не включает в себя процедуры, обеспечивающие автоматизацию распределения VLAN между инстанциями, поэтому задачи построения и обслуживания региона должны решаться путем индивидуального администрирования всех входящих в него коммутаторов.

Принципы реализации MSTP

Взаимодействие коммутаторов при выполнении протокола MSTP организуется в соответствии с принципами, принятыми для протоколов STP и RSTP, в основе которых лежит обмен конфигурационными сообщениями. Для выполнения этих алгоритмов мосты снабжаются идентификаторами. Ранее было отмечено, что общий и внутренний алгоритм Spanning Tree — *CIST* (Common & Internal Spanning Tree) выполняется всеми коммутаторами ЛВС. По результатам выполнения этого алгоритма один из мостов приобретает статус корневого моста для общего дерева (CIST-root). В дополнение к этому, каждый из MSTP-коммутаторов может участвовать в формировании активных топологий одного или нескольких независимых планов (инстанций) для выделенных групп виртуальных сетей. Каждому из таких планов соответствует уникальное значение идентификатора плана — *MSTI* (MST Identifier). Распределение виртуальных сетей по планам задается в виде конфигурационной таблицы (MST Configuration Table), которая имеет 4 096 записей (по одной для каждого идентификатора виртуальной сети — VID). Каждая такая запись содержит двухбайтовое значение идентификатора того плана, к которому принадлежит данная виртуальная сеть. Выделенное значение MSTI = 0 в некоторой строке таблицы говорит о том, что соответствующая виртуальная сеть не принадлежит ни к одному из индивидуальных планов, и, следовательно, кадры этой VLAN могут передаваться только через активную топологию, соответствующую общему покрывающему дереву CIST.

Как уже было отмечено, группа непосредственно связанных коммутаторов, имеющих одинаковые таблицы конфигурации планов, образует MST Region — область, в пределах которой для каждого из сформированных планов VLAN могут быть простроены индивидуальные активные топологии. Следует отметить, что в протоколе MSTP для определения принадлежности к региону не используется анализ содержимого конфигурационных таблиц прозрачных мостов вследствие большого размера этих таблиц. Вместо этого, чтобы установить свою принадлежность к региону, в котором находится его непосредственный сосед, прозрачный мост сравнивает значения двух идентификаторов конфигурации — один хранится в его запоминающем устройстве, другой принимается от соседнего коммутатора в сообщении BPDU. Главной частью идентификатора конфигурации является конфигурационный дайджест (Configuration Digest), представляющий собой 16-байтовый числовой

код, полученный путем применения алгоритма *HMAC-MD5* (IETF RFC 2104) с ключом 0x13AC06A62E47FD51F95D2BA243CD0346 к содержимому полной таблицы виртуальных сетей MST.

Во всем остальном алгоритм протокола MSTP имеет лишь незначительные отклонения от классического или быстрого алгоритма Spanning Tree. Все эти изменения, однако, непосредственно связаны именно со спецификой построения множества связующих деревьев внутри региона. Каждое из таких деревьев строится по обычным правилам Spanning Tree с выбором корневого моста, определением корневых и назначенных портов.

При обмене конфигурационными сообщениями в каждом регионе определяется региональный корневой мост общего дерева (CIST Regional Root). Им становится коммутатор, имеющий минимальную стоимость маршрута до CIST-Root.

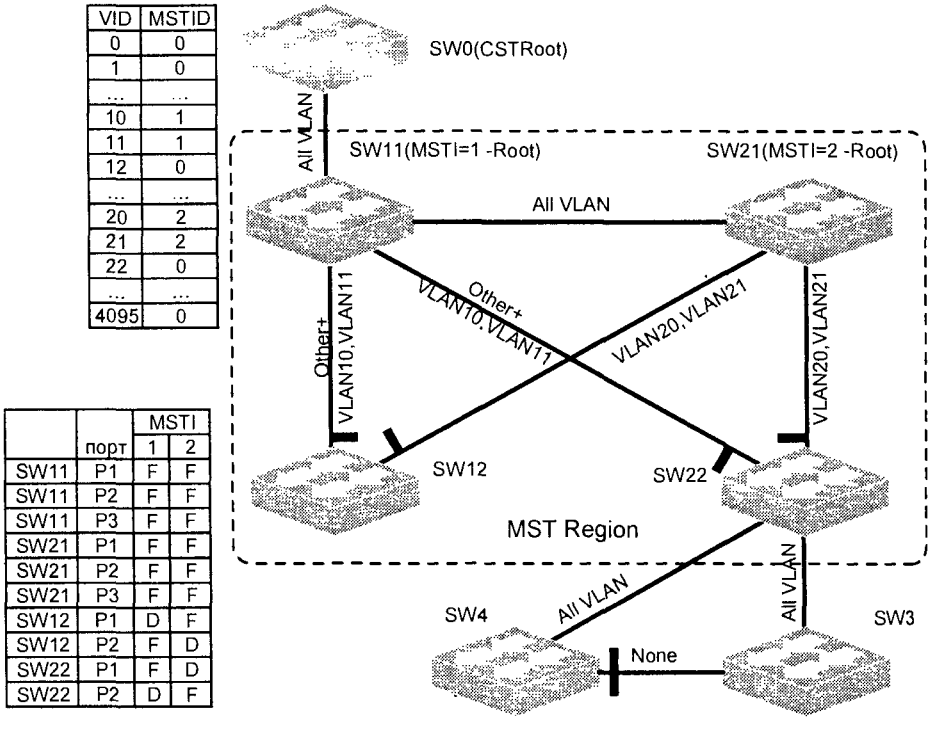
Примечание

В том случае, если локальная сеть состоит только из одного MST-региона, региональный корневой мост одновременно будет являться глобальным корневым мостом общего связующего дерева — CIST-Root.

Для каждого плана (instance) региона также определяется корневой мост (MSTI Regional Root), относительно которого строится независимое дерево передачи трафика соответствующей группы VLAN внутри этого региона.

На рис. 8.9 приведен пример использования протокола MSTP для распределения трафика двух групп виртуальных сетей.

В левом верхнем углу рисунка приведен пример конфигурационной таблицы, в соответствии с которой первый план данного региона (MSTI = 1) образуют VLAN10 и VLAN11, второй план региона (MSTI = 2) образуют VLAN20 и VLAN21. Остальные виртуальные сети (на рисунке для их обозначения использован идентификатор "Other") образуют общий план сети (MSTI = 0). Индивидуальные настройки выполнены таким образом, что коммутатор SW11 выполняет функции корневого моста для CIST и MSTI = 1, а коммутатор SW21 — функции корневого моста для MSTI = 2. Таблица установленных алгоритмом Spanning Tree состояний портов коммутаторов региона приведена в нижнем левом углу рис. 8.9. Сформированные варианты активных топологий данного региона обеспечивают передачу трафика VLAN20 и VLAN21 через каналы, соединяющие коммутатор SW21 с коммутаторами SW12 и SW22. Трафик остальных виртуальных сетей передается через каналы, соединяющие коммутатор SW11 с коммутаторами SW12 и SW22. Такое решение позволяет выровнять нагрузки на ресурсы резервированных компонентов ЛВС, поскольку у коммутаторов региона все порты в той или иной степени будут использованы для передачи полезного трафика.



	порт	MSTI 1	MSTI 2
SW11	P1	F	F
SW11	P2	F	F
SW11	P3	F	F
SW21	P1	F	F
SW21	P2	F	F
SW21	P3	F	F
SW12	P1	D	F
SW12	P2	F	D
SW22	P1	F	D
SW22	P2	D	F

Рис. 8.9. Использование протокола MSTP для распределения трафика двух групп виртуальных сетей

Структура сообщений протокола MSTP

Сообщение протокола MSTP включает в себя основную и дополнительную часть. В основной части содержатся данные, используемые для построения активной топологии для базового плана региона. В дополнительной части содержатся данные, используемые для построения активной топологии для индивидуальных планов региона.

В табл. 8.8 приведена структура основной части конфигурационного сообщения протокола MSTP.

Таблица 8.8. *Структура основной части конфигурационного сообщения протокола MSTP*

Номер поля	Наименование и содержание поля	Значение (шест.)	Номера занимаемых байтов
1	PROTOCOL IDENTIFIER — идентификатор протокола MSTP	00-00	1—2

Таблица 8.8 *(окончание)*

Номер поля	Наименование и содержание поля	Значение (шест.)	Номера занимаемых байтов
2	VERSION — версия протокола MSTP	00	3
3	BPDU TYPE — тип сообщения MSTP	00	4
4	CIST FLAG — поле флагов MSTP		5
5	CIST ROOT ID — идентификатор корневого моста CIST		6—13
6	CIST EXTERNAL PATH COST — стоимость корневого пути		14—17
7	CIST REGIONAL ROOT ID — идентификатор корневого моста общего связующего дерева региона		18—25
8	CIST PORT ID — идентификатор порта, через который это сообщение было отправлено		26—27
9	MESSAGE AGE — текущее время жизни сообщения		28—29
10	MAXIMUM AGE — максимальное значение времени жизни сообщения		30—31
11	HELLO TIME — период отправки регулярных сообщений		32—33
12	FORWARD DELAY — время задержки переключения между режимами STP		34—35
13	VERSION 1 LENGTH — длина сообщения STP	00-00	36
14	VERSION 3 LENGTH — длина специфической части сообщения MSTP	—	37—38
15	MST CONFIGURATION ID — идентификатор конфигурации региона	—	39—89
16	CIST INTERNAL PATH COST — стоимость пути до корневого моста для базового плана региона	—	90—93
17	CIST BRIDGE ID — идентификатор моста, сформировавшего данное сообщение	—	94—101
18	CIST REMAINING HOPS — максимальное число мостов, которое может пройти сообщение	—	102
19	MSTI CONFIGURATION MESSAGES — конфигурационные сообщения для планов региона	—	103—(103+Version 3 Lenghth+39)

Поскольку для протоколов STP, RSTP и MSTP используется единый универсальный формат сообщений, поля PROTOCOL IDENTIFIER, VERSION, BPDU TYPE используются для идентификации типа используемого протокола и сообщения. В табл. 8.9 приведены коды этих полей для различных версий протокола Spanning Tree и типов используемых сообщений.

Таблица 8.9. *Коды полей PROTOCOL IDENTIFIER, Version, BPDU TYPE*

Протокол	Тип сообщения	Поля сообщений протокола MSTP		
		PROTOCOL IDENTIFIER	VERSION	BPDU TYPE
STP	BPDU-C	0000	00	00
STP	BPDU-TCN	0000	00	80
RSTP	BPDU-C	0000	02	02
MSTP	BPDU-C	0000	03	02

- Поле CIST FLAG предназначено для кодирования управляющих флагов в сообщениях протокола MSTP и формируется в соответствии с правилами, принятыми для протокола RSTP (см. табл. 8.7).
- Поля CIST ROOT ID и CIST EXTERNAL PATH COST, в которых размещаются идентификатор корневого моста CIST и стоимость корневого маршрута соответственно, имеют единый смысл для всех вариантов реализации протокола.
- В поле CIST REGIONAL ROOT ID сообщений протоколов STP и RSTP размещается идентификатор моста, сформировавшего данное сообщение. В сообщениях протокола MSTP это поле используется для размещения идентификатора корневого моста региона для базового плана.
- В поле CIST PORT ID размещается идентификатор порта моста, сформировавшего данное сообщение.
- Значения полей MESSAGE AGE, MAXIMUM AGE, HELLO TIME, FORWARD DELAY также остались неизменными по отношению к одноименным полям сообщений STP и RSTP.
- Поле VERSION 1 LENGTH в сообщениях протокола MSTP формируется равным нулю. Описываемые далее поля используются только в сообщениях протокола MSTP.
- Поле VERSION 3 LENGTH предназначено для размещения значения, соответствующего длине специфической части сообщения MSTP, выраженной в байтах.

- В поле MST CONFIGURATION ID размещается идентификатор конфигурации региона, состоящий из следующих компонентов:
  - идентификатор формата конфигурации — Configuration Identifier Format Selector (1 байт = 0000);
  - идентификатор конфигурации (региона) — Configuration Name (32 байта);
  - номер версии конфигурации — Revision Level (2 байта);
  - дайджест конфигурации — Configuration Digest (16 байтов).

  Наличие в поле MST CONFIGURATION ID идентификатора формата конфигурации обеспечивает совместимость с последующими версиями протокола MSTP. Идентификатор конфигурации предназначен для размещения текстовой строки, используемой для обозначения коммутаторов региона. Номер версии конфигурации должен изменяться всякий раз, когда изменяется содержимое таблицы виртуальных сетей MST, которое в виде дайджеста конфигурации содержится в последнем поле MST CONFIGURATION ID.
- В поле CIST INTERNAL PATH COST размещается стоимость пути до корневого моста для базового плана региона (MSTI = 0), к которому по умолчанию принадлежат все виртуальные сети.
- Поле CIST BRIDGE ID используется для указания единого для всех планов региона идентификатора моста, сформировавшего данное сообщение.
- В поле CIST REMAINING HOPS основной части MSTP-сообщения указывается максимальное число мостов, которое может пройти сообщение от данного моста для базового плана.

В дополнительной части конфигурационного MSTP-сообщения размещаются конфигурационные сообщения для каждого из планов, сформированных в данном регионе. Если в регионе не определено никаких планов, кроме базового, то дополнительная часть конфигурационного MSTP-сообщения не формируется.

В табл. 8.10 приведена структура дополнительной части конфигурационного сообщения протокола MSTP.

Таблица 8.10. *Структура дополнительной части конфигурационного сообщения протокола MSTP*

Номер поля	Наименование и содержание поля	Значение (шест.)	Номера занимаемых байтов
1	MSTI FLAGS — коды управляющих флагов	00-00	1
2	MSTI REGIONAL ROOT ID — идентификатор корневого моста плана	00	2—9

Таблица 8.10 (окончание)

Номер поля	Наименование и содержание поля	Значение (шест.)	Номера занимаемых байтов
3	MSTI INTERNAL PATH COST — стоимость пути до корневого моста	00	10—13
4	MSTI BRIDGE PRIORITY — приоритет моста		14
5	MSTI PORT PRIORITY — приоритет порта		15
6	MSTI REMAINING HOPS — максимальное число мостов, которое может пройти сообщение		16

- Поле MSTI FLAGS предназначено для кодирования управляющих флагов в сообщениях протокола MSTP и формируется в соответствии с теми же правилами, что и поле CIST FLAG основной части сообщения.
- Поле MSTI REGIONAL ROOT ID используется для размещения идентификатора корневого моста региона для данного плана. Поскольку один и тот же мост может быть корневым в нескольких планах, два старших байта этого идентификатора содержат значение номера плана региона — MSTID (биты с 1 по 4 первого байта и все биты второго байта).
- В поле MSTI INTERNAL PATH COST размещается стоимость пути до корневого моста для данного плана региона.
- Поля MSTI PORT PRIORITY и MSTI BRIDGE PRIORITY содержат для данного плана региона приоритеты порта и моста сформировавшего сообщение, соответственно.

Примечание

Для указания значения приоритета в обоих случаях используются только четыре старших разряда байта.

- В поле MSTI REMAINING HOPS дополнительной части MSTP-сообщения указывается максимальное число мостов, которое может пройти сообщение от этого моста для данного плана. Значение этого поля используется для ограничения времени существования конфигурационных MSTP-сообщений в ЛВС.

Примеры использования Spanning Tree при построении мультисервисных ЛВС

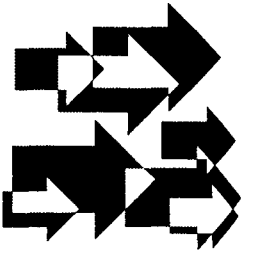
В табл. 8.11 приведены варианты настройки протокола MSTP на коммутаторах Catalyst 2950 Cisco Systems и Allied Telesyn AT9724-TS. Обе конфигура-

ции предусматривают включение VLAN10 во второй план STP и повышение приоритета конфигурируемого порта для данного плана.

Таблица 8.11. *Настройка параметров протокола MSTP на коммутаторах Cisco Systems и Allied Telesyn*

Действие	Allied Telesyn AT9724-TS	Cisco Catalyst 2950
Включить протокол Spanning Tree	`enable stp`	
Включить протокол MSTP	`config stp version mstp`	`(config)# spanning-tree mode mst`
Создать план (MSTI = 2) и включить в него VLAN10	`create stp instance_id 2` `config stp instance_id 2 add_vlan 10`	`(config-mst)# instance 2 vlan 10`
Установить идентификатор и номер версии конфигурации региона	`config stp mst_config_id revision_level 1` `name newregion`	`(config-mst)# name newregion` `(config-mst)# revision 1`
Установить приоритет порта для плана 2	`config stp mst_ports 1:2 instance_id 2 internalCost auto priority 32`	`(config-if)# spanning-tree mst 2 port-priority 32`
Установить приоритет коммутатора для плана 2	—	`(config-if)# spanning-tree mst 2 priority 8192`

ГЛАВА 9



Выравнивание загрузки резервированных узлов мультисервисных ЛВС

Применение горячего резервирования предполагает наличие в ЛВС дополнительного оборудования, которое либо используется при выходе из строя основных компонентов, либо используется постоянно, обеспечивая при этом снижение нагрузки на основные компоненты. Если, например, резервируемым устройством является сервер, то часть абонентов ЛВС сможет получать данные от основного сервера, а другая часть — от резервного. Основной сервер и резервный серверы в этом случае представляются пользователям в виде единого логического устройства, которое имеет все необходимые атрибуты для обеспечения информационного взаимодействия (например, адреса сетевого и канального уровня). Очевидно, что для реализации подобных режимов резервирования должны быть использованы специальные алгоритмы и методы, которые обеспечивают резервирование критических компонентов мультисервисных ЛВС и, при необходимости, динамическое перераспределение нагрузки между основным и резервными компонентами.

Основными узлами множественного доступа абонентов мультисервисных ЛВС, для которых целесообразно использовать горячее резервирование с перераспределением нагрузки, являются сетевые шлюзы (граничные маршрутизаторы) и разнообразные серверы. Учитывая специфику мультисервисных сетей, крайне желательно, чтобы методы и алгоритмы резервирования этих устройств были бы прозрачны с точки зрения абонента — для обеспечения выравнивания загрузки резервированных узлов ЛВС на клиентском оборудовании не должны использоваться никакие дополнительные настройки или специальное программное обеспечение.

Первый раздел данной главы посвящен рассмотрению алгоритмов и способов динамического резервирования шлюзов мультисервисных ЛВС. В нем, в частности, рассматриваются такие протоколы динамического резервирования,

как собственный протокол Cisco Systems Inc. — *HSRP* (Hot Standby Router Protocol), и стандартный протокол IETF — *VRRP* (Virtual Router Redundancy Protocol). Характерными особенностями этих протоколов являются ограниченные возможности по обеспечению выравнивания нагрузки (Load Balancing) между основным и резервными блоками.

Во втором разделе на примере собственного протокола Cisco Systems Inc. — *GLBP* (Gateway Load Balancing Protocol) и протокола *CARP* (Common Address Redundancy Protocol) рассматриваются основные принципы организации перераспределения нагрузки при динамическом резервировании шлюзов и других сетевых устройств множественного доступа ЛВС.

В третьем разделе рассматриваются альтернативные схемы и способы динамического резервирования устройств с множественным доступом абонентов мультисервисных ЛВС.

В четвертом разделе приведены примеры практического использования протоколов динамического резервирования компонентов мультисервисных ЛВС.

Динамическое резервирование компонентов ЛВС

Специальные приемы целесообразно использовать для резервирования именно тех критических компонентов ЛВС, отказ которых неминуемо приводит к нарушению информационного обмена в сети. В большинстве ЛВС такими критическими компонентами являются:

- межсетевые экраны;
- шлюзы (граничные маршрутизаторы);
- серверы приложений.

Особенности резервирования критических компонентов ЛВС вызваны тем, что эти компоненты используют постоянные сетевые адреса и поддерживают информационное взаимодействие со многими из абонентов сети одновременно. Следовательно, для того, чтобы резервный компонент смог взять на себя функции основного, необходимо, чтобы их адреса сетевого (и канального) уровня OSI ISO 7498 были одинаковыми. Это требование, однако, противоречит основным принципам организации информационного взаимодействия на сетевом (и канальном) уровне OSI ISO 7498, что вынуждает применять специальные методы, которые обеспечивают:

- формирование группы, состоящей из основного и резервирующих устройств;
- коллективное использование сетевых адресов членами группы;

- создание виртуального устройства для взаимодействия с внешними абонентами группы;
- постоянный мониторинг состояния резервируемого устройства членами группы.

Все перечисленные функции обычно реализуются в форме специальных протоколов, которые выполняются на основном и резервных устройствах ЛВС.

В частности, протоколы Cisco Systems Inc. — HSRP и VRRP предназначены для обеспечения гибкого резервирования наиболее ответственных узлов сети — маршрутизаторов.

Машрутизатор является обязательным компонентом любой ЛВС, поскольку обеспечивает реализацию базовых функций информационного взаимодействия — разделение сетей, определение пути передачи данных, доставку принимаемых пакетов локальным абонентам и т. д. Тот факт, что в современных сетях функции маршрутизатора, как правило, выполняют резервированные многоуровневые коммутаторы, делает еще более актуальной задачу обеспечения резервирования функции маршрутизации для этих устройств.

В такой ситуации именно применение протоколов, подобных HSRP или VRRP, позволяет строить современные надежные резервированные сети, мгновенно и автоматически восстанавливающие свою работоспособность при возникновении неисправностей.

Протокол динамического резервирования HSRP

Одним из первых протоколов динамического резервирования компонентов ЛВС был протокол Cisco Systems Inc. — *HSRP* (Hot Standby Router Protocol) IETF RFC 2281: March 1998 : Category: Informational.

Примечание

Компании Cisco Systems Inc. принадлежит патент на протокол HSRP (US Patent number 5,473,599)

Протокол HSRP может быть использован для выполнения процедур динамического резервирования маршрутизаторов и многоуровневых коммутаторов компании Cisco Systems Inc.

Особенности резервирования маршрутизаторов ЛВС

Как уже упоминалось ранее, метод горячего резервирования ответственных узлов сети достаточно часто используется для повышения надежности всей ЛВС в целом. Однако, в том случае, если резервируемым узлом является маршрутизатор, процедура резервирования существенно усложняется. Дело в том, что при выходе из строя основного маршрутизатора узлы, использовав-

шие его в качестве *шлюза по умолчанию* (default gateway), должны будут оперативно изменить свою таблицу маршрутизации. Суть этого изменения состоит в замене IP-адреса основного маршрутизатора на IP-адрес резервного маршрутизатора. Этот процесс можно автоматизировать и ускорить в том случае, если таблица маршрутизации узла формируется динамически при помощи протокола DHCP или протоколов маршрутизации.

Примечание

Следует отметить, что в последнем случае изменение конфигурации произойдет далеко не мгновенно, поскольку для любого протокола маршрутизации определяются ограниченные интервалы времени для определения статуса партнера.

Ситуация, однако, усложняется тем, что таблицы маршрутизации локальных узлов современных ЛВС в подавляющем большинстве формируются статически и состоят, по сути, из одной записи "default gateway" — шлюза по умолчанию, в качестве которого используется ближайший маршрутизатор ЛВС. Следовательно, для обеспечения достаточно быстрого изменения конфигурации и основной, и резервный маршрутизаторы должны использовать один и тот же IP-адрес.

Примечание

К сожалению, проблема подключения резервного маршрутизатора не ограничивается только сетевым уровнем. Даже если резервный маршрутизатор примет на себя IP-адрес вышедшего из строя основного маршрутизатора, локальные узлы на канальном уровне все равно будут продолжать передавать трафик, используя MAC-адрес неисправного маршрутизатора в течение периода времени жизни записи в ARP-кэш (120—180 сек). Поэтому протокол, обеспечивающий прозрачное для пользователя резервирование маршрутизаторов, кажется особенно актуальным.

Принципы реализации протокола HSRP

Обязательным условием использования протокола HSRP для резервирования маршрутизаторов является применение технологии множественного доступа к среде передачи данных (например, *CSMA/CD* (Carrier-Sense-Multiply-Access with Collision Detection) в сетях Ethernet), поскольку в его основе лежит принцип ротации адресов канального и сетевого уровня внутри так называемой *резервирующей группы* (Standby Group) маршрутизаторов. Только один член резервирующей группы обладает адресами виртуального маршрутизатора. Резервирующую группу образуют основной и резервный (или резервные) маршрутизаторы. Остальным компонентам сети резервирующая группа HSRP представляется в виде одного виртуального маршрутизатора, которому соответствует один адрес сетевого уровня (IP-адрес) и один адрес канального уровня (MAC-адрес).

Примечание

Каждый из маршрутизаторов резервирующей группы, естественно, имеет индивидуальный MAC-адрес и может иметь собственный IP-адрес для удобства управления. Таким образом, резервирующая группа из N маршрутизаторов имеет N+1 MAC-адресов.

После того, как один из маршрутизаторов резервирующей группы выбирается в качестве основного (активного), он принимает на себя виртуальные адреса канального и сетевого уровня и собственно функцию маршрутизации. Для того чтобы подтвердить свой статус, активный маршрутизатор через установленные интервалы времени посылает маршрутизаторам резервирующей группы специальное сообщение HELLO. Если маршрутизаторы резервирующей группы не получают HELLO от активного маршрутизатора в течение установленного интервала времени, то они констатируют, что активный маршрутизатор вышел из строя или выключен, и выбирают новый активный маршрутизатор.

На рис. 9.1 представлен вариант построения резервирующей группы из двух маршрутизаторов. Виртуальному маршрутизатору в этом случае присвоен адрес 10.4.5.1. Маршрутизатор с адресом 10.4.5.2 является активным членом резервирующей группы и фактически выполняет все функции виртуального маршрутизатора. Он принимает и обрабатывает пакеты, адресованные 10.4.5.1, и, кроме того, в ответ на запрос ARP-Request по адресу 10.4.5.1 передает ответное сообщение ARP- - Reply с MAC-адресом виртуального маршрутизатора в данной резервирующей группе. Кадры Ethernet, адресованные виртуальному маршрутизатору, также обрабатываются активным маршрутизатором группы. Таким образом, пакет, переданный рабочей станцией 10.4.5.200 в адрес шлюза по умолчанию (default gateway) (на представленном рисунке он имеет адрес 10.4.5.1) — виртуального маршрутизатора группы, фактически будет обработан и передан активным маршрутизатором группы — M1. В задачи активного маршрутизатора также входит периодическое формирование сообщений HELLO, подтверждающих его активность.

Примечание

Следует обратить внимание на то, что для передачи пакетов во внешнюю сеть маршрутизаторы — члены резервирующей группы, как правило, используют не те интерфейсы, через которые транслируются сообщения HELLO. Следовательно, при аварии внешнего интерфейса возможно возникновение ситуации, при которой вполне активный маршрутизатор фактически является неработоспособным.

Маршрутизатор с адресом 10.4.5.3 в данном случае является пассивным членом резервирующей группы. Его задача состоит в том, чтобы контролировать состояние активного члена группы и, при необходимости, принять на себя все его функции.

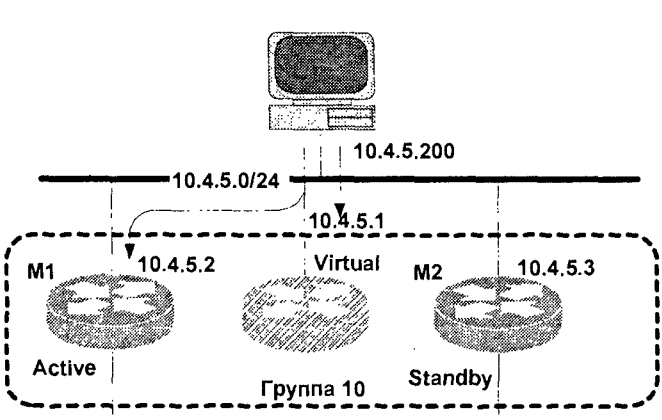


Рис. 9.1. Вариант построения резервирующей группы, состоящей из двух маршрутизаторов

Основные параметры протокола HSRP

Для выполнения согласованного взаимодействия в составе резервирующей группы, у всех маршрутизаторов, входящих в ее состав, должны быть определены согласованные значения параметров протокола HSRP, которые представлены в табл. 9.1.

Таблица 9.1. *Параметры протокола HSRP*

Параметр	Значение по умолчанию	Назначение
Standby group number	—	Порядковый номер резервирующей группы
Virtual MAC address	—	MAC-адрес виртуального маршрутизатора
Priority	100	Приоритет маршрутизатора
Authentication Data	"cisco___"	Данные, используемые для аутентификации
Hello time	3 сек	Период посылки сообщений HELLO
Hold time	10 сек	Интервал ожидания получения сообщения HELLO

Порядковый номер присваивается резервирующей группе для того, чтобы обеспечить возможность одновременного использования нескольких резервирующих групп на одном сегменте сети. В этом случае один маршрутизатор может являться членом нескольких резервирующих групп одновременно. Значение приоритета определяет относительную степень притязаний данного маршрутизатора на должность активного маршрутизатора резервирующей группы — чем выше приоритет, тем выше притязания.

Таймер Hello time определяет период формирования сообщений HELLO активным маршрутизатором резервирующей группы. Для маршрутизаторов Cisco Systems это значение по умолчанию составляет 3 сек.

Значение таймера Hold time определяет максимальный интервал времени, в течение которого пассивные маршрутизаторы резервирующей группы HSRP ожидают поступление сообщения HELLO от активного маршрутизатора их группы. Для маршрутизаторов корпорации Cisco Systems это значение по умолчанию составляет 10 сек.

Относительный приоритет маршрутизатора определяет его шансы быть использованным в качестве активного маршрутизатора резервирующей группы. Установленное для маршрутизаторов Cisco Systems по умолчанию значение приоритета маршрутизатора HSRP равно 100.

Основная особенность протокола HSRP заключается в том, что при его использовании только один из маршрутизаторов резервирующей группы (Standby — *резервный*) контролирует состояние активного маршрутизатора и, следовательно, может заменить его в случае отказа. Остальные маршрутизаторы резервирующей группы при этом являются *запасными* (Backup) и контролируют состояние резервного маршрутизатора. При выходе из строя резервного маршрутизатора его функции принимает на себя тот запасной маршрутизатор из резервирующей группы, который имеет наибольший приоритет.

При выполнении процедур протокола HSRP маршрутизатор резервирующей группы может находиться в одном из шести возможных состояний, перечень которых представлен в табл. 9.2.

Таблица 9.2. *Состояния маршрутизаторов HSRP*

Текущее состояние	Описание состояния	Последующее состояние
Initial	Начальное состояние	Learn
Learn	Состояние обучения	Listen
Listen	Прослушивание сети	Speak
Speak	Трансляция сообщений	Standby / Active / Listen
Standby	Резервный маршрутизатор	Initial
Active	Активный маршрутизатор	Initial

Сразу после включения интерфейса или изменения конфигурации интерфейс маршрутизатора находится в начальном состоянии Initial. Интерфейс, находящийся в этом состоянии, не принимает участия в процедурах протокола

HSRP. Однако, в том случае, если этот протокол сконфигурирован на данном интерфейсе, он автоматически переходит в следующее состояние обучения — Learn.

В состоянии Learn интерфейс маршрутизатора HSRP находится до получения первого сообщения HELLO от активного маршрутизатора. Из этого сообщения обучаемый маршрутизатор получает информацию об IP-адресе виртуальной группы и установленных для группы значений таймеров.

В состояние прослушивания (Listen) интерфейс маршрутизатора HSRP переводится после того, как на него было получено первое сообщение HELLO от активного маршрутизатора. Пока маршрутизатор HSRP находится в состоянии прослушивания — Listen, он по сути не является ни активным, ни резервным. В этом состоянии маршрутизатор только прослушивает сообщения активных и резервных маршрутизаторов и может перейти в следующее состояние трансляции сообщений (Speak) в том случае, если обладает достаточным приоритетом.

Маршрутизатор HSRP, находящийся в состоянии Speak, посылает периодические сообщения HELLO для участия в выборах, в итоге которых он становится активным или резервным маршрутизатором.

Примечание

Следует отметить, что протокол HSRP обеспечивает возможность управляемой замены нормально функционирующего активного или резервного маршрутизатора в том случае, если вновь включенный маршрутизатор имеет больший приоритет.

В дальнейшем маршрутизатор, получивший статус резервного маршрутизатора HSRP, контролирует состояние активного маршрутизатора путем анализа сообщений HELLO, сформированных активным маршрутизатором HSRP. Сам резервный маршрутизатор также формирует свои сообщения HELLO для того, чтобы подтвердить свой статус среди остальных маршрутизаторов резервирующей группы.

Каждый маршрутизатор при выполнении правил протокола HSRP использует значения трех таймеров:

- Active timer — применяется для мониторинга состояния активного маршрутизатора;
- Standby timer — применяется для мониторинга состояния резервного маршрутизатора;
- Hello timer — применяется для периодического формирования сообщений HELLO на активном и резервном маршрутизаторах.

Формат и типы сообщений HSRP

Для передачи сообщений протокола HSRP используются дейтаграммы протокола UDP (порт 1985). Для адресации сообщений применяется групповой адрес 224.0.0.2. Структура сообщения HSRP представлена в табл.9.3.

Таблица 9.3. *Структура сообщения протокола HSRP*

Номер поля	Наименование и содержание поля	Значение	Длина поля (байт)
1	VERSION — номер версии протокола HSRP	1	1
2	OP CODE — тип сообщения HSRP	0/1/2	1
3	STATE — состояние маршрутизатора HSRP	0/1/2/4/8/16	1
4	HELLO TIME — значение таймера Hello timer	1—255	1
5	HOLD TIME — значение таймера Hold timer	1—255	1
6	PRIORITY — относительный приоритет HSRP	1—255	1
7	GROUP — идентификатор резервирующей группы	1—255	1
8	RESERVED — поле, зарезервированное для дальнейшего использования	—	1
9	AUTHENTICATION DATA — открытый пароль для аутентификации участников резервирующей группы	—	8
10	VIRTUAL IP ADDRESS — адрес виртуального маршрутизатора резервирующей группы	—	4

В поле VERSION сообщения протокола HSRP размещается номер версии протокола, который был использован для формирования данного сообщения.

Содержимое поля OP CODE сообщения протокола HSRP определяет тип этого сообщения:

- значение OP CODE 0 — соответствует сообщению `HELLO`;
- значение OP CODE 1 — соответствует сообщению `Coup`;
- значение OP CODE 2 — соответствует сообщению `Resign`.

Назначение сообщений `HELLO` было достаточно подробно описано ранее. Сообщение `Coup` маршрутизатор передает в том случае, если собирается занять место активного маршрутизатора. Если, наоборот, маршрутизатор не желает больше быть активным, то он должен передать сообщение `Resign`.

В поле STATE размещается кодировка, определяющая текущее состояние маршрутизатора HSRP, сформировавшего это сообщение. Это значение вместе со значением поля PRIORITY используется для определения текущего статуса данного маршрутизатора в резервирующей группе HSRP.

Содержимое полей HELLO TIME и HOLD TIME имеет осмысленное значение только в сообщениях HELLO. Если в конфигурации маршрутизатора HSRP значение интервалов Hello time и Hold time не указано явно, то он должен использовать значения, полученные в сообщении HELLO от активного маршрутизатора. В противном случае маршрутизатор должен использовать значения, установленные по умолчанию для таймеров Hello time и Hold time — 3 и 10 сек соответственно.

В поле AUTHENTICATION DATA помещается открытый пароль, используемый для аутентификации участников резервирующей группы. В качестве значения, используемого по умолчанию, документ RFC 2281 рекомендует использование 0x63 0x69 0x73 0x63 0x6F 0x00 0x00 0x00 (текстовая строка "cisco___").

Особенности применения протокола HSRP

Для того чтобы обеспечить нормальное функционирование протокола HSRP, каждая группа резервирующих маршрутизаторов должна использовать уникальный виртуальный MAC-адрес. Структура виртуального MAC-адреса определяется типом протокола канального уровня. Протокол HSRP рекомендует использование для идентификации виртуальных групп, создаваемых в сетях Ethernet/IEEE 802.3, виртуального адреса: 00-00-0C-07-AC-XX, где XX — соответствует номеру резервирующей группы.

Активный маршрутизатор должен выполнять функции посредника (proxy — ARP-сервера) в отношении виртуального маршрутизатора. Если активный маршрутизатор принимает ARP-запрос на виртуальный IP-адрес своей резервирующей группы, то он должен сформировать ответ, где он указывает соответствующий виртуальный MAC-адрес своей группы.

Особенностью протокола HSRP является требование блокирования функции ICMP Redirect на маршрутизаторах резервирующей группы. Очевидно, что несогласованное использование IP-адресов различными маршрутизаторами из этой группы может нарушить ее правильное функционирование.

Полезной функцией протокола HSRP является возможность динамического изменения приоритета маршрутизатора резервирующей группы в зависимости от состояния выбранного интерфейса (Interface tracking). Эта функция в сочетании с возможностью перевыборов активного маршрутизатора (preempt) обеспечивает оперативное переключение на резервный или запасной маршрутизатор при аварии внешнего интерфейса.

К недостаткам протокола HSRP следует отнести отсутствие открытой спецификации и недостаточную надежность использованных в нем процедур аутентификации абонентов резервирующих групп.

Распределение нагрузки между основным и резервными маршрутизаторами группы может быть обеспечено только при наличии нескольких резервирующих групп в сети. В этом случае выравнивание нагрузки может быть достигнуто за счет того, например, что один и тот же маршрутизатор одновременно выполняет функции основного в одной группе и резервного в другой.

Протокол VRRP

Протокол *VRRP* (Virtual Router Redundancy Protocol — IETF RFC 3768 : April 2004 : Category: Standards Track), в отличие от HSRP, имеет статус стандартного протокола и предназначен для выполнения тех же функций, что и "фирменные" протоколы HSRP корпорации Cisco Systems и *IPSTB* (IP Standby Protocol) корпорации DEC. Протокол VRRP предусматривает также использование дополнительных процедур, исключающих возможность проведения перевыборов основного (Master) маршрутизатора при его нормальном функционировании.

Примечание

Первая версия протокола VRRP предусматривала использование развитой системы аутентификации участников резервирующей группы и, в частности, возможность использования протокола IP Authentication Header (AUTH) для установления подлинности абонентов. Однако опыт практической эксплуатации этой версии показал, что применение аутентификации при обмене сообщениями протокола VRRP не приводит к ожидаемому повышению уровня информационной безопасности и существенно усложняет реализацию основных функций протокола.

Компоненты протокола VRRP

Использование протокола VRRP предусматривает наличие группы маршрутизаторов, в пределах которой выполняются процедуры резервирования. Поскольку одна резервирующая группа маршрутизаторов образует один виртуальный маршрутизатор, для обозначения таких групп в протоколе VRRP используется идентификатор виртуального маршрутизатора — VRID (Virtual Router Identifier).

Примечание

Один реальный маршрутизатор может быть членом нескольких резервирующих групп одновременно. При этом он может выполнять функции активного маршрутизатора для одной или нескольких групп.

Правила протокола VRRP предусматривают, что только один маршрутизатор резервирующей группы формирует периодические сообщения для подтверждения своего активного статуса. Для сравнения: в протоколе HSRP такие

сообщения формируют как основной, так и резервный маршрутизаторы. По мнению разработчиков протокола VRRP такое усовершенствование позволяет существенно уменьшить долю пропускной способности ЛВС, используемой для передачи служебных сообщений. Маршрутизатор резервирующей группы VRRP, который имеет наибольший приоритет в группе, выполняет функции активного маршрутизатора (Master), остальные маршрутизаторы этой группы выполняют функции резервных маршрутизаторов группы (Backup Router), контролируя сообщения, формируемые активным маршрутизатором VRRP. В случае отсутствия этих сообщений в течение установленного периода времени, активный маршрутизатор считается неисправным и его функции принимает на себя наиболее приоритетный из числа резервных маршрутизаторов группы.

Структура сообщений VRRP

Сообщения протокола VRRP передаются в пакетах протокола IP с установленным значением поля PROTOCOL = 112 (VRRP). В качестве IP-адреса назначения этих сообщений используется Multicast-адрес 224.0.0.18. Структура сообщения VRRP представлена в табл. 9.4.

Таблица 9.4. *Структура сообщения протокола VRRP*

Номер поля	Наименование и содержание поля	Значение	Длина поля (байт)
1	VER — номер версии протокола VRRP	2	0,5
2	TYPE — тип сообщения VRRP	1	0,5
3	VRID — номер виртуального маршрутизатора (резервирующей группы) VRRP	1—255	1
4	PRIORITY — относительный приоритет маршрутизатора	1—255	1
5	COUNT IP ADDRS — количество IP-адресов, представляемых в данном сообщении	1—255	1
6	AUTHENTICATION TYPE — тип используемой схемы установления подлинности	0/1/2	1
7	ADVER INT — интервал передачи сообщений VRRP	1—255	1
8	CHECKSUM — контрольная сумма информационной части сообщения VRRP	—	2
9	IP ADDRESS (1)	—	4
	IP ADDRESS (N)	—	4
	AUTHENTICATION DATA (1)	—	4
	AUTHENTICATION DATA (2)	—	4

В поле VER сообщения протокола VRRP помещается номер версии. В настоящее время используется вторая версия протокола.

В поле TYPE указывается тип сообщения VRRP. В последней версии протокола используется только один тип сообщений, которые периодически формируются активным маршрутизатором резервирующей группы.

Поле VRID предназначено для размещения номера виртуального маршрутизатора, который однозначно определяет номер резервирующей группы VRRP. Один маршрутизатор может быть членом нескольких таких групп одновременно и, как следствие, может формировать несколько сообщений VRRP с различными значениями VRID.

Поле PRIORITY используется для размещения относительного приоритета маршрутизатора в указанной значением VRID виртуальной группе. Значение 0 является зарезервированным и используется только в тех случаях, когда необходимо выполнить мгновенное переключение действующего маршрутизатора резервирующей группы.

Поле COUNT IP ADDRS применяется для указания количества адресов, передаваемых в последующих полях данного сообщения.

Примечание

Дополнительные адреса виртуального маршрутизатора используются, как правило, в процессе настройки или изменения конфигурации протокола VRRP.

Поле AUTHENTICATION TYPE применяется для указания типа используемой процедуры установления подлинности. Как уже отмечалось, во второй версии протокола VRRP процедуры аутентификации не используются. Данное поле предназначено для обеспечения совместимости с первой версией протокола. Размещаемые в этом поле значения соответствуют:

- AUTHENTICATION TYPE = 0 — процедуры аутентификации не используются;
- AUTHENTICATION TYPE = 1 и 2 — зарезервированы для совместимости с первой версией протокола.

В поле ADVER INT размещается величина интервала циклической передачи сообщений VRRP.

Поле CHECKSUM используется для размещения контрольной суммы сообщения VRRP. Для вычисления этой контрольной суммы складываются значения всех полей сообщения, начиная с поля VER.

Поля IP ADDRESS предназначены для размещения IP-адресов, связанных с маршрутизатором VRRP, который сформировал данное сообщение.

В полях AUTHENTICATION DATA (1) и AUTHENTICATION DATA (2) при необходимости могут быть размещены данные, используемые при выполнении процедур установления подлинности абонента.

Особенности применения протокола VRRP

Главной особенностью протокола VRRP является наличие открытой спецификации. Протокол VRRP входит в список стандартных решений, используемых при построении мультисервисных ЛВС. Протокол VRRP предполагает использование для идентификации виртуальных групп, создаваемых в сетях Ethernet/IEEE 802.3, виртуального MAC-адреса: 00-00-5E-00-01-XX, где XX — соответствует номеру резервирующей группы.

Что касается сравнения характеристик этого протокола и протокола HSRP, то, в первую очередь, обращает на себя внимание отсутствие полезной процедуры мониторинга состояния внешних интерфейсов маршрутизатора. Не секрет, что эффективность функционирования маршрутизатора определяется не только состоянием его внутренних систем и управляющего процессора, но и степенью готовности к передаче данных подключенных к нему каналов. Невозможность учитывать последний фактор при определении приоритета маршрутизатора в виртуальной группе делает процедуру выбора активного маршрутизатора VRRP слишком формальной.

Примечание

Автоматическое парирование отказов внешних интерфейсов может быть выполнено путем использования протоколов динамической маршрутизации.

В то же время отсутствие во второй версии протокола VRRP процедур определения подлинности абонента не следует относить к недостаткам протокола. Протокол VRRP предназначен для использования в центральных узлах ЛВС, которые, как правило, достаточно сильно защищены от несанкционированного доступа. Кроме того, использование упрощенных процедур аутентификации HSRP не обеспечивает существенного повышения уровня информационной безопасности, поскольку не позволяет оказать противодействие атакам, основанным на подмене MAC-адресов маршрутизаторов при помощи сообщений протокола ARP.

Использование протокола динамического резервирования

Протокол VRRP, так же как и протокол HSRP компании Cisco Systems, обеспечивает возможность построения гибких и эффективных схем резервирования с множественным участием маршрутизаторов в резервирующих группах. Однако для того, чтобы обеспечить выравнивание загрузки основных и резервных маршрутизаторов в группе, администратор ЛВС должен выполнить специальные процедуры планирования и закрепить за каждым из маршрутизаторов резервирующей группы соответствующую ему группу абонентов.

При этом, в случае отсутствия неисправностей в системе все маршрутизаторы резервирующей группы смогут обрабатывать некоторую часть передаваемых данных, обеспечивая повышение производительности системы. В качестве примера реализации подобного решения рассмотрим схему построения ЛВС, которая представлена на рис. 9.2.

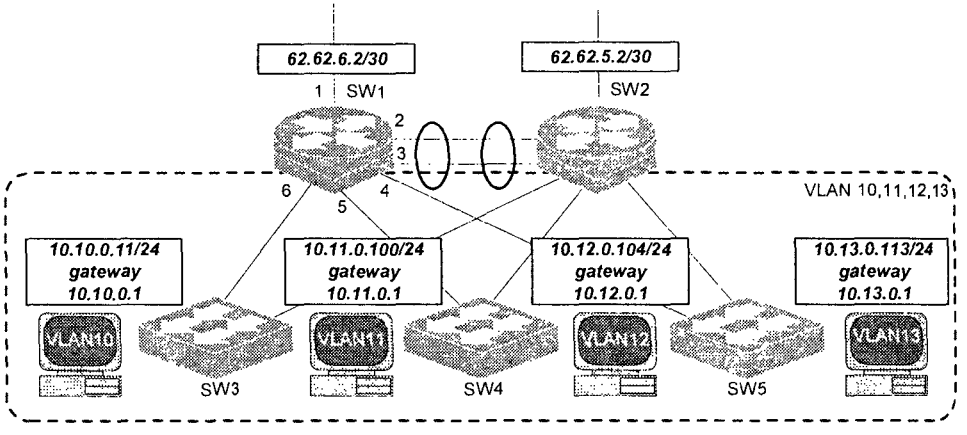


Рис. 9.2. Статическое распределение нагрузки у маршрутизаторов резервирующей группы

В данном случае протокол HSRP используется для динамического резервирования магистральных маршрутизирующих коммутаторов SW1 и SW2, а также выполнения статического распределения нагрузки между ними. Статическое выравнивание нагрузки достигается за счет разделения маршрутизируемого трафика на две части.

Первую часть образует трафик VLAN10 и VLAN11, а вторую — трафик VLAN12 и VLAN13. Настройка виртуальных маршрутизаторов соответствующих групп выполняется таким образом, чтобы активным маршрутизатором для первой части трафика был выбран SW1, а для второй — SW2. На приведенной схеме это обеспечивается установкой повышенных значений приоритета (110 — против 100, назначаемых по умолчанию). Применение протокола HSRP позволяет в данном случае выполнить также мониторинг состояния внешних интерфейсов маршрутизирующих коммутаторов (g0/1) с тем, чтобы при отказе одного из этих интерфейсов предоставить возможность перевода трафика на другой коммутатор. Так, при отказе интерфейса g0/1 приоритет маршрутизатора SW1 снизится до значения 90, вследствие чего он перейдет в состояние запасного и не будет использоваться для передачи данных.

Очевидно, что такая схема помимо обеспечения динамического резервирования позволяет значительно более эффективно использовать ресурсы сетевых

устройств, поскольку каждый из маршрутизаторов резервирующей группы при отсутствии отказов в ЛВС обрабатывает примерно половину совокупного трафика сети.

В листинге 9.1 приведен фрагмент конфигурационного файла маршрутизирующего коммутатора SW1 в части настроек протокола HSRP для резервирующих групп 1 и 4. Настройка резервирующей группы 2 выполняется аналогично группе 1 за исключением используемого номера VLAN и IP-адресов (в группе 2 используется VLAN11 и адреса 10.11.0.0). Настройка резервирующей группы 3 выполняется аналогично группе 4 за исключением используемого номера VLAN и IP-адресов (в группе 2 используется VLAN12 и адреса 10.12.0.0).

Листинг 9.1. Настройка параметров протокола HSRP на коммутаторе SW1 Cisco Systems для обеспечения статического распределения нагрузки в ЛВС (рис. 9.2)

```
   1. Переход в режим конфигурирования интерфейса VLAN10
Interface Vlan 10
   2. Установка индивидуального IP-адреса SW1 на интерфейсе VLAN10
Ip address 10.10.0.2 255.255.255.0
   3. Установка виртуального IP-адреса SW1 для первой группы HSRP
Standby 1 ip 10.10.0.1
   4. Установка значения приоритета SW1 для первой группы HSRP
Standby 1 priority 110
   5. Определение номера трассируемого интерфейса и величины уменьшения
      приоритета
Standby 1 track g0/1 20
   6. Определение возможности возврата в активное состояние при
      повышении приоритета
Standby 1 preempt
                                  * * *
   7. Переход в режим конфигурирования интерфейса VLAN13
Interface Vlan 13
   8. Установка индивидуального IP-адреса SW1 на интерфейсе VLAN13
Ip address 10.13.0.2 255.255.255.0
   9. Установка виртуального IP-адреса SW1 для четвертой группы HSRP
Standby 4 ip 10.13.0.1
```

В листинге 9.2 приведен фрагмент конфигурационного файла маршрутизирующего коммутатора SW2 в части настроек протокола HSRP для резервирующих групп 1 и 4. Настройка резервирующей группы 2 выполняется аналогично группе 1 за исключением используемого номера VLAN и IP-адресов (в группе 2 используется VLAN11 и адреса 10.11.0.0). Настройка резервирующей

рующей группы 3 выполняется аналогично группе 4 за исключением используемого номера VLAN и IP-адресов (в группе 2 используется VLAN12 и адреса 10.12.0.0). Следует отметить, что для обеспечения статического выравнивания нагрузки настройки SW1 и SW2 выполняются "зеркально".

Листинг 9.2. Настройка параметров протокола HSRP на коммутаторе SW2 Cisco Systems для обеспечения статического распределения нагрузки в ЛВС (рис. 9.2)

```
   1. Переход в режим конфигурирования интерфейса VLAN10
Interface Vlan 10
   2. Установка индивидуального IP-адреса SW2 на интерфейсе VLAN10
Ip address 10.10.0.3 255.255.255.0
   3. Установка виртуального IP-адреса SW2 для первой группы HSRP
Standby 1 ip 10.10.0.1
                              * * *
   4. Переход в режим конфигурирования интерфейса VLAN13
Interface Vlan 13
   5. Установка индивидуального IP-адреса SW2 на интерфейсе VLAN13
Ip address 10.13.0.3 255.255.255.0
   6. Установка виртуального IP-адреса SW2 для четвертой группы HSRP
Standby 4 ip 10.13.0.1
   7. Установка значения приоритета SW2 для четвертой группы HSRP
Standby 4 priority 110
   8. Определение номера трассируемого интерфейса и величины уменьшения
      приоритета
Standby 4 track g0/1 20
   9. Определение возможности возврата в активное состояние при
      повышении приоритета
Standby 4 preempt
```

Протоколы распределения нагрузки между компонентами ЛВС

Приведенный в конце предыдущего раздела вариант динамического резервирования маршрутизаторов при помощи протокола HSRP представляет собой характерный пример статического перераспределения трафика между резервными компонентами ЛВС. Отличительными чертами такого вида распределения являются:

- большой объем изменений, вносимых в конфигурацию оборудования;
- невозможность обеспечения реального распределения нагрузки.

Все изменения, которые вносятся в конфигурацию оборудования для организации статического перераспределения трафика между резервными компонентами, должны быть выполнены администратором вручную на основании измеренных или предполагаемых значений объемов трафика ЛВС.

Очевидно, что коррекции, единожды внесенные в конфигурацию, не учитывают реального соотношения объемов передаваемого трафика и однозначно не могут учесть возможные изменения этого соотношения во времени. Так, например, вполне может оказаться, что семь восьмых трафика активных пользователей сети, схема которой представлена на рис. 9.2, будут обрабатываться коммутатором SW1 и только одна восьмая — коммутатором SW2. В другой момент времени это соотношение объемов передаваемого трафика в сети может измениться на противоположное.

По результатам анализа недостатков статического распределения можно сформулировать основные признаки динамического распределения нагрузки внутри резервирующей группы:

- для выполнения распределения не требуется предварительного изменения конфигурации абонентов ЛВС;
- распределение нагрузки выполняется по алгоритму, определяемому администратором ЛВС, при этом могут учитываться возможности резервирующего узла и его текущая загрузка абонентами ЛВС;
- нагрузка распределяется только между теми из резервирующих узлов, которые имеют достаточный приоритет в резервирующей группе и своевременно подтверждают свою исправность.

В основе протоколов динамического распределения нагрузки между компонентами ЛВС, построенной с использованием технологии Ethernet/IEEE 802.3, лежит принцип коллективного использования MAC-адресов. Все члены резервирующей группы используют одновременно один адрес сетевого уровня, что обеспечивает устойчивость системы к отказу одного (или нескольких) элементов и распределение нагрузки между ними.

Характерным примером протокола подобного рода является протокол GLBP (Gateway Load Balancing Protocol) корпорации Cisco Systems. Хотя протокол CARP (Common Address Redundancy Protocol), который входит в комплект программного обеспечения операционной системы UNIX, также может обеспечивать выравнивание нагрузки между компонентами резервирующей группы, он, однако, не обладает всеми признаками протоколов динамического распределения нагрузки.

Протокол GLBP

Протокол *GLBP* (Gateway Load Balancing Protocol) разработан компанией Cisco Systems и предназначен для динамического выравнивания нагрузки в

группах резервированных узлов ЛВС. В этом протоколе получили дальнейшее развитие принципы динамического резервирования, заложенные в протоколах HSRP и VRRP.

Главное отличие от ранее описанных протоколов заключается в том, что при использовании протокола GLBP функцию активного шлюза могут выполнять не один, а несколько компонентов резервирующей группы одновременно. Эта возможность обеспечивается благодаря применению для доступа к виртуальному шлюзу группы адресов канального уровня (4 MAC-адреса) вместо использования для этих целей одного адреса, как это делается в протоколах HSRP и VRRP. Этим достигается возможность одновременного использования четырех компонентов резервирующей группы для обслуживания запросов, поступающих от абонентов ЛВС.

Назначение протокола GLBP

Как уже было отмечено, протокол GLBP предполагает наличие нескольких компонентов — шлюзов ЛВС, которые образуют резервирующую группу. В процессе выполнения процедур протокола GLBP эти компоненты распределяют между собой группу адресов канального уровня, каждый из которых соответствует IP-адресу виртуального шлюза. Таким образом, с точки зрения абонентов ЛВС, резервирующая группа представляется единым устройством.

Один из компонентов резервирующей группы выполняет функции активного шлюза-диспетчера — AVG (Active Virtual Gateway). Остальные компоненты резервирующей группы могут получить статус активных шлюзов-отправителей — AVF (Active Virtual Forwarder). Основными задачами шлюза-диспетчера AVG при выполнении протокола GLBP являются:

- выбор активных компонентов резервирующей группы и распределение между ними MAC-адресов виртуального шлюза;
- распределение внешних запросов между активными компонентами резервирующей группы.

При выполнении первой функции обязательно учитывается текущий статус компонента резервирующей группы и его относительный приоритет.

Примечание

Только ограниченное количество членов резервирующей группы получает статус активных компонентов — AVF (Active Virtual Forwarder). Сам активный диспетчер в соответствии с требованиями протокола GLBP обычно также выполняет функции AVF.

Технически менее совершенные или временно неисправные компоненты не получают от AVG право использования адресов виртуального шлюза и, следовательно, не участвуют в информационном взаимодействии с абонентами

ЛВС. Весовой коэффициент компонента резервирующей группы, определяющий его возможность получить статус AVF, устанавливается администратором системы, но может динамически изменяться (например, при возникновении аварии на внешнем интерфейсе этого компонента).

При выполнении второй своей функции (распределение внешних запросов) диспетчер виртуальной группы может использовать несколько различных алгоритмов с тем, чтобы обеспечить наиболее равномерное распределение загрузки между компонентами резервирующей группы. Распределение нагрузки реализуется следующим образом — получив очередное обращение к виртуальному шлюзу в виде ARP-запроса от абонента ЛВС, AVG формирует ответное сообщение `ARP Reply`, в котором указывает виртуальный MAC-адрес наименее загруженного AVF.

Очевидно, что при такой организации виртуальной группы наиболее ответственным компонентом является AVG. Для обеспечения требуемого уровня надежности резервирование самого AVG выполняется стандартным образом при помощи периодических сообщений `HELLO`. Такие же периодические сообщения используются для контроля текущего состояния каждого из AVF. Отсутствие регулярных сообщений от любого из компонентов резервирующей группы в соответствии с правилами протокола GLBP означает неисправность данного компонента и необходимость его замены.

Организация взаимодействия компонентов GLBP

На рис. 9.3 приведена схема организации взаимодействия виртуального шлюза GLBP с абонентами ЛВС. На приведенной схеме функции AVG выполняет

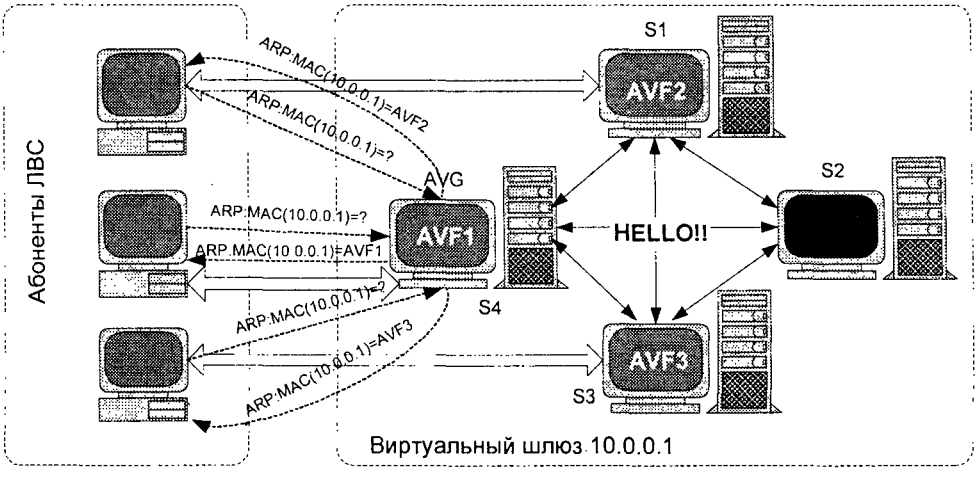


Рис. 9.3. Схема взаимодействия виртуального шлюза GLBP с абонентами ЛВС

шлюз S4. Шлюзы S1 и S3 в этой сети имеют статус AVF, а шлюз S2 находится в резерве.

Пунктирными линиями на рис. 9.3 показаны ARP-запросы, поступающие активному диспетчеру виртуального шлюза от абонентов ЛВС. В ответ на эти запросы AVG направляет виртуальные MAC-адреса, принадлежащие различным AVF, обеспечивая тем самым распределение нагрузки между ними. Будучи пассивным членом резервирующей группы, шлюз S2 контролирует состояние активных членов по формируемым ими сообщениям HELLO с тем, чтобы при отказе любого из них занять место выбывшего из строя активного члена.

Способы выравнивания нагрузки

При использовании протокола GLBP администратор может выбрать один из четырех возможных режимов распределения нагрузки между компонентами резервирующей группы:

- *монопольный* — None;
- *взвешенный* — Weighted;
- *по адресу абонента* — Host dependent;
- *циклический* — Round robin.

Первый из приведенных режимов — монопольный (None) — не предусматривает распределения нагрузки. При использовании этого режима все запросы, которые поступают на AVG, обрабатываются на нем же.

Примечание

При использовании этого режима распределения правила протокола GLBP практически полностью соответствуют правилам протокола HSRP.

Использование взвешенного режима (Weighted) предполагает наличие весовых коэффициентов у каждого из компонентов резервирующей группы. При использовании этого режима выравнивания нагрузки запросы, получаемые от абонентов, AVG распределяет между AVF пропорционально значениям их весовых коэффициентов.

Основное назначение весовых коэффициентов протокола GLBP состоит в управлении состоянием компонента резервирующей группы. Активный статус обычно получает тот компонент, чей весовой коэффициент превышает установленное пороговое значение. Значение весового коэффициента определяется эксплуатационными характеристиками шлюза, но это значение может изменяться в соответствии с изменениями состояния внешних его интерфейсов. Режим трассировки состояния ответственных интерфейсов, применяемый в протоколе GLBP, во многом похож на тот, что используется в

протоколе HSRP. Отличие заключается в том, что трассировка GLBP обеспечивает возможность изменения весового коэффициента шлюза в зависимости от состояния протокола сетевого уровня на контролируемом интерфейсе.

Режим, определяемый абонентом (Host dependent), используется в тех случаях, когда желательно, чтобы один и тот же абонент ЛВС получал в ответ на все свои ARP-запросы к AVG один и тот же виртуальный MAC-адрес.

Циклический режим выравнивания (Round robin) является наиболее простым для реализации, поскольку предполагает поочередное использование всех активных AVF для обслуживания запросов, поступающих от абонентов ЛВС.

Особенности применения протокола GLBP в мультисервисных ЛВС

Протокол GLBP является одним из немногих протоколов резервирования, которые способны обеспечивать управляемое динамическое распределение нагрузки между компонентами резервирующей группы, и, безусловно, может быть рекомендован к применению в современных мультисервисных ЛВС. К факторам, ограничивающим возможность внедрения протокола GLBP в мультисервисные ЛВС, в первую очередь следует отнести:

- отсутствие промышленного стандарта или открытой спецификации протокола;
- отсутствие поддержки этого протокола производителями системного программного обеспечения.

Таким образом, наиболее оправданным при построении мультисервисной ЛВС следует считать использование протокола GLBP для динамического резервирования магистральных маршрутизирующих коммутаторов.

Протокол CARP

Протокол *CARP* (Common Address Redundancy Protocol) предназначен для обеспечения динамического резервирования серверов и шлюзов, которые работают под управлением операционных систем, развиваемых в рамках проекта OpenBSD.

Хотя протокол CARP имеет некоторые черты, которые делают его похожим на HSRP или VRRP, он является самостоятельным протоколом и обеспечивает возможность реализации дополнительных функций.

Так же, как и протоколы HSRP и VRRP, протокол CARP используется для взаимодействия компонентов резервирующей группы.

Каждая резервирующая группа представляется протоколом CARP в виде виртуального интерфейса carpX, где X = 0, 1, ... n — номер интерфейса. Этому

интерфейсу присваиваются номер виртуального узла vhid, IP-адрес, приоритет и значения других необходимых параметров.

Основные особенности протокола CARP

В качестве главного отличия от предшествующих протоколов динамического резервирования создатели протокола CARP отмечают развитую систему аутентификации компонентов резервирующей группы. Однако целесообразность наличия такой системы у протокола подобного рода не кажется бесспорной. Действительно, для успешного применения протокола динамического резервирования необходимо, чтобы все компоненты резервирующей группы находились в пределах одного сегмента ЛВС. Поэтому сообщения, которыми обмениваются компоненты резервирующей группы, не могут ни уходить за пределы этого сегмента, ни приходить из-за его пределов. Если к тому же принять во внимание то, что резервируемое оборудование подключается, как правило, к центральному, наиболее защищенному сегменту ЛВС, то становится понятно, почему разработчики протокола VRRP отказались от использования аутентификации во второй версии протокола.

Еще одним полезным отличием CARP от протоколов HSRP и VRRP является наличие функции распределения нагрузки между компонентами резервирующей группы. Впрочем, в отличие от схемы, использованной в протоколе GLBP, это распределение выполняется по достаточно упрощенным правилам и принципиально не может обеспечить реального выравнивания нагрузок.

Для реализации такого распределения, например, в резервирующей группе, состоящей из двух серверов A и B, предлагается создать на каждом из них по два виртуальных узла (1 и 2) с одним и тем же IP-адресом. Приоритеты серверов при этом следует установить таким образом, чтобы сервер A, например, выполнял функцию активного сервера для узла 1, а сервер B выполнял функцию активного сервера для узла 2. После включения функции выравнивания на обоих серверах (net.inet.carp.arpbalance = 1), они будут выполнять анализ адреса источника поступающих ARP-запросов с тем, чтобы определить номер виртуального узла, который будет его обрабатывать. Поскольку каждому из виртуальных узлов соответствует только один реальный сервер, часть запросов при этом будет обработана на сервере A, а оставшиеся запросы — на сервере B. При отказе одного из серверов, например A, оба виртуальных узла на оставшемся сервере B перейдут в активное состояние, и при продолжении действия функции выравнивания все последующие запросы будут обрабатываться именно на этом сервере.

Полезной функцией протокола CARP является автоматическая трассировка состояния физических интерфейсов сервера. При аварии на таком интерфейсе приоритеты на всех виртуальных интерфейсах carpX данного сервера устанавливаются равными 240.

Область применения протокола CARP

Принимая во внимание описанные ранее особенности протокола CARP, следует отметить, что он может быть использован для организации динамического резервирования серверного оборудования мультисервисных ЛВС. Этот протокол достаточно прост для конфигурирования и не предъявляет повышенных требований к характеристикам резервируемых серверов.

При принятии решения об использовании протокола CARP, однако, следует учитывать возможность возникновения проблем, вызванных инициативным характером его разработки. В некоторых случаях отсутствие промышленного стандарта является серьезным доводом против технического решения, поскольку означает ограниченные возможности его масштабирования. Следует отметить, что на момент публикации нерешенными оставались вопросы о выделении фиксированного номера порта или номера протокола для CARP. Следствием таких организационных проблем могут быть конфликты при одновременном использовании протокола CARP с его промышленными аналогами.

Еще одним существенным фактором, который может сдерживать внедрение протокола CARP, является отсутствие поддержки этого протокола во многих современных операционных системах (например, Windows, Solaris).

Вместе с тем нельзя не заметить, что протокол CARP безусловно обладает рядом несомненных достоинств, которые наверняка получат дальнейшее развитие в последующих версиях этого протокола.

Альтернативные способы распределения нагрузки

Описанные в предыдущих разделах данной главы протоколы могут использоваться для динамического резервирования различных компонентов мультисервисных ЛВС. Каждый из этих протоколов имеет индивидуальные особенности, что дает администратору возможность выбора наиболее подходящего из них в зависимости от конфигурации резервируемой системы. В табл. 9.5 приведены обобщенные характеристики наиболее популярных протоколов динамического резервирования.

Протоколы динамического резервирования являются эффективным, но не единственным средством повышения надежности и производительности компонентов мультисервисных сетей.

Среди альтернативных решений, обеспечивающих динамическое резервирование серверного оборудования мультисервисных ЛВС, в первую очередь следует выделить серверные кластеры. Надежное функционирование высо-

копроизводительных шлюзов также может быть обеспечено при помощи построения отказоустойчивых стеков многоуровневых коммутаторов.

Таблица 9.5. *Обобщенные характеристики протоколов динамического резервирования*

Характеристика	Протокол			
	HSRP	VRRP	GLBP	CARP
Наличие промышленного стандарта	нет	да	нет	нет
Автоматическое переключение на резервный компонент при аварии основного	да	да	да	да
Автоматическое уменьшение приоритета при аварии трассируемого интерфейса	да	нет	да	да*
Автоматическое распределение нагрузки между компонентами резервирующей группы	нет	нет	да	да**
Возможность использования протокола на многоуровневых коммутаторах и маршрутизаторах	да***	да	да***	нет
Возможность использования протокола для резервирования серверов	нет	нет	нет	да****

Примечания к таблице:

* Не обеспечена возможность управления выбором интерфейса.
** Не обеспечена возможность управления выбором алгоритма.
** Только на устройствах Cisco Systems.
**** Только под управлением OS Open BSD.

Серверные кластеры

Кластером серверов называют группу независимых компьютеров, объединенных в единую систему с тем, чтобы обеспечить постоянную доступность для клиентов находящихся на них ресурсов и приложений. Серверные кластеры имеют достаточно много общих черт с виртуальными резервирующими группами, которые достаточно подробно были описаны в предыдущих разделах настоящей главы. Так, серверы, объединяемые в кластер, также образуют виртуальный объект, через который и производится взаимодействие с абонентом. Естественно, что обмен с серверным кластером клиент производит таким же образом, как и с независимым сервером. В пределах кластера серверы также обмениваются периодическими сообщениями с тем, чтобы определить степень работоспособности партнера. В зависимости от используемой конфигурации, один или несколько активных серверов принимают на себя функцию обработки клиентских запросов, поступающих на кластер.

Специфика построения серверных кластеров заключается в том, что современные серверные системы, как правило, имеют в своем составе такие мощ-

ные инструменты, как разделяемые отказоустойчивые массивы хранения данных — *RAID* (Redundant Array Of Independent Disks). Поскольку устройства подобного рода сами по себе являются высоконадежными компонентами, их использование в составе кластера серверов обеспечивает существенное повышение устойчивости к отказам системы в целом. Дальнейшего повышения надежности можно добиться при помощи включения в состав кластера нескольких массивов RAID.

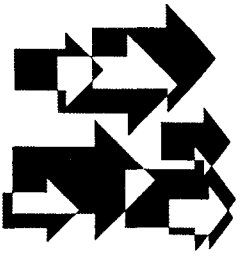
Для получения более подробной информации о возможностях создания, процедурах построения и особенностях использования серверных кластеров следует обратиться к эксплуатационной документации используемых операционных систем.

Стеки многоуровневых коммутаторов

Повышения надежности и производительности магистральных шлюзов ЛВС можно добиться путем их объединения в специальные отказоустойчивые стеки. Для создания таких стеков могут быть использованы патентованные технологии фирм-изготовителей телекоммуникационного оборудования. Примером подобной технологии является технология *eXpandable Resilient Networking* (XRN) компании 3Com. Благодаря использованию этой технологии соединенные друг с другом специальными каналами коммутаторы объединяются в единый коммутирующий и маршрутизирующий блок, наращиваемый простым добавлением в него новых маршрутизирующих коммутаторов. Этот блок образует так называемую распределенную коммутационную XRN-матрицу. Поскольку отключение неисправных элементов и распределение нагрузки между компонентами XRN-матрицы производится автоматически системными средствами, администратор ЛВС освобожден от необходимости внесения дополнительных изменений в конфигурации коммутаторов.

Следует учитывать, что неизбежным следствием применения патентованных фирменных технологий является принципиальная несовместимость выбранных решений с оборудованием других производителей, а в некоторых случаях, и с оборудованием другой серии этого же производителя.

ГЛАВА 10



Увеличение пропускной способности каналов ЛВС

Известно, что мультисервисные сети предъявляют повышенные требования к пропускной способности каналов ЛВС. Эти требования далеко не всегда удается выполнить путем внедрения нового каналообразующего оборудования. Дело в том, что каждая последующая скорость информационного обмена в технологии Ethernet IEEE 802.3 превышает предыдущую в 10 раз. Поэтому, если вследствие повышения интенсивности информационного обмена в сети пользователей перестал устраивать канал с пропускной способностью 1000 Мбит/сек, разработчик ЛВС будет вынужден заменить его каналом с пропускной способностью 10 Гбит/сек. Такая замена, однако, может не всегда быть оправданной и целесообразной. Наиболее простым и доступным способом увеличения пропускной способности каналов ЛВС является объединение нескольких параллельных каналов в один, производительность которого теоретически равна сумме пропускных способностей образующих его каналов. Очевидно, что при использовании этого способа гораздо проще построить объединенный — *агрегированный канал* (aggregated channel), характеристики которого более полно отвечают предъявляемым требованиям.

При построении объединенного канала следует в первую очередь обратить внимание на способ распределения нагрузки между составляющими его каналами. Очень важно также, чтобы использованная технология обеспечивала автоматическое создание и обслуживание объединенного канала на оборудовании различных производителей.

Первый раздел настоящей главы включает в себя рассмотрение способов построения агрегированных каналов и рекомендации по их применению.

Во втором разделе рассматриваются основные способы распределения трафика в объединенных каналах ЛВС.

Третий раздел посвящен рассмотрению принципов построения и реализации стандартного протокола объединения параллельных каналов ЛВС.

В заключительных разделах главы приведены рекомендации по построению и использованию агрегированных каналов в мультисервисных ЛВС.

Применение агрегированных каналов в мультисервисных ЛВС

Построение магистральных каналов ЛВС является достаточно сложной задачей, поскольку к пропускной способности и надежности таких каналов обычно предъявляются повышенные требования. Данные через магистральные каналы обычно передаются со скоростью, которая на порядок превышает скорость передачи данных любого из подключенных абонентов. Для реализации магистральных соединений можно использовать специальные высокоскоростные порты коммутаторов, однако количество таких портов на коммутаторах современных производителей строго ограничено (обычно 2 или 4) и может оказаться недостаточным для реализации требуемой конфигурации ЛВС. Более того, как было показано во введении к данной главе, их применение может оказаться неэффективным по экономическим соображениям.

Отдельную задачу представляет собой обеспечение требуемого уровня надежности магистральных соединений. В большинстве случаев выход из строя нерезервированного магистрального канала на коммутаторе почти всегда приводит к полному отключению от сетевых ресурсов всех подключенных к этому коммутатору абонентов. Использование технологий Spanning Tree и Multiple Spanning Tree (см. *главу 8*) позволяет создавать резервированные магистральные соединения ЛВС, однако для построения и эффективного использования таких соединений в большинстве случаев требуется внесение значительных изменений в конфигурацию коммутатора.

Агрегирование каналов ЛВС обеспечивает управляемое повышение пропускной способности магистральных каналов ЛВС и является разумной альтернативой применению более дорогих магистральных интерфейсов. В объединенный канал, соединяющий двух абонентов, могут быть включены несколько обычных интерфейсов (от 2 до 8). При этом использование адекватного алгоритма распределения трафика между компонентами позволяет обеспечить линейное увеличение пропускной способности агрегированного канала.

Кроме того, применение объединенных каналов позволяет реализовать эффективное резервирование сетевых подключений. Включение дополнительного интерфейса в агрегированный канал благодаря использованию специальных фильтров не приводит к возникновению циклических маршрутов распространения широковещательных кадров в ЛВС. Выход из строя одного или нескольких компонентов не приводит к полному отказу агрегированного канала, а лишь пропорционально снижает его пропускную способность.

Следует, однако, иметь в виду, что само по себе применение агрегированных каналов не обеспечивает автоматического решения всех проблем построения магистральных соединений. Решение о внедрении объединенных каналов должно приниматься после тщательного анализа особенностей данной технологии и структуры информационных потоков в модернизируемой ЛВС.

Агрегирование магистральных каналов коммутаторов

Объединение каналов предусматривает включение нескольких сетевых интерфейсов Ethernet/IEEE 802.3 в единый блок — агрегированный канал. Этот канал должен обладать всеми признаками обычного интерфейса и в дополнение к этому решать следующие основные задачи:

- реализацию алгоритма распределения трафика между интерфейсами агрегированного канала;
- мониторинг состояния интерфейсов агрегированного канала;
- динамическое изменение алгоритма распределения трафика при изменениях конфигурации системы;
- обеспечение согласованного взаимодействия оборудования различных производителей.

Принципы построения агрегированных интерфейсов

Поскольку построение агрегированного канала предполагает использование нескольких интерфейсов, весьма целесообразным является его применение именно на многопортовых прозрачных мостах — коммутаторах Ethernet/IEEE 802.

Агрегированный канал представляется на коммутаторе в виде дополнительного виртуального логического интерфейса, который конфигурируется и управляется по стандартным правилам и процедурам, принятым для обычных интерфейсов. В то же время реальные интерфейсы, которые входят в этот агрегированный канал, теряют возможность индивидуального конфигурирования.

Примечание

При необходимости изменение конфигурации всех интерфейсов (компонентов канала) производится одновременно с изменением конфигурации образуемого ими агрегированного канала.

Для тех интерфейсов, которые образуют агрегированный канал, на коммутаторе выполняются выбранные процедуры распределения трафика виртуального агрегированного интерфейса.

Кадры, передаваемые через агрегированный канал, обрабатываются с использованием специальных процедур, предотвращающих возможность обратной передачи через агрегированный канал того кадра, который был по нему получен. Применение этих процедур фильтрации делает невозможным циклическую передачу широковещательных и других кадров через компоненты агрегированного канала.

Ускорение процедуры распределения кадров

Как правило, для выполнения алгоритма распределения кадров между компонентами агрегированного канала требуется произвести анализ значений различных полей блоков данных кадра. Более подробно эти процедуры описаны в следующем разделе настоящей главы. Очень часто для обеспечения эффективного распределения трафика между компонентами агрегированного канала приходится использовать сложные процедуры, которые должны анализировать значения полей нескольких инкапсулированных в кадр блоков данных. При построении сложных многоступенчатых процедур распределения трафика виртуального агрегированного интерфейса следует учитывать, что их реализация приводит к повышению нагрузки на центральный процессор коммутатора. Следствием этого может стать перегрузка центрального процессора и потеря обрабатываемых кадров. Для предотвращения подобных ситуаций было бы желательно ускорить выполнение на коммутаторе процедуры распределения кадров между компонентами агрегированного канала.

Наиболее простым способом ускорения процедуры распределения кадров на коммутаторе является упрощение этой процедуры. Например, при построении агрегированного канала, состоящего из двух портов, вместо анализа содержимого всего поля MAC-адреса назначения кадра можно анализировать только значения младшего бита этого адреса. Кадры с четным MAC-адресом назначения можно передавать через один компонент агрегированного канала, с нечетным MAC-адресом назначения — через другой. Распределение кадров между компонентами агрегированного канала при этом вряд ли будет достаточно равномерным, но зато выполнение подобной процедуры на коммутаторе достаточно просто реализовать аппаратно. Путем незначительного усложнения этой процедуры можно обеспечить возможность одновременного анализа значений нескольких полей передаваемого кадра. Например, требуется построить агрегированный канал из четырех портов, для распределения трафика между которыми следует учитывать значения двух полей кадра — MAC-адрес назначения и MAC-адрес источника. Для реализации этого алгоритма можно реализовать упрощенную процедуру, которая в дополнение к анализу значений двух младших битов указанных адресов выполняет процедуру "суммирование по модулю 2" для полученных результатов. В табл. 10.1 приведен пример реализации упрощенной процедуры для распределения кадров в агрегированном канале из 4 портов.

Таблица 10.1. *Использование логического суммирования для распределения кадров в агрегированном канале*

Порядковый номер комбинации	Младшие биты MAC-адреса назначения	Младшие биты MAC-адреса источника	Поразрядная сумма по модулю 2	Номер интерфейса для передачи кадра
1	00	00	00	0
2	00	01	01	1
3	00	10	10	2
4	00	11	11	3
5	01	00	01	1
6	01	01	00	0
7	01	10	11	3
8	01	11	10	2
...	...	...	...	...
15	11	10	01	1
16	11	11	00	0

Очень важно, что для выполнения упрощенных процедур распределения кадров обычно не требуется использование центрального процессора коммутатора, поскольку они выполняются специальными аппаратными модулями. Более подробно о процедурах распределения трафика рассказывается в следующем разделе настоящей главы.

Особенности агрегирования каналов IEEE 802.3

Основной особенностью применения агрегирования на оборудовании является наличие ограничений на тип интерфейсов, используемых при построении агрегированного канала.

В частности, все интерфейсы, которые используются при построении агрегированного канала, должны иметь одинаковую технологию и скорость передачи данных (все 10, 100 или 1000 Мбит/сек).

Не допускается также агрегирование интерфейсов, которые настроены для передачи данных в полудуплексном (Half Duplex) режиме. Как следствие, невозможно построение агрегированных каналов на средах передачи данных с общим доступом абонентов (коаксиальный кабель) и в сетях с раздельным доступом к среде передачи данных (витая пара), где используются промежуточные повторители.

Управление агрегированным каналом

Управление агрегированным каналом включает в себя набор процедур, которые обеспечивают:

- создание агрегированного канала на коммутаторе;
- добавление дополнительного интерфейса к агрегированному каналу;
- удаление выбранного интерфейса из агрегированного канала;
- удаление агрегированного канала из коммутатора.

Создание и удаление агрегированного канала на коммутаторе

Создание агрегированного канала на коммутаторе предусматривает построение единого блока, через который в дальнейшем будет выполняться оперативное управление агрегированным каналом и контроль его состояния. Для создания агрегированного канала администратор должен определить список портов коммутатора, входящих в этот канал, а также алгоритм, который будет использоваться для распределения трафика между этими портами. Агрегированный канал может быть построен с использованием ручного или автоматического (с применением протокола *LACP* (Link Aggregation Control Protocol)) режима управления. Более подробно этот протокол описан в последующих разделах настоящей главы.

Обычно агрегированный канал представляется для администрирования в виде виртуального интерфейса, причем администратор, как правило, не может создать и использовать более 8—16 подобных интерфейсов на одном коммутаторе одновременно. Количество портов, которые могут быть включены в агрегированный канал, также обычно ограничено (не более 8). В некоторых случаях администратор может использовать только один тип процедуры для распределения трафика между компонентами для всех агрегированных каналов одного коммутатора. После создания виртуального интерфейса агрегированного канала администратор может выполнять с ним обычные процедуры: включение/выключение, мониторинг состояния и характеристик агрегированного интерфейса. В зависимости от реализации администратор имеет возможность контролировать:

- текущие значения скоростей передачи и приема данных в агрегированном канале;
- состояние и текущие характеристики интерфейсов, входящих в агрегированный канал.

Анализируя эти значения, администратор может определить, насколько эффективно функционирует агрегированный канал и, при необходимости, изменить его конфигурацию.

Удаление агрегированного канала на коммутаторе приводит к уничтожению соответствующего виртуального интерфейса и освобождению всех используемых этим каналом физических интерфейсов коммутатора.

Добавление дополнительного интерфейса к агрегированному каналу

Для того чтобы некоторый интерфейс коммутатора стал компонентом агрегированного канала, необходимо, чтобы установленные для него параметры информационного обмена совпадали со значениями аналогичных параметров остальных интерфейсов, образующих агрегированный канал. К числу таких параметров обычно относятся:

- *скорость (технология) передачи данных* (например, 100 Base T);
- *тип информационного обмена* (например, полный дуплекс);
- *настройки виртуальных сетей* (например, маркирующий интерфейс для VLAN 2-1024).

В том случае, если значения критических параметров подключаемого к группе интерфейса отличаются от значения параметров, установленных для группы, включение этого интерфейса в группу не происходит. Такой интерфейс сохраняет статус индивидуального интерфейса, о чем и формируется диагностическое сообщение. Кроме того, на оборудовании некоторых производителей существуют дополнительные требования, которым должен удовлетворять сетевой интерфейс для включения в агрегированный канал. Например, на коммутаторах серии 4500 компании 3COM в агрегированный канал не могут быть включены стековые интерфейсы. Поэтому для правильного построения агрегированного канала необходимо внимательно ознакомиться с эксплуатационной документацией на используемый коммутатор.

Удаление интерфейса из агрегированного канала

Для административного удаления некоторого интерфейса из агрегированного канала обычно достаточно в специальной команде указать идентификаторы агрегированного канала и этого интерфейса. После административного удаления из агрегированного канала для интерфейса восстанавливается возможность автономного управления.

Удаление интерфейса из агрегированного канала может быть также выполнено автоматически в случаях аварии интерфейса или превышения установленного порогового значения уровня ошибок на этом интерфейсе.

Во всех случаях интерфейс исключается из агрегированного канала, а передаваемая им часть трафика перераспределяется между оставшимися компонентами канала.

Примечание

Используя протокол LACP, администратор при необходимости может определить резервный интерфейс, который будет автоматически подключаться к агрегированному каналу вместо удаленного или выключенного интерфейса. В этом случае отключение любого из интерфейсов не приведет к уменьшению общей пропускной способности агрегированного канала.

Распределение трафика в объединенном канале

Выравнивание нагрузки между объединяемыми каналами обычно достигается путем разделения общего трафика канала на несколько групп — по числу используемых каналов. В качестве критериев для такого разделения могут быть использованы параметры трафика, передаваемого через канал. Обычно при построении агрегированного канала принято использовать следующие параметры:

- MAC-адрес источника данных (Source MAC address);
- MAC-адрес приемника данных (Destination MAC address);
- тип адреса назначения (Type of destination address);
- значение Ethernet Length/Type;
- значения полей блоков данных протоколов транспортного (например, порт назначения) и более высоких уровней;
- произвольная комбинация описанных выше критериев.

Для корректного выбора алгоритма необходимо иметь четкое представление о способах и структуре информационного взаимодействия в ЛВС.

Использование признаков канального уровня

На рис. 10.1 приведен пример использования агрегированного канала для подключения нескольких абонентов к мультимедийному серверу.

Агрегированный канал в данном случае создается между коммутаторами SW1 и SW2. В качестве критерия разделения трафика используется MAC-адрес назначения кадров, поступающих от сервера.

Примечание

Следует обратить внимание на то, что для разделения трафика в данном случае достаточно анализировать только два младших бита этого адреса.

После получения очередного кадра, который нужно передать через агрегированный канал, коммутатор SW2 анализирует поле DESTINATION ADDRESS и принимает решение о том, через какой порт (1, 2, 3 или 4) его следует пере-

давать. В данном случае кадры, адресованные каждой из рабочих станций, будут передаваться через отдельный интерфейс, обеспечивая тем самым равномерную загрузку компонентов агрегированного канала и увеличение в 4 раза пропускной способности канала, который связывает коммутатор SW1 и SW2. Однако если такой же критерий будет использовать коммутатор SW1 для отправки кадров, следующих от рабочих станций PC1, PC2, PC3 и PC4 к серверу, то все эти кадры будут иметь одинаковый адрес назначения и будут отправлены только через один его порт. Очевидно, что никакого выравнивания нагрузки между каналами в данном случае не получится. Эффективного разделения для данного случая можно добиться, если в качестве признака разделения трафика использовать адрес источника кадра. Таким образом, эффективность применения агрегированного канала определяется степенью соответствия выбранной схемы разделения трафика и структуры информационных потоков ЛВС.

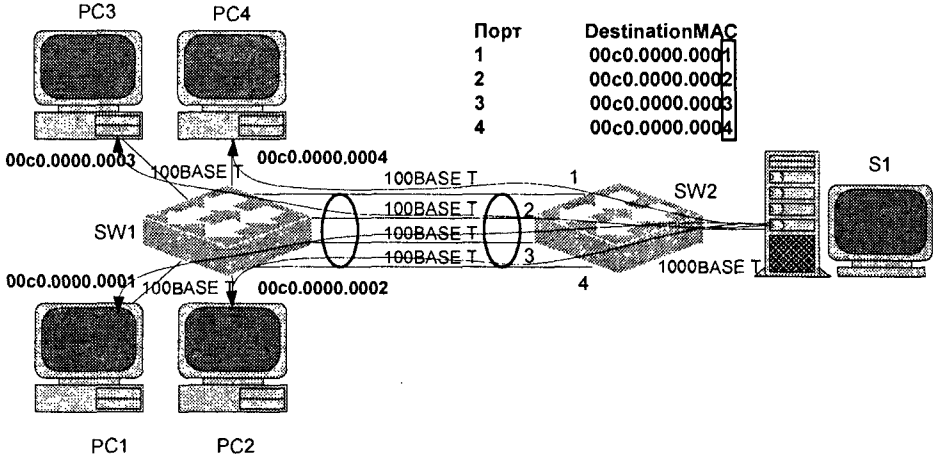


Рис. 10.1. Подключение нескольких абонентов к мультимедийному серверу

Использование признаков сетевого уровня

В тех случаях, когда разделение трафика принципиально не может быть выполнено на канальном уровне, оно реализуется по значениям полей блоков данных протоколов сетевого или транспортного уровней. На рис. 10.2 приведен пример построения агрегированного канала с использованием адресов сетевого уровня для разделения трафика.

В представленной схеме источником пользовательского трафика является сервер S2. Сервер S1 в данном случае выполняет функции сервера-посред-

ника (Proxy). Наличие сервера-посредника делает невозможным использование параметров канального уровня для разделения трафика в агрегированном канале, поскольку все кадры, поступающие на коммутатор SW2, имеют одинаковый адрес назначения — MAC-адрес этого сервера.

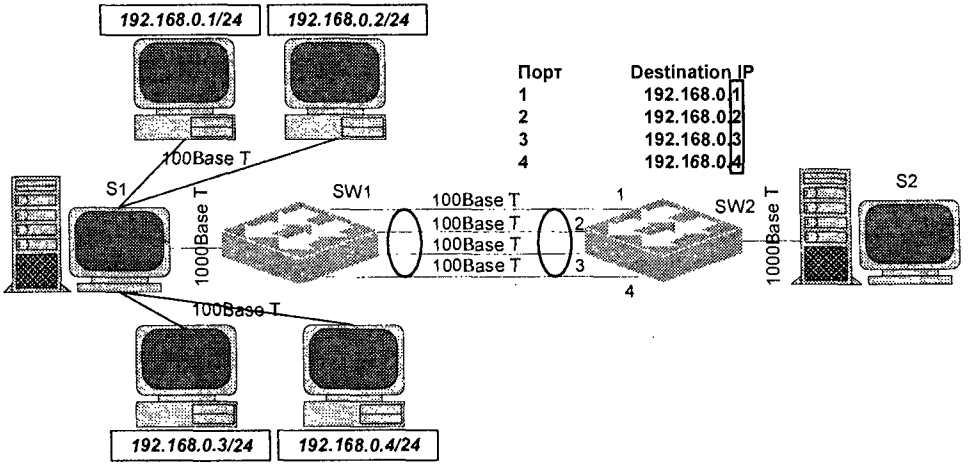


Рис. 10.2. Использование адресов сетевого уровня для разделения трафика в агрегированном канале

Комбинирование признаков

В предыдущих разделах были представлены основные принципы построения агрегированных каналов ЛВС с распределением трафика по значениям полей блоков данных протоколов канального и сетевого уровня. В некоторых случаях, однако, использование только одного поля блока данных протокола оказывается недостаточным для эффективного распределения трафика в агрегированном канале.

На рис. 10.3 приведен пример построения агрегированного канала для эффективного распределения трафика, в котором необходимо анализировать два поля адресов сетевого уровня. В представленной сети используются два мультимедийных сервера S1 и S2, каждый из которых подключен к отдельному коммутатору SW1 и SW2. К этим же коммутаторам подключены и абоненты (PC1—PC8), которые имеют доступ к ресурсам обоих серверов. Передача данных между коммутаторами выполняется через агрегированный канал, состоящий из четырех интерфейсов 1000BaseT. Очевидно, что эффективного распределения трафика между компонентами этого канала не получится, если для его обеспечения использовать только один из адресов сетевого уровня. Действительно, если использовать для распределения тра-

фика между интерфейсами агрегированного канала коммутатора SW2 IP-адрес источника, то весь исходящий поток сервера S2 будет проходить только через один (в данном случае — четвертый) интерфейс. Если использовать для распределения трафика между интерфейсами агрегированного канала коммутатора SW2 IP-адрес назначения пакета, то весь исходящий трафик на сервер S1 так же будет проходить через один интерфейс.

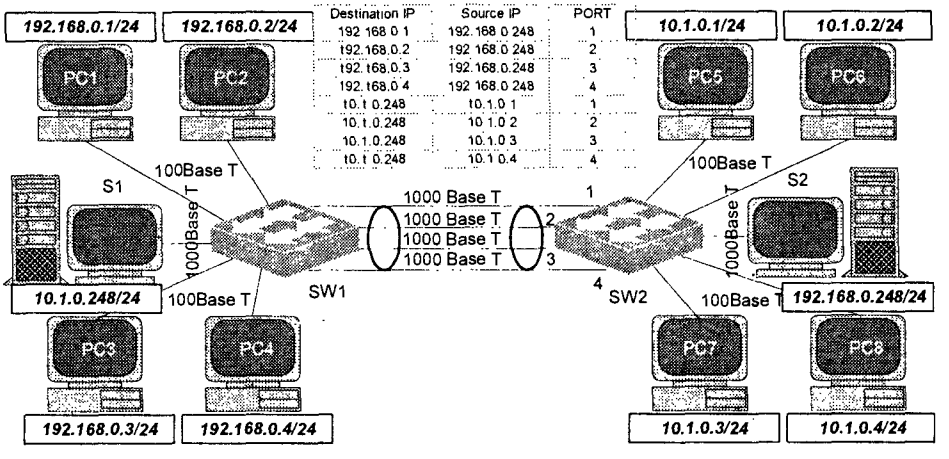


Рис. 10.3. Использование адресов сетевого уровня для разделения трафика в агрегированном канале

Обеспечить выравнивание загрузки в данном случае можно, если для распределения трафика в агрегированном канале коммутатора SW2 использовать значения адреса источника и адреса назначения пакета одновременно. В данном случае для определения номера порта может быть использовано логическое суммирование по модулю 2 двух младших разрядов этих адресов.

На коммутаторах различных производителей коммуникационного оборудования могут быть также использованы более сложные алгоритмы для распределения трафика в агрегированном канале, например, комбинирование адреса назначения сетевого уровня и адреса источника канального уровня. Для того чтобы правильно применять эти возможности при построении агрегированного канала, администратор должен внимательно ознакомиться с эксплуатационной документацией.

Протокол LACP IEEE 802.3AD

Протокол управления агрегированным каналом — *LACP* (Link Aggregation Control Protocol) предназначен для автоматического построения и обслуживания агрегированных каналов на сетевых устройствах с интерфейсами

Ethernet/IEEE 802.3. Используя этот протокол, коммутаторы и другие сетевые устройства могут обмениваться информацией о текущих настройках и состоянии интерфейсов, входящих в агрегированный канал, что позволяет существенно упростить процедуры построения и обслуживания этого канала. Поскольку описание протокола LACP является частью стандарта IEEE 802.3 (Part 3 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications, Chapter 43 — Link Aggregation), он является обязательным к реализации на сетевом оборудовании с интерфейсами Ethernet/IEEE 802.3. Применение протокола LACP обеспечивает следующие дополнительные преимущества при построении и использовании агрегированных каналов:

- автоматическое построение агрегированного канала;
- автоматическое изменение конфигурации при выходе из строя или выключении компонентов агрегированного канала.

Принципы реализации протокола LACP

В стандарте IEEE 802.3 протокол LACP определен в качестве одного из вариантов медленных протоколов Ethernet (Slow Protocols), предназначенных для выполнения функций, не связанных непосредственно с процессом передачи кадров.

Компоненты протокола LACP

Основными компонентами протокола LACP являются два сетевых устройства с интерфейсами Ethernet/IEEE 802.3, исполняющие правила этого протокола, и каналы передачи данных, связывающие эти устройства.

Определение

Партнером LACP (LACP Partner) называется сетевое устройство с интерфейсами Ethernet/IEEE 802.3, выполняющее правила протокола LACP.

Правила протокола LACP предусматривают, что между партнерами LACP выполняется периодический обмен информационными сообщениями LACPDU (Link Aggregation Control Protocol Data Units). При выполнении этого обмена один из партнеров LACP выполняет функции *ведущего партнера* (Actor Partner) и является инициатором информационного взаимодействия. Обычно ведущий партнер LACP периодически формирует информационные сообщения, однако в некоторых ситуациях он может передать и внеочередное информационное сообщение. Другой партнер LACP является *ведомым партнером* (Passive Partner) и формирует ответные информационные сообщения. Оба партнера при этом входят в одну объединенную группу интерфейсов (Aggregated Group), образующих агрегированный канал. Протокол LACP не

использует механизмов гарантированной доставки информационных сообщений, предполагается, что вероятность потери или искажения информационного сообщения LACPDU невелика. Признаком потери очередного или внеочередного сообщения LACPDU для ведущего партнера является отсутствие реакции со стороны ведомого партнера. В подобных ситуациях ведущий партнер должен повторить передачу потерянного информационного сообщения.

Для выполнения функций протокола LACP в состав прозрачного моста (коммутатора Ethernet) вводится дополнительный блок — агрегатор. Таким образом, каждый из интерфейсов коммутатора предполагается состоящим из двух компонентов: блока внешнего интерфейса — порта и блока внутреннего интерфейса — агрегатора. При этом порт выполняет обработку данных на физическом уровне и на промежуточном уровне MAC-канального уровня. Задачей агрегатора в общем случае является распределение данных между компонентами агрегированного канала на промежуточном уровне, который расположен между уровнями MAC и LLC. Если в агрегированный канал включен только один интерфейс, то агрегатор выполняет только функцию трансляции данных. Задачей агрегатора также является определение состава группы интерфейсов агрегированного канала в соответствии с установленными значениями их ключей.

Определение

Ключом LACP называется совокупность характеристик интерфейса, отражающих его способность участвовать в построении агрегированного канала.

Ключ в сокращенной форме содержит информацию о физических характеристиках интерфейса (например, значение скорости передачи данных) и установках, сделанных администратором сетевого устройства (например, номер агрегированного канала). В агрегированный канал могут входить только интерфейсы с совпадающими значениями ключей. На рис. 10.4 представлена схема построения агрегированных каналов между двумя коммутаторами Ethernet/IEEE 802.3.

В виде больших прямоугольников на этой схеме показаны сетевые интерфейсы коммутаторов SW1 и SW2. Маленькими прямоугольниками на схеме обозначены логические интерфейсы — агрегаторы, а кругами — физические порты соответствующих интерфейсов коммутатора. Для каждого из коммутаторов SW1 и SW2 администратор определил по 2 агрегированных канала. На коммутаторе SW1 первый канал образован сетевым интерфейсом № 8, второй канал — сетевыми интерфейсами № 7, 9 и 10. На коммутаторе SW2 первый канал образован сетевым интерфейсом № 1, второй канал — сетевыми интерфейсами № 2, 3 и 4. Таким образом, первый канал между SW1 и SW2 является индивидуальным, а второй — агрегированным. На рис. 10.4 на при-

надлежность интерфейсов различным каналам указывают значения ключей. Важно отметить, что в каждом из каналов используется только по одному блоку агрегации, который принадлежит интерфейсу с минимальным значением идентификатора. На коммутаторе SW1 это блок агрегации интерфейса № 7, а на коммутаторе SW2 это блок агрегации интерфейса № 2. Назначенный агрегатор используется даже в том случае, если, как это показано на рис. 10.4, соответствующий ему физический интерфейс по каким-либо причинам не вошел в состав агрегированного канала. В данном случае причиной отказа от включения пары интерфейсов SW1/7—SW2/2 в агрегированный канал № 2 является несовпадение установленных для них скоростей передачи данных.

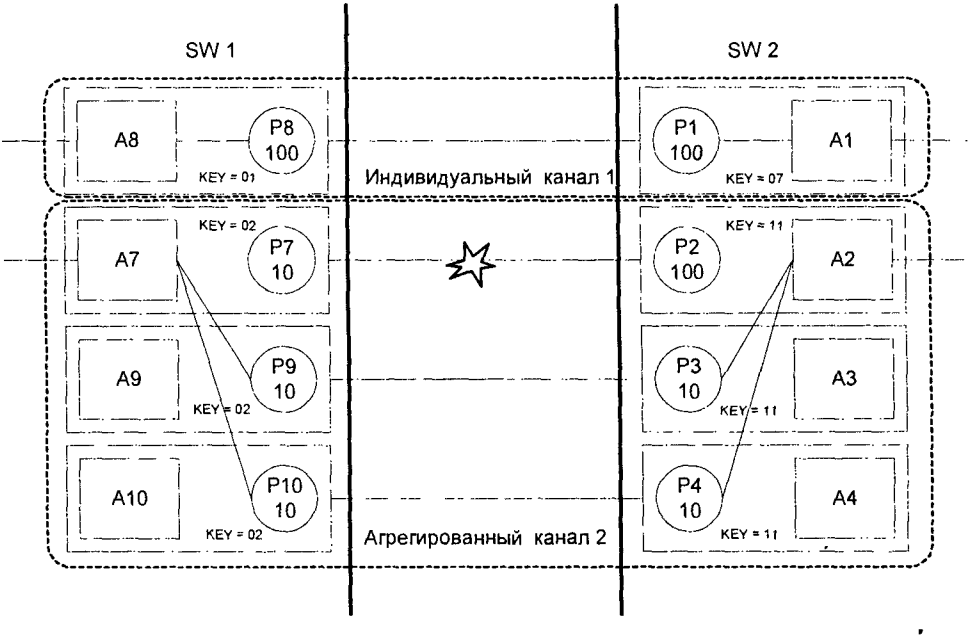


Рис. 10.4. Схема построения агрегированных каналов между коммутаторами Ethernet/IEEE 802.3

Администратор имеет возможность управлять процессом выбора агрегаторов, изменяя индивидуальные приоритеты LACP для выбранных интерфейсов коммутатора. Идентификация партнеров протокола LACP также выполняется с использованием индивидуального MAC-адреса соответствующего сетевого интерфейса (агрегатора).

Структура блока данных LACP

Информационные сообщения протокола LACP инкапсулируются в кадры Ethernet/IEEE 802.3. Структура кадра Ethernet/IEEE 802.3, переносящего ин-

формационные сообщения LACPDU, представлена в табл. 10.2. В качестве адреса назначения этих кадров используется групповой адрес медленных протоколов Ethernet (Slow_Protocols_Multicast Address). Адрес источника в данном случае содержит индивидуальный адрес LACP партнера.

Таблица 10.2. *Структура кадра Ethernet, переносящего информационное сообщение протокола LACP*

Номер поля	Наименование и содержание поля	Значение	Длина поля (байт)
1	DESTINATION ADDRESS — групповой адрес Slow Protocols	01-80-C2-00-00-02	6
2	SOURCE ADDRESS — адрес партнера LACP	—	6
3	LENGTH/TYPE — тип нагрузки — Slow Protocol	88-09	2
4	SUBTYPE — тип Slow Protocol — LACP	01	1
5	VERSION NUMBER — номер версии LACP	01	1
6/15	ACTOR/PARTNER INFORMATION — признак информации партнера LACP	01	1
7/16	ACTOR/PARTNER INFORMATION LENGTH — длина поля информации партнера LACP	14	1
8/17	ACTOR/PARTNER SYSTEM PRIORITY — приоритет партнера LACP	—	2
9/18	ACTOR/PARTNER SYSTEM — идентификатор партнера LACP	—	6
10/19	ACTOR/PARTNER KEY — индивидуальный ключ партнера LACP	—	2
11/20	ACTOR/PARTNER PORT PRIORITY — приоритет порта партнера LACP	—	2
12/21	ACTOR/PARTNER PORT — номер порта партнера LACP	—	2
13/22	ACTOR/PARTNER STATE — состояние порта партнера LACP	—	1
14/23	ACTOR/PARTNER RESERVED — резервное поле	—	3/12
...	...	...	...
	FRAME CHECK SEQUENCE — контрольная последовательность кадра	—	4

- В поле LENGTH/TYPE помещается признак, указывающий на то, что для формирования полезной нагрузки кадра был использован один из медленных протоколов Ethernet (Slow_Protocols_Type).

- В поле SUBTYPE указывается тип медленного протокола, который был использован для формирования полезной нагрузки кадра. Далее перечислены возможные значения поля SUBTYPE и их интерпретация:
  - 0 — не используется — признак ошибочного сообщения;
  - 1 — протокол LACP (Link Aggregation Control Protocol);
  - 2 — протокол маркера LAMP (Link Aggregation-Marker Protocol).
- Содержимое пятого поля протокола LACP — VERSION NUMBER — указывает номер версии протокола LACP, который был использован для формирования информационного сообщения.

Последующие поля 6—23 информационного сообщения LACPDU предназначены для размещения информационных блоков ведущего и ведомого партнеров LACP. Поскольку структура этих полей одинакова, целесообразно привести только их общее описание.

- В полях ACTOR/PARTNER INFORMATION размещается признак того, что в последующих полях сообщения содержится информация ведущего или ведомого партнера LACP:
  - 01 — информация ведущего партнера;
  - 02 — информация ведомого партнера.
- Поля ACTOR/PARTNER INFORMATION LENGTH предназначены для указания длины информационного блока соответствующего партнера LACP. Для обоих партнеров эта длина составляет 20 байт.
- В полях ACTOR/PARTNER SYSTEM PRIORITY размещается приоритет партнера LACP, установленный для него в системе для обеспечения управления процессом со стороны администратора.
- Поля ACTOR/PARTNER SYSTEM используются для размещения идентификатора соответствующего партнера LACP. В качестве таких идентификаторов обычно используют индивидуальные MAC-адреса соответствующих интерфейсов. Полный 8-байтовый идентификатор партнера, который используется для определения соотношения приоритетов партнеров, образуется путем добавления к 6-байтовому значению поля ACTOR/PARTNER SYSTEM двух старших байтов поля ACTOR/PARTNER SYSTEM PRIORITY. Больший приоритет LACP имеет система с меньшим значением полного идентификатора.
- Поля ACTOR/PARTNER KEY предназначены для указания значения индивидуальных ключей, определенных для установления отношений между партнерами LACP. Автоматически в агрегированный канал могут быть включены только те интерфейсы сетевого устройства, значения ключей которых совпадают.

- В полях ACTOR/PARTNER PORT PRIORITY размещаются приоритеты соответствующих портов партнера LACP.
- В полях ACTOR/PARTNER PORT указываются номера портов, используемых для построения агрегированного канала. Полный 4-байтовый идентификатор порта партнера, определяющий соотношение приоритетов портов партнеров, образуется путем добавления к 2-байтовому значению поля ACTOR/PARTNER PORT двух старших байтов поля ACTOR/PARTNER PORT PRIORITY. Больший приоритет LACP имеет порт с меньшим значением полного идентификатора.
- Поле ACTOR/PARTNER STATE используется для размещения восьми флагов признаков текущего состояния партнера LACP. Названия и назначение этих флагов признаков перечислены далее.
  - Флаг LACP_Activity (бит 0 поля ACTOR/PARTNER STATE) используется для указания признака активности партнера. Значение "1" этого флага соответствует признаку активного LACP.
  - Флаг LACP_Timeout (бит 1 поля ACTOR/PARTNER STATE) используется для управления величиной тайм-аута протокола LACP. Значение "1" этого флага соответствует короткому тайм-ауту, "0" — соответствует длинному тайм-ауту.
  - Флаг Aggregation (бит 2 поля ACTOR/PARTNER STATE) используется для указания возможности включения данного интерфейса в агрегированный канал. Значение "1" этого флага указывает на то, что данный интерфейс может быть использован в качестве одного из компонентов агрегированного канала. Значение "0" этого флага указывает на то, что данный интерфейс представляет собой индивидуальный канал передачи данных.
  - Флаг Synchronization (бит 3 поля ACTOR/PARTNER STATE) используется для указания того факта, что данный интерфейс корректно прошел процедуру включения в агрегированный канал (значение "1" данного флага). Значение "0" этого флага указывает на то, что процедура включения данного интерфейса в агрегированный канал была завершена некорректно.
  - Флаг Collecting (бит 4 поля ACTOR/PARTNER STATE) указывает на отношение данного интерфейса к процедуре приема кадров, полученных по агрегированному каналу. В частности, значение "1" этого флага указывает на то, что данный интерфейс участвует в приеме кадров агрегированного канала.
  - Флаг Distributing (бит 5 поля ACTOR/PARTNER STATE) указывает на участие данного интерфейса в процедуре распределения кадров. Значе-

ние "0" этого флага означает, что данный интерфейс не участвует в процедуре распределения кадров, полученных для передачи по агрегированному каналу. Значение "1", наоборот, указывает на то, что интерфейс обычным образом участвует в этой процедуре.

- Значение "1" флага Defaulted (бит 6 поля ACTOR/PARTNER STATE) указывает на то, что текущее состояние партнера определяется автономными настройками. Значение "0" этого флага говорит о том, что исходное состояние партнера было изменено в соответствии с информацией, полученной в LACPDU.
- Значение "1" флага Expired (бит 7 поля ACTOR/PARTNER STATE) указывает на то, что управляющий автомат протокола LACP у партнера находится в состоянии EXPIRED.

Примечание

Значения флагов Defaulted и Expired, полученные во входном информационном сообщении LACPBDU, не анализируются и не используются для выполнения процедур протокола.

Принципы взаимодействия партнеров LACP

Взаимодействие партнеров LACP выполняется при помощи обмена информационными сообщениями. Инициатором этого обмена является ведущий партнер.

Основной задачей информационного обмена LACP является определение текущего состояния интерфейса партнера. В зависимости от этого состояния могут быть выполнены следующие действия:

1. Включение интерфейса в агрегированный канал или исключение интерфейса из агрегированного канала.
2. Включение или выключение функции распределения передаваемых кадров для интерфейса, входящего в агрегированный канал.
3. Включение или выключение функции распределения принимаемых кадров для интерфейса, входящего в агрегированный канал.

Первое из указанных действий выполняется для интерфейса после реализации процедуры сравнения значений ключевых признаков, один из которых был определен для данного интерфейса, а другой был установлен для агрегированного канала. Как правило, на этом этапе выполняется сравнение установленных значений скорости передачи данных, номера агрегированного канала. В некоторых случаях для агрегированного канала ограничивается максимальное количество интерфейсов, которые могут быть в него включены. Если это ограничение превышено и вновь включаемый интерфейс имеет

наименьший приоритет в агрегированной группе, он будет переведен в пассивное состояние. Интерфейсы, которые находятся в этом состоянии, принадлежат агрегированной группе, обмениваются информационными сообщениями, но не принимают участие в процедурах передачи и приема кадров агрегированного канала.

Остальные действия могут быть выполнены только для тех интерфейсов, которые являются членами агрегированной группы и находятся в активном состоянии. Кроме того, эти интерфейсы должны успешно пройти процедуру согласования ключевых признаков с удаленным партнером LACP. Эта процедура выполняется при помощи обмена информационными сообщениями и также предполагает сравнение значений установленных для партнеров, основных признаков, основными из которых являются:

- текущее состояние интерфейса партнера;
- установленное значение скорости передачи данных интерфейса партнера;
- участие интерфейса партнера в процедуре распределения принятых и передаваемых кадров.

В том случае, если все необходимые процедуры согласования были выполнены успешно, оба интерфейса становятся активными участниками агрегированной группы и активно участвуют в передаче данных через объединенный канал.

В процессе этого обмена партнеры LACP обмениваются информационными сообщениями для подтверждения текущего статуса партнера. Ведущий партнер передает сообщения LACPDU с постоянным периодом, величина которого определяется одним из двух установленных значений:

- *Fast_Periodic_Time* = 1 сек (режим короткого тайм-аута);
- *Slow_Periodic_Time* = 30 сек (режим длинного тайм-аута).

Когда ведомый партнер принимает информационное сообщение, он определяет текущий статус ведущего партнера и посылает ответное сообщение LACPDU, в котором в соответствии со своим текущим состоянием формирует поля с 15 по 23.

Примечание

Если оба интерфейса (партнера LACP) были сконфигурированы администратором в качестве ведущих, в процессе согласования параметров тот из них, который имеет меньший приоритет (большее значение идентификатора), автоматически получит статус ведомого.

Используя протокол LACP, оба партнера имеют возможность постоянно контролировать состояние друг друга и в случае изменения этого состояния соответствующим образом изменять конфигурацию агрегированного канала.

Если входящий в агрегированный канал интерфейс одного из партнеров выйдет из строя таким образом, что не сможет сформировать очередное сообщение LACPDU, оставшийся партнер зафиксирует этот факт после истечения времени тайм-аута, величина которого определяется одним из двух установленных значений:

- *Short_Timeout_Time* = 3 сек (режим короткого тайм-аута);
- *Long_Timeout_Time* = 90 сек (режим длинного тайм-аута).

Кроме того, протокол LACP предполагает использование дополнительных таймеров в тех случаях, когда на одном из партнеров производится изменение конфигурации. Таким образом, применение протокола LACP позволяет постоянно контролировать состояние обоих партнеров и, при необходимости, выполнять оперативное изменение конфигурации агрегированного канала.

Рекомендации по созданию и использованию объединенных каналов мультисервисных ЛВС

Агрегированные каналы могут применяться в мультисервисных ЛВС как для обеспечения гибкого резервирования каналов передачи данных, так и для повышения пропускной способности магистральных каналов. Применение технологии агрегирования каналов, так же, как и технологии Spanning Tree, позволяет существенно повысить надежность мультисервисной ЛВС, обеспечивая при этом значительное увеличение скорости передачи данных в магистральных соединениях ЛВС. Однако далеко не во всех случаях применение агрегирования каналов в мультисервисных ЛВС позволяет добиться желаемых результатов. Внедрение этой технологии должно проводиться после детального анализа следующих факторов:

- структуры информационных потоков в ЛВС;
- возможности взаимодействия с используемыми в ЛВС технологиями;
- особенностей применяемого оборудования.

Путем анализа структуры информационных потоков в ЛВС можно определить оптимальные точки подключения и сделать правильный выбор алгоритмов распределения нагрузки в агрегированных каналах. Своевременный анализ возможностей взаимодействия агрегированных каналов с используемыми в ЛВС и перспективными технологиями позволит избежать конфликтов в процессе реализации принятых решений и обеспечит возможность их дальнейшего развития. Очевидно также, что без исследования особенностей применяемого оборудования невозможно корректное и грамотное внедрение выбранных решений.

Применение протокола STP в ЛВС с агрегированными каналами

Использование агрегированных каналов позволяет выполнять построение высокоскоростных магистральных соединений между коммутаторами путем объединения нескольких интерфейсов, однако не избавляет от необходимости использования протокола STP (Spanning Tree Protocol) для управления конфигурацией ЛВС. Агрегирование позволяет избежать появления локальных петель при включении нескольких параллельных интерфейсов между двумя коммутаторами, поскольку все эти интерфейсы образуют единый канал. Однако включение агрегированного канала вполне может привести к возникновению циклического маршрута и, следовательно, может вызвать Broadcast-шторм в ЛВС. Кроме того, современные мультисервисные ЛВС, как правило, имеют в своем составе дублирующие и резервные каналы, коммутаторы горячего резерва, что само по себе приводит к появлению циклических маршрутов в сети. При совместном использовании технологий Spanning Tree и агрегирования каналов необходимо обеспечить:

- адекватное преобразование скорости агрегированного канала в значение стоимости STP COST;
- оптимальное размещение корневого моста.

Для обеспечения эффективного использования агрегированных каналов в мультисервисных ЛВС с кольцевой структурой администратор должен аккуратно управлять настройками протокола STP используемых коммутаторов и внимательно контролировать текущее состояние активной топологии сети (см. *главу 8*). Дело в том, что именно при использовании агрегированных каналов автоматически построенная протоколом STP активная топология ЛВС может быть особенно плохо предсказуема. Во многом это объясняется сложностью алгоритма расчета значения величины STP cost для агрегированного канала, которая, в конечном счете, и определяет, какие именно каналы будут использоваться для передачи данных, а какие останутся заблокированными. Например, в том случае, если величина STP cost для агрегированного канала, построенного из четырех интерфейсов IEEE 802.3 100BaseT, ошибочно будет установлена равной 19 (один интерфейс), агрегированный канал может оказаться заблокированным. На рис. 10.5, *а* приведен пример ЛВС, где агрегированный канал между коммутаторами SW2 и SW4 заблокирован из-за неправильного расчета значения STP cost.

Возникновения подобной ситуации можно избежать, как минимум, двумя способами — путем изменения положения корневого моста рис. 10.5, *б* или путем изменения величины STP cost для агрегированного канала рис. 10.5, *в*. Первый вариант может быть реализован изменением значения приоритета STP PRIORITY на коммутаторе SW2 со значения, установленного по умол-

чанию, — 32768 на меньшее значение, например, 8192. При этом для корректного назначения корневого моста важно, чтобы установленное на коммутаторе SW2 значение STP Priority было наименьшим в данной ЛВС. Аналогичной конфигурации активной топологии ЛВС можно добиться, если изменить значение STP cost на агрегированном канале с ошибочно установленного значения — 19 на меньшее значение, например — 15. В этом случае, открытым для передачи данных останется агрегированный канал, поскольку стоимость проходящего через него корневого маршрута равна 34 (19 + 15), в то время как стоимость заблокированного альтернативного маршрута составит 38 (19 + 19).

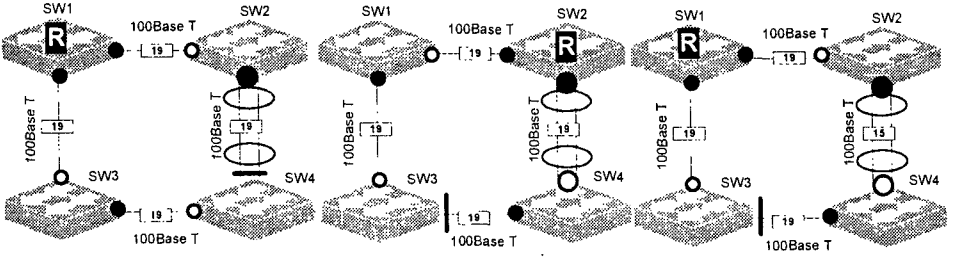


Рис. 10.5. Управление активной топологией STP в ЛВС с агрегированным каналом

Передача группового трафика по агрегированным каналам

Эффективность применения агрегированных каналов ЛВС во многом обеспечивается правильным выбором алгоритма распределения трафика в этих каналах. Одна из основных особенностей организации информационного взаимодействия в мультисервисных ЛВС заключается в широком использовании группового (Multicast) режима передачи данных. При использовании этого режима данные от сервера к абонентам передаются в виде расходящихся потоков. Поэтому через каждый из каналов ЛВС может передаваться не более одного потока для одной группы. Все пакеты, передаваемые в одном групповом потоке, имеют, как правило, один адрес назначения (адрес группы) и один адрес источника (адрес сервера). По этой причине становится ненужным и невозможным использование этих параметров в качестве критериев разделения трафика для выравнивания нагрузки в агрегированном канале. Следовательно, выравнивания нагрузки при передаче группового трафика можно добиться только в том случае, если через канал осуществляется трансляция трафика нескольких Multicast-групп одновременно. Естественно, что в

качестве критерия для разделения трафика при этом можно использовать только IP-адрес назначения пакета, который в данном случае совпадает с номером Multicast-группы.

Примеры построения агрегированных каналов

Как уже было отмечено ранее, создание и обслуживание агрегированного канала на современных коммутаторах Ethernet/IEEE 802.3 может быть выполнено как в ручном режиме, так и в автоматическом режиме. Автоматический режим реализуется с использованием стандартного протокола LACP, требует меньше настроек и предоставляет гораздо больше возможностей для администратора в части обеспечения устойчивости ЛВС к отказам. Настройка агрегирования каналов с использованием протокола LACP в основном сводится к определению индивидуального номера канала, номеров входящих в него интерфейсов и способа распределения трафика между компонентами агрегированного канала.

На рис. 10.6 приведена схема мультисервисной сети, магистральные каналы которой построены на основе агрегированных интерфейсов Ethernet/IEEE 802.3. Для обслуживания клиентов, подключаемых к периферийным коммутаторам SW3 и SW4, в этой сети используются два сервера S1 и S2, подключенных к центральным коммутаторам SW1 и SW2 соответственно. Все магистральные каналы в этой сети образованы парами интерфейсов IEEE 802.3 1000BaseT или 100BaseT.

Учитывая особенности взаимного расположения серверов и клиентов, в качестве критерия распределения трафика между компонентами агрегированного канала в данном случае целесообразно выбрать комбинацию IP-адреса источника и IP-адреса назначения. Для обеспечения стабильности конфигурации активной топологии в данной ЛВС целесообразно также определить положение основного и резервного корневых мостов. На эти роли, с учетом расположения серверов и пропускной способности каналов ЛВС, больше всего подходят коммутаторы SW1 и SW2 соответственно.

В листинге 10.1 приведен пример настройки агрегированных каналов с использованием протокола LACP на коммутаторе SW1 (Cisco Systems Catalyst 3750-24TS)

Листинг 10.1. Применение протокола LACP для построения агрегированных каналов на коммутаторе Cisco Systems

```
1. Определение данного коммутатора в качестве корневого
   для VLAN1-1024
spanning-tree vlan 1-1024 root primary
```

2. Определение метода выравнивания нагрузки между компонентами агрегированного канала

```
port-channel load-balance src-dst-ip
```

3. Установка значения приоритета партнера LACP

```
lacp system-priority 100
```

4. Переход в режим конфигурирования группы интерфейсов

```
interface range fastEthernet 0/1 – 2
```

5. Определение типа протокола автоматического агрегирования канала

```
channel-protocol lacp
```

6. Определение номера агрегированного канала и статуса партнера

```
channel-group 1 mode active
```

7. Определение приоритета интерфейса в агрегированном канале*

```
lacp port-priority 100
```

8. Переход в режим конфигурирования агрегированного канала

```
interface port-channel 1
```

9. Установка значения STP cost для агрегированного канала**

```
spanning-tree cost 15
```

10. Выход из режима конфигурирования и сохранение изменений в энергонезависимом ЗУ

```
exit
write memory
```

11. Примечания: команды помеченные символами * и **, не являются обязательными для данной структуры ЛВС.

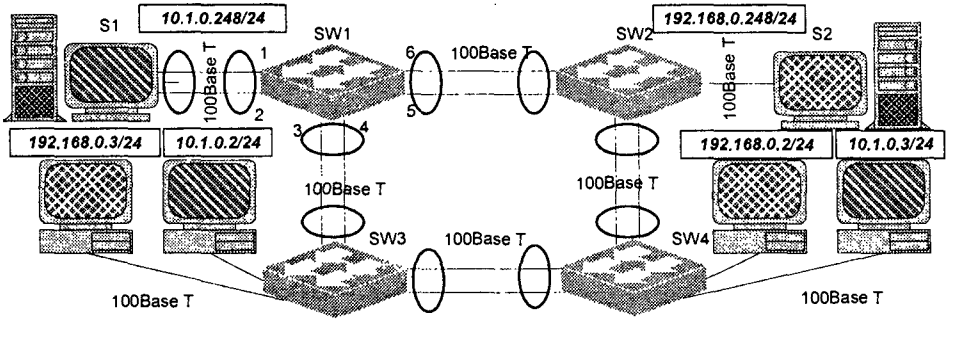
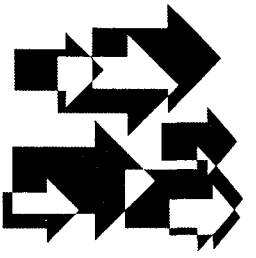


Рис. 10.6. Применение агрегированных каналов для построения магистралей мультисервисной ЛВС

ГЛАВА 11



Организация группового вещания в мультисервисных ЛВС

Эта глава посвящена рассмотрению особенностей использования режима группового обмена (Multicast) для передачи данных в мультисервисных сетях. Поскольку групповой режим предназначен для оптимизации передачи информационных потоков через сети общего назначения, то применение этого режима позволяет существенно повысить эффективность использования каналов передачи данных в ЛВС.

Режим группового обмена данными удачно сочетает в себе основные достоинства одноадресного и широковещательного режимов. Так же, как и режим индивидуального, одноадресного обмена, групповой режим позволяет создавать в сети направленные информационные потоки. Групповой режим обмена так же, как и широковещательный, не требует создания индивидуального информационного потока для каждого из абонентов. Именно поэтому Multicast-режим активно используется для организации группового вещания в современных мультисервисных сетях.

Однако для того, чтобы достоинства группового режима обмена при организации вещания в мультисервисной сети проявились наиболее полно, необходимо, чтобы при построении этой сети были учтены специфические особенности организации информационного обмена на канальном и сетевом уровне OSI ISO 7498 в этом режиме. Кроме того, при интенсивном использовании Multicast-режима к характеристикам активного оборудования ЛВС предъявляется ряд дополнительных требований (например, необходимость прослушивания сообщений протокола IGMP), невыполнение которых может привести к резкому снижению качества передачи данных в сети.

В первом разделе данной главы рассматриваются основные особенности и преимущества организации режима группового обмена в мультисервисных ЛВС.

Второй раздел посвящен рассмотрению основных принципов организации и практической реализации группового обмена на канальном уровне в сетях Ethernet/IEEE 802.3. В этом разделе рассматривается протокол IGMP и особенности его использования в мультисервисных сетях.

В третьем разделе рассматриваются особенности организации группового вещания на сетевом уровне OSI ISO 7498 и основные протоколы групповой маршрутизации.

Особенности режима группового обмена

В *главе 6* было отмечено, что для обеспечения передачи данных в современных мультисервисных сетях может быть использован один из трех основных режимов информационного обмена:

- Broadcast — широковещательный;
- Unicast — одноадресный;
- Multicast — групповой.

Режим Broadcast (безадресная широковещательная передача) предназначен для передачи данных всем абонентам сети и используется в основном в технологических целях — в передаче информации о маршрутах, в определении адреса сервера и т. д. Область распространения сообщений этого типа обычно ограничена локальным сегментом сети.

Режим Unicast (одноадресная передача) используется в том случае, когда адрес назначения точно известен источнику информации. В этом случае в информационном обмене участвуют только два узла сети (если не считать маршрутизаторы) — передатчик и приемник. Этот режим информационного обмена традиционно является основным, на его долю приходится от 90 до 99% всего информационного обмена в сети TCP/IP.

Использование режима Multicast (групповая многоадресная передача) в вычислительных сетях целесообразно в тех случаях, когда передаваемая информация предназначена для группы приемников. Такой режим может быть эффективно использован при организации группового вещания по принципу "один для многих". Использование режима многоадресной передачи в данном случае позволяет значительно более экономно использовать пропускную способность вычислительной сети — поскольку передается только одна порция информации для всех приемников. Функция тиражирования блоков данных при этом возлагается на промежуточные сетевые устройства — групповые маршрутизаторы. Эти устройства периодически опрашивают потенциальных потребителей и используют специальные алгоритмы маршрутизации для того, чтобы определить необходимость ретрансляции группового трафика через

те или иные свои интерфейсы. Поскольку источник группового трафика формирует только один поток данных независимо от количества приемников, пропускная способность его канала не оказывает практически никакого влияния на темп информационного обмена. Увеличение числа приемников группового трафика может привести только к подключению новых ветвей сети, по которым распространяется этот трафик. Важно то, что интенсивность информационного потока на существующих ветвях при этом никак не изменяется.

На рис. 11.1 приведена схема организации информационного обмена с использованием групповых адресов. В этом примере маршрутизатор ГМ2 формирует две копии блоков данных, получаемых от источника 224.0.1.128, поскольку потребители этого трафика подключены к двум его интерфейсам. Групповой маршрутизатор обязан передавать групповой трафик до тех пор, пока у него есть хотя бы один потребитель этого трафика. При этом один групповой маршрутизатор может быть использован для обеспечения информационного обмена нескольких Multicast-групп одновременно. На приведенном примере маршрутизаторы ГМ1 и ГМ2 обслуживают по две группы.

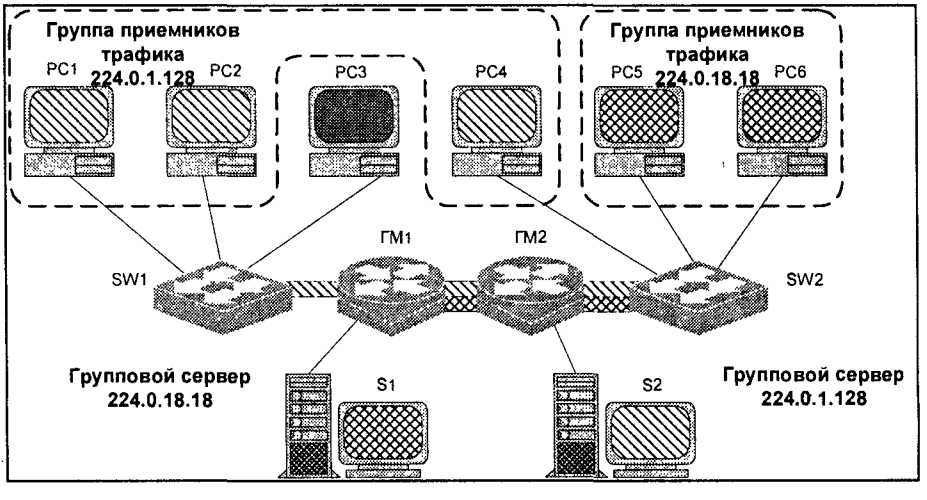


Рис. 11.1. Схема организации информационного обмена с использованием групповых адресов

Основным недостатком, свойственным режиму Multicast, является то, что при его использовании возникают существенные затруднения при организации гарантированной доставки сообщений и управления темпом информационного обмена. Эти недостатки, однако, могут быть частично скомпенсированы благодаря использованию специальных режимов информационного обмена.

Групповые адреса TCP/IP

Для обеспечения режима групповой адресации в сети TCP/IP используется специальный класс адресов — класс "D". Групповые адреса Интернета находятся в диапазоне от 224.0.0.1 до 239.255.255.255. В отличие от адресов Unicast групповые адреса назначаются не узлам, а группам узлов. При этом один и тот же групповой адрес имеет все узлы, входящие в такую группу.

Примечание

Групповые адреса при формировании дейтаграмм TCP/IP могут быть использованы только в качестве адресов назначения.

Например, узлам P, Q и R назначен один групповой адрес — X. Тогда для того, чтобы отправить дейтаграмму всем трем узлам (P, Q и R), достаточно отправить ее по адресу X.

Весь диапазон групповых адресов TCP/IP разделен на несколько функциональных блоков специального назначения.

В табл. 11.1 приведены диапазоны функциональных блоков групповых адресов, зарезервированных организацией IANA.

Таблица 11.1. *Адреса функциональных блоков групповых адресов*

Диапазон	Наименование	Назначение
224.0.0.0—224.0.0.255	Local Network Control Block	Адреса компонентов локальной сети
224.0.1.0—224.0.1.255	Internetwork Control Block	Адреса компонентов глобальной сети
224.0.2.0—224.0.255.0	AD-HOC Block	Блок специальных адресов
224.1.0.0—224.1.255.255	ST Multicast Groups [RFC 1190, KS14]	Блок адресов Internet Stream Protocol
224.2.0.0—224.2.255.255	SDP/SAP Block	Блок динамически назначаемых и технологических адресов
224.3.0.0—224.251.255.255	Reserved	Зарезервировано IANA
225.0.0.0—231.255.255.255	Reserved	Зарезервировано IANA
232.0.0.0—232.255.255.255	Source Specific Multicast	Блок адресов групп с ограниченным перечнем источников
233.0.0.0—233.255.255.255	GLOP Block — [RFC 3180]	Блок адресов, статически назначаемых по схеме GLOP
234.0.0.0—238.255.255.255	Reserved [IANA]	Зарезервировано IANA
239.0.0.0—239.255.255.255	Administratively Scoped [IANA, RFC 2365]	Блок адресов для административно-ограниченных областей

Локальные групповые адреса

Локальные групповые адреса IP используются, как правило, для технологических целей. Различные протоколы сети Интернет используют адреса этого диапазона для обеспечения информационного обмена между своими компонентами вместо адресов Broadcast, что обеспечивает более эффективное использование ресурсов локальной сети. Например, адрес 224.0.0.9 используется маршрутизаторами RIP II для передачи обновлений маршрутной информации.

Часть адресов из диапазона 224.0.0.0/24 относится к группе широко известных (well known), назначение некоторых из этих адресов приведено в табл. 11.2. Распространение IP-дейтаграмм с групповыми адресами локального диапазона ограничивается локальным сегментом сети независимо от установленного значения TTL (нормальным значением TTL для дейтаграмм такого типа является 1).

В табл. 11.2 приведены групповые адреса некоторых компонентов локальных сетей.

Таблица 11.2. *Групповые адреса ряда компонентов локальных сетей*

Начальный адрес	Назначение
224.0.0.1	Узлы, которые используют групповой режим адресации
224.0.0.2	Маршрутизаторы, которые обеспечивают групповой режим адресации
224.0.0.3	Маршрутизаторы DVRMP
224.0.0.5	Маршрутизаторы OSPF
224.0.0.6	Назначенные (DR) маршрутизаторы OSPF
224.0.0.9	Маршрутизаторы RIP II
224.0.0.13	Маршрутизаторы PIM

Блок 239.0.0.0—239.255.255.255 образует динамически и статически назначаемые групповые адреса, предназначенные для использования внутри замкнутых областей. По своему назначению адреса этого диапазона аналогичны адресам частных сетей, назначаемых в соответствии с рекомендациями IETF RFC 1918 (Address Allocation for Private Internets).

Глобальные Multicast-адреса TCP/IP

Групповые адреса диапазона 224.0.1.0/24 предназначены для организации Multicast-групп, компонентами которых являются узлы глобальной сети. Распространение по сети Интернет трафика, направленного в эти адреса, может быть ограничено только временем существования дейтаграммы в сети (TTL).

Назначение адресов из этого диапазона производится статически путем согласования и выпуска необходимых организационных документов. Глобальные групповые адреса могут быть использованы как для организации сетевого вещания, так и для корпоративных технологических целей. Например, адрес 224.0.1.40 зарезервирован корпорацией Cisco Systems для обеспечения поиска групповых маршрутизаторов (CISCO-RP-DISCOVERY), а право использования группового вещания по адресу 224.0.1.128 закреплено за корпорацией CNN.

В специальный блок выделены традиционно определенные групповые адреса, принцип использования которых не совпадает с принципами использования адресов первой и второй групп. Групповые адреса AD-HOC применяются для обеспечения приложений, оперирующих с небольшим количеством Multicast-групп. Назначение адресов этого диапазона, как правило, производится без санкции организации IANA.

В блок SDP/SAP входят как технологические адреса этих протоколов, так и адреса, присваиваемые динамически источникам группового трафика. Протокол объявления сессий — протокол *SAP* (Session Announcement Protocol) применяется источником группового трафика для того, чтобы занести свою сессию в список анонсируемых сессий. Благодаря тому, что информация об анонсируемых сессиях свободно распространяется по сети, любой желающий может получить перечень зарегистрированных активных источников при помощи протокола описания сессий — протокола *SDP* (Session Description Protocol).

Блок адресов групп с ограниченным перечнем источников предназначен для использования группами, которые применяют расширенную процедуру группового информационного взаимодействия. Приемники группового трафика — члены таких групп, в частности, могут явно определять перечень допустимых источников для поставки им группового трафика.

Адреса блока GLOP применяются при использовании специальной практики статического назначения групповых адресов. Уникальность групповых адресов в этом случае обеспечивается без участия организации IANA благодаря тому, что в групповой адрес включается уникальный номер автономной системы источника группового трафика. Номер автономной системы размещается во втором и третьем байте адреса. Младший байт при этом используется для назначения адресов различным группам внутри системы.

Групповые адреса, которые имеют глобальное значение, присваиваются группам централизованно с использованием специальных динамических процедур. В соответствии с этими процедурами пространство групповых адресов распределяется по иерархическому принципу, когда домен нижнего уровня арендует у домена верхнего уровня блок адресов на ограниченный период времени. Однако вследствие глобального характера сети TCP/IP прак-

тическая реализация таких процедур представляется весьма затруднительной для практической реализации.

Принципы организации группового обмена

Назначение группового адреса узлу можно рассматривать как обобщение его персонального IP-адреса. В то время как индивидуальный IP-адрес узла отображается в адрес канального уровня этого узла, групповой Multicast-IP-адрес должен отображаться в группу адресов канального уровня. Групповая адресация в сети с множественным доступом Ethernet — это, пожалуй, самый естественный способ построения Multicast-IP-адресации при реализации доставки на канальном уровне.

Особенности формирования группового адреса

Специальный диапазон адресов канального уровня сети Ethernet предназначен для формирования групповых Multicast-адресов. Групповые Ethernet-адреса канального уровня, предназначенные для отображения групповых адресов интернет-сети, занимают область адресов с 01-00-5E-00-00-00 по 01-00-5E-7F-FF-FF.

IP-адрес группы узлов ассоциируется с Ethernet Multicast-адресом следующим образом: 23 младших бита IP-адреса группы помещаются в 23 младших бита группового Ethernet-адреса. Вследствие того, что диапазон групповых адресов канального уровня существенно меньше диапазона адресов сетевого уровня, такое отображение не может быть однозначным. Одному Multicast Ethernet-адресу можно поставить в соответствие 31 IP-группу.

Например, IP-адрес 224.1.10.111 соотносится с адресом 01-00-5E-01-0A-6F. Аналогичным образом с этим адресом канального уровня могут быть соотнесены и такие групповые адреса: 224.129.10.111, 225.1.10.111 и т. п.

Определение состава группы

Основным понятием в групповой адресации является понятие Multicast-группы узлов.

Определение

Multicast-группой называется группа узлов, имеющих одинаковый адрес из диапазона адресов 224.0.0.0—239.255.255.255.

Multicast-группа не накладывает никаких ограничений на количество и расположение членов Multicast-группы. Узел может быть членом одной или нескольких Multicast-групп одновременно.

Членом группы может стать любой узел Н, который подключен к сети, после того, как он выполнит процедуру установления своего членства в группе GA. Процедура установления членства в группе начинается передачей запроса с указанием адреса группы GA по адресу группового маршрутизатора (ГМ). В том случае, если маршрутизатор уже принимает трафик, адресованный членам этой группы, никаких дополнительных действий не предпринимается. Такая ситуация возникает тогда, когда в том сегменте сети, в котором находится узел Н, уже имеются члены группы GA. В том случае, если узел Н является первым или единственным членом этой группы, маршрутизатор должен выполнить действия, которые обеспечивают передачу ему трафика группы GA. Для того чтобы определить оптимальный путь в сети, по которому маршрутизатору ГМ должен быть передан трафик группы GA, используются специальные алгоритмы маршрутизации.

Организация доставки группового трафика

В отличие от одноадресного режима передачи данных, при передаче данных с использованием групповой адресацией основные усилия по организации информационного взаимодействия возлагаются на принимающую сторону. Передатчик — формирователь группового трафика не знает адресов станций, которые принимают его данные, сколько таких приемников и есть ли они вообще. Основные действия по доставке группового трафика до конечного абонента выполняются активными компонентами сети — групповыми маршрутизаторами.

При информационном обмене с использованием групповых адресов маршрутизатор должен поддерживать следующие дополнительные компоненты протокола IP:

- таблицу маршрутизации Multicast-группы, содержащую информацию о ближайшем шлюзе для каждой сети;
- таблицу членов Multicast-группы сети, содержащую запись о каждой Multicast-группе в данной сети и о других сетях, которые содержат членов этой же Multicast-группы;
- таблицу членов Multicast-группы узла. Таблица содержит записи, по одной для каждой Multicast-группы, члены которой расположены в сети, непосредственно подсоединенной к данному узлу, т. е. каждая запись определяет один из узлов, который является членом данной группы.

Узел отправляет многоадресную дейтаграмму, используя обычный способ отправки дейтаграмм. Дейтаграмма, адресованная группе узлов, сначала отправляется на шлюз, присоединенный к сети отправителя. Шлюз, по таблице членов Multicast-группы, определяет адреса сетей, куда следует переправить

эту Multicast-дейтаграмму. Если требуемая сеть подсоединена к шлюзу напрямую, то он передает туда копию дейтаграммы, используя групповой адрес канального уровня. В том случае, если искомая сеть не входит в состав непосредственно подключенных сетей данного маршрутизатора, дейтаграмма снабжается заголовком канального уровня, который обеспечивает ее доставку до следующего группового маршрутизатора.

Групповое взаимодействие на канальном уровне

Основные задачи по обеспечению доставки группового трафика абонентам в ЛВС решаются благодаря использованию протокола *IGMP* (Internet Group Management Protocol: IETF RFC 2236: November 1997: Status: PROPOSED STANDARD).

В сетях, используемых для передачи группового трафика, протокол IGMP играет такую же роль, какую играет протокол ICMP (Internet Control Message Protocol) в обычной сети Интернет. Основной функцией протокола IGMP является определение динамического членства в группе. Маршрутизатор узнает о наличии потребителей группового трафика в подключенных к нему сегментах сети с помощью специальных сообщений протокола IGMP.

Протокол IGMP

Процедуры протокола IGMP выполняют объекты двух типов:

- групповые маршрутизаторы;
- узлы — потребители группового трафика.

Свою потребность в приеме трафика некоторой группы, имеющей групповой адрес назначения — *GDA* (Group Destination Address), узел может обозначить по собственной инициативе либо в ответ на соответствующий запрос, переданный групповым маршрутизатором.

Групповой маршрутизатор периодически передает запросы (Query) потенциальным потребителям группового трафика и обрабатывает полученные от них ответы (Report). Для определения потребности в групповом трафике у абонентов подключенного к нему сегмента сети маршрутизатор формирует запросы двух видов:

- *общий запрос* (`General Membership Query`);
- *специальный запрос* (`Group-Specific Membership Query`).

Общий запрос `General Membership Query` предназначен для определения потребности в групповом трафике без указания адреса конкретной группы. На

такой запрос должны отвечать все узлы — потенциальные потребители группового трафика с указанием группового адреса GDA. Такой запрос групповой маршрутизатор отправляет, используя в качестве адреса назначения групповой адрес 224.0.0.1 ("всем узлам, принимающим групповой трафик").

Специальный запрос `Group-Specific Membership Query` предназначен для определения потребности в групповом трафике некоторой группы. На такой запрос должны отвечать только те узлы, которые заинтересованы в приеме группового трафика группы, имеющей GDA.

Пакеты запросов `General Membership Query` и `Group-Specific Membership Query` отличаются только содержанием поля Group Address: у общего запроса содержимое этого поля соответствует IP-адресу 0.0.0.0, а у специального запроса в этом поле размещается конкретное значение адреса группы.

Для обеспечения более эффективного использования пропускной способности сети при выполнении процедуры IGMP может быть использован специальный алгоритм подавления дублирующих ответов узлов на запросы активного группового маршрутизатора. В этом случае активный маршрутизатор снабжает каждый свой запрос параметром Max Response Time (максимальное время для ответа). Получив такой запрос, узел, заинтересованный в приеме группового трафика, отвечает на него с задержкой, случайным образом распределенной в диапазоне (0, Max Response Time). В том случае, если до истечения вычисленного временного интервала узел зафиксирует передачу ответного сообщения другим членом группы, данный узел не формирует собственное ответное сообщение.

Формат сообщения IGMP

В настоящее время используются три версии протокола IGMP. Отличия между различными версиями протокола заключаются в номенклатуре и способе обработки формируемых сообщений. Далее будут рассматриваться сообщения и алгоритмы их обработки второй версии протокола IGMP v2.

Все сообщения протокола IGMP инкапсулируются в IP-дейтаграммы с полем PROTOCOL — "тип протокола" равным 2.

В листинге 11.1 приведена структура кадра Ethernet, содержащего сообщение протокола IGMP. Данный листинг получен с использованием программного анализатора протоколов SoftPerfect Network Protocol Analyzer компании SoftPerfect Research. Анализируемый кадр содержит IGMP-запрос, передаваемый от группового сервера 10.0.2.129 для абонентов Multicast-группы 239.255.255.255. Для обеспечения требуемого уровня качества обслуживания у этого кадра установлено предельное значение признака QoS сетевого уровня в формате IPprec = 6.

Листинг 11.1. Структура кадра Ethernet, содержащего сообщение протокола IGMP

```
1. Заголовок канального уровня (Ethernet)
   Destination: 01:00:5E:7F:FF:FF
   Source: 00:12:01:27:09:7F
   Type: 0x0800 Internet Protocol
2. Заголовок сетевого уровня (IPv4)
   Version: 4 (IP, Internet Protocol)
   Header length: 5 (20 bytes)
   Type of service: 0xC0
          110..... (Internetwork Control)
          ...0.... (Normal delay)
          ....0... (Normal throughput)
          .....0.. (Normal relibility)
          ......0. (Normal monetary cost)
          .......0 (Reserved flag is not set)
   Total length: 28 bytes
   Identification: 4458
   Flags: 0x00
          DF .0..... (May fragment)
          MF ..0..... (Last fragment)
   Fragment offset: 0
   Time to live: 1 hops (seconds)
   Protocol: IGMP (0x02)
   Header checksum: 0xAB36 (Correct)
   Source IP: 10.0.2.129
   Destination IP: 239.255.255.255
   No options
Data (26 bytes)
```

Сообщения протокола IGMP могут иметь переменную длину и снабжаются специальным заголовком. Структура заголовка сообщения IGMP приведена в табл. 11.3.

Таблица 11.3. *Структура заголовка сообщения протокола IGMP*

Номер поля	Наименование и содержание поля	Длина поля (байт)
1	TYPE — тип сообщения IGMP	1
2	MAX RESPONSE TIME — максимальное время задержки ответа	1
3	CHECKSUM — контрольная сумма заголовка	2
4	GROUP ADDRESS — групповой адрес GDA	4

Как уже было отмечено, основными сообщениями протокола IGMP являются запросы (Query), которые передает маршрутизатор, и ответы (Report), формируемые узлами. Основные типы сообщений протокола IGMP приведены в табл. 11.4.

Таблица 11.4. *Основные типы сообщений протокола IGMP*

TYPE	Источник	Тип сообщения IGMP	Назначение сообщения
0x11	Маршрутизатор	`Membership Query`	Запрос к членам группы
0x12	Узел	`Membership Report` IGMP v1	Ответ членов группы (версия 1)
0x16	Узел	`Membership Report` IGMP v2	Ответ членов группы (версия 2)
0x17	Узел	`Leave Group`	Отключение от группы

Код сообщения второй версии протокола IGMP сформирован таким образом, чтобы обеспечить совместимость форматов сообщений с первой версией протокола. В первой версии IGMP используются только два типа сообщения `Membership Query` (код 1) и `Membership Report IGMP` (код 2). В первом полубайте первого байта сообщения протокола IGMP v1 размещался номер версии протокола — 1. Поэтому коды сообщений `Membership Query` и `Membership Report IGMP`, формируемых в первой версии протокола, равны 11 и 12 соответственно.

Содержимое поля MAX RESPONSE TIME является осмысленным только для сообщений `Membership Query`, формируемых групповым маршрутизатором. В это поле групповой маршрутизатор, использующий вторую версию протокола IGMP, помещает максимальную величину временного интервала задержки ответа на данное сообщение. Значение задержки выражается в десятых долях секунды. Поскольку маршрутизатор, применяющий протокол IGMP v1, не формирует поле MAX RESPONSE TIME (точнее это поле при использовании протокола IGMP v1 формируется равным 0), считается, что по умолчанию значение поля MAX RESPONSE TIME равно 100 (10 сек). Во всех остальных сообщениях протокола IGMP поле MAX RESPONSE TIME не формируется и не анализируется.

Контрольная сумма сообщения IGMP предназначена для обеспечения обнаружения искажений информации при передаче сообщения по сети. Контрольная сумма занимает два байта в заголовке сообщения IGMP и вычисляется суммированием всех полей исходного сообщения, за исключением собственно поля CHECKSUM. Если значение вычисленной приемником контрольной суммы не совпадает с переданным значением, сообщение IGMP считается искаженным и уничтожается.

В поле GROUP ADDRESS размещаются групповые адреса сети Интернет. Содержание и назначение этого поля определяется типом сообщения IGMP. При передаче сообщения General Membership Query в поле GROUP ADDRESS помещается код 0.0.0.0. При формировании специального запроса Group-Specific Membership Query в это поле должен быть помещен адрес группы, для которой требуется установить наличие приемников. В сообщениях Membership Report, формируемых узлами — приемниками группового трафика, в поле GROUP ADDRESS должен быть размещен групповой адрес GDA той группы, в которой участвует или желает участвовать этот узел. В сообщении Leave Group в этом поле узел размещает адрес той группы, в которой он не желает больше участвовать.

В листинге 11.2 приведены структуры сообщений Group-Specific Membership Query и Membership Report, сформированных в процессе группового обмена мультисервисной сети (заголовки сообщений IGMP отмечены маркером, т. е. серым цветом). В качестве MAC-адреса назначения кадров использован адрес канального уровня, соответствующий адресу GDA: 239.255.0.23 01-00-5E-7F-00-17.

Листинг 11.2. Структура сообщений протокола IGMP

```
    1. Кадр, содержащий сообщение протокола IGMP Group-Specific
       Membership Query
0100 5E7F 0017 0012 0127 097F 0800 45C0 001C 10DB 0000 0102 ABAE 0A00
0281 EFFF 0017 110A FEDE EFFF 0017 8486 0000 0000 0000 0000 0000 0000
0000 0000
    TYPE=11
    MAX RESPONSE TIME = 10(100s)
    CHECKSUM = FEDE
    GROUP ADDRESS = 239.255.0.23
    2. Кадр, содержащий сообщение протокола IGMP Membership Report
0100 5E7F 0017 YYYY YYYY YYYY 0800 4600 0020 DEA4 0000 0102 08E5 D431
XXXX EFFF 0017 9404 0000 1600 F9E8 EFFF 0017
    TYPE=16
    MAX RESPONSE TIME = 0
    CHECKSUM = F9E8
    GROUP ADDRESS = 239.255.0.23
```

Для обеспечения обратной совместимости с первой версией протокола, сообщение протокола IGMP может содержать дополнительные поля и быть длиннее 8 байтов. Хотя маршрутизаторы и узлы, применяющие вторую версию протокола, могут игнорировать содержимое этих полей, однако следует учитывать, что при вычислении контрольной суммы сообщения суммируются все поля сообщения — в том числе и дополнительные.

Дополнительные функции протокола IGMP

Последняя, третья, редакция протокола IGMP изложена в документе IETF RFC 3376: Internet Group Management Protocol, Version 3. October 2002. Status: PROPOSED STANDARD. В дополнение к основным функциям предыдущих версий (IGMP v1 и IGMP v2) в новой версии обеспечена возможность использования дополнительного режима информационного обмена с применением групповых адресов — Source Specific Multicast. Особенность этого режима заключается в том, что при его использовании узлы, заинтересованные в приеме группового трафика, могут определять адреса поставщиков такого трафика. Эта дополнительная возможность позволяет обеспечить более высокий уровень информационной безопасности и более эффективное использование ресурсов вычислительных сетей. Благодаря использованию дополнительных сообщений новой версии протокола узел может определить как адреса желательных поставщиков группового трафика (белый список), так и адреса нежелательных поставщиков (черный список).

Практическая реализация протокола IGMP в современных сетях

В современных сетях использование всех преимуществ информационного взаимодействия с применением групповых адресов невозможно без включения дополнительных функций в существующие сетевые инфраструктуры.

Совершенно очевидно, что схема информационного взаимодействия с использованием групповых адресов изначально достаточно плохо согласуется с современной концепцией построения сети. Это происходит потому, что режим группового информационного обмена в отличие от одноадресного режима предполагает активность приемника, а не источника трафика. Действительно, используя стандартный режим обучения, коммутатор не сможет установить потребность некоторого узла в групповом трафике, поскольку групповые адреса могут быть использованы только в качестве адресов назначения. Следовательно, коммутатор должен будет обрабатывать групповой трафик, так же как и широковещательный, т. е. передавать его на все активные порты. Однако в отличие от широковещательного трафика групповой трафик имеет большую интенсивность, поэтому наличие даже всего одного потребителя такого трафика в сети может привести к существенному уменьшению пропускной способности вследствие загрузки портов коммутатора невостребованным групповым трафиком.

Описанная проблема может быть решена тремя способами:

- статическим конфигурированием коммутатора;
- получением коммутатором информации о членах групп от группового *маршрутизатора;*
- посильным участием коммутатора в процедурах протокола IGMP.

Наиболее перспективным представляется третий способ решения указанной проблемы. В этом случае, для обеспечения автоматического построения таблицы коммутации для обработки группового трафика коммутатор берет на себя часть функций устройства третьего уровня OSI. При этом коммутатор должен анализировать содержимое пакетов, выискивая среди них пакеты протокола IGMP. Именно поэтому подобные методы и получили свое название: *прослушивание (snooping) сообщений IGMP*. Применение подобных методов, безусловно, приводит к резкому увеличению вычислительной нагрузки коммутатора. Поэтому выполнение коммутатором описанных функций возможно только в том случае, если для этих целей будут использоваться специализированные интегральные микросхемы.

Прослушивание сообщений IGMP коммутаторами ЛВС

Формирование таблицы коммутации для обработки группового трафика коммутатор может выполнить самостоятельно в том случае, если будет анализировать сообщения, направляемые групповому маршрутизатору. На первый взгляд, схема информационного обмена в данном случае существенно упрощается. Коммутатор принимает сообщение IGMP `Membership Report`, анализирует его и устанавливает канальный адрес группы, к которой хочет подключиться потребитель группового трафика. Поскольку номер порта, к которому подключен потребитель, в данном случае, определить очень легко, то корректировка таблицы коммутации выполняется также несложно. Когда коммутатор получит сообщение `Leave Group`, сформированное этим потребителем, он произведет обратные действия и извлечет номер порта потребителя из своей таблицы коммутации.

На самом деле информационный обмен производится по существенно более сложной схеме, поскольку коммутатор должен учитывать следующие факторы:

1. При получении сообщения `Leave Group` обязательно нужно провести проверку его достоверности, поскольку оно вполне может быть послано не последним членом группы.
2. Узлы, использующие протокол IGMP v1, вообще не способны формировать сообщения `Leave Group`.
3. Коммутатор должен уметь определять, к какому из его портов подключен групповой маршрутизатор для того, чтобы не отправлять полученные сообщения протокола IGMP во все порты.
4. Сообщение протокола IGMP `Membership Report` формируют не только узлы, намеревающиеся стать членами группы, но и в основном, те, которые уже являются членами этой группы.

Рассмотрим пример сети, представленной на рис. 11.2, *а*. После получения на первый порт IGMP-сообщения `Membership Query` коммутатор может с уверенностью констатировать, что к этому порту подключен групповой маршрутизатор. В ответ на полученное сообщение `Membership Query` узлы, заинтересованные в приеме группового трафика, формируют ответные IGMP-сообщения `Membership Report`. При обработке IGMP-сообщений `Membership Report` коммутатор должен проанализировать, не является ли пославший его узел новым членом данной группы. В таком случае коммутатор выполняет корректировку таблицы коммутации, добавляя новый порт в существующую группу.

Коммутатор, выполняющий прослушивание сообщений IGMP, принимает на себя также некоторые дополнительные функции, такие, например, как функция проверки достоверности принимаемых IGMP-сообщений `Leave Group`. В примере, представленном на рис. 11.2, *б*, узел MAC3 сформировал сообщение IGMP `Leave Group`, не будучи последним членом группы 224.0.18.18 на своем сегменте сети. Коммутатор вместо того, чтобы отправить это сообщение групповому маршрутизатору, может сам выполнить проверку его достоверности. Для этого коммутатор должен направить в сегмент собственное сообщение `Membership Query`. Поскольку в рассматриваемом примере на это сообщение было получено сообщение `Membership Report` от узла MAC4, коммутатору не следует передавать сообщение `Leave` на групповой маршрутизатор.

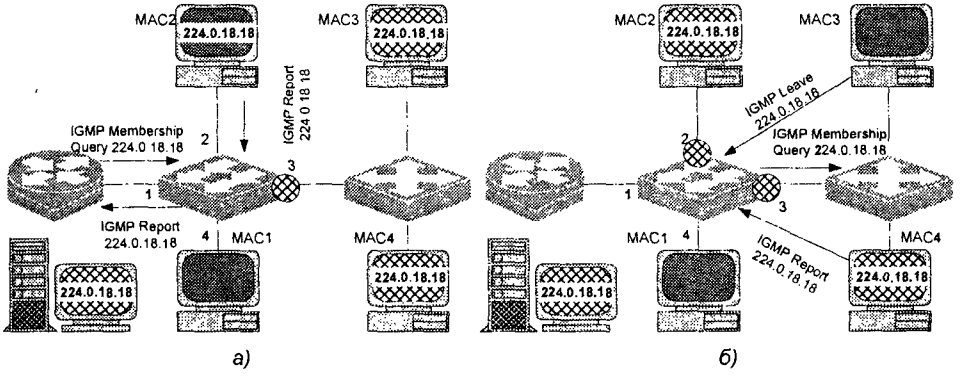


Рис. 11.2. Прослушивание сообщений протокола IGMP

Режим прослушивания сообщений протокола IGMP, таким образом, позволяет не только обеспечить повышение эффективности использования пропускной способности вычислительной сети, но и снизить нагрузку на маршрутизатор. Следует, однако, учитывать, что применение этого режима, во-первых, резко увеличивает нагрузку на коммутатор, а во-вторых, требует внимательного конфигурирования и правильного администрирования.

В листинге 11.3 приведен пример настройки функции igmp_snooping на коммутаторе Allied Telesyn.

Листинг 11.3. Пример настройки функции igmp_snooping на коммутаторе Allied Telesyn

```
    1. Установка значения интервала времени, в течение которого узел
       считается членом Multicast-группы после передачи последнего
       сообщения IGMP Report
AT-9724TS:4# config igmp_snooping default host_timeout 200
state enable
Command: config igmp_snooping default host_timeout 200
state enable
Success.
AT-9724TS:4#
    2. Установка значения интервала времени, по истечении которого
       коммутатор формирует очередное сообщение IGMP General Query
AT-9724TS:4# config igmp_snooping querier default
query_interval 120 state enable
Command: config igmp_snooping querier default query_interval
120 state enable
Success.
AT-9724TS:4#
```

Групповое взаимодействие на сетевом уровне

Для того чтобы обеспечить распространение группового трафика в нужном направлении по сети, групповые маршрутизаторы используют специальные протоколы маршрутизации (multicast routing protocols). Эти протоколы позволяют строить оптимальные пути распространения Multicast-трафика от одного маршрутизатора к другому. Вначале групповой маршрутизатор при помощи протокола IGMP узнает о необходимости приема трафика некоторой группы G, а затем при помощи протоколов групповой маршрутизации подыскивает в сети подходящий источник такого трафика.

Так же, как и обычные протоколы одноадресной маршрутизации, протоколы групповой маршрутизации основаны на концепции Hop-By-Hop, следовательно, маршрутизатору достаточно определить, от какого из соседних маршрутизаторов он будет получать трафик для группы G. Так, от одного маршрутизатора к другому, запрос проходит в направлении от потребителя к источнику. Затем, по проложенному таким образом маршруту направляется групповой трафик от источника к потребителю.

Способы доставки группового трафика

Для построения маршрута доставки группового трафика могут быть использованы два основных способа:

- DENSE — плотное размещение абонентов;
- SPARSE — редкое размещение абонентов.

При использовании DENSE каждый маршрутизатор по умолчанию считается заинтересованным в приеме группового трафика. Если на самом деле это не так, то групповой маршрутизатор должен направить вышестоящему маршрутизатору сообщение об отказе от приема группового трафика. В противоположность DENSE, при использовании способа SPARSE групповой трафик направляется маршрутизатором только после получения запроса от потребителя этого трафика. Естественно, что реализация режима SPARSE представляет значительные трудности, поскольку круг задач, решаемых маршрутизатором в этом режиме, значительно более широк.

Доставка группового трафика в режиме DENSE

При использовании режима DENSE сеть сначала "затапливается" трафиком некоторой группы, а затем те сегменты, в которых нет потребителей данного трафика, отключаются от общего потока. В результате этих процессов формируется дерево, корнем которого является источник, а листьями приемники группового трафика. Ветви этого дерева образуют промежуточные маршрутизаторы. Такое дерево называется *деревом распространения группового трафика* (Distributed Tree). Режим DENSE идейно очень хорошо согласуется с концепцией информационного взаимодействия с использованием групповых адресов и достаточно прост для реализации.

Основным недостатком этого метода является то, что маршрутное дерево DENSE принципиально не может иметь стабильную структуру. Легко заметить, что в том случае, если потенциальный потребитель группового трафика не успел подать соответствующую заявку до того, как "волна" этого трафика омоет ближайший к нему групповой маршрутизатор, у него практически не остается шансов на получение этого трафика. Следовательно, "волны" группового трафика должны формироваться регулярно и с не очень большим периодом, поскольку именно величина этого периода определяет оперативность подключения абонента к источнику группового трафика. Очевидно, что при использовании режима DENSE не может быть и речи об эффективном применении сетевых ресурсов, поскольку периодическую повышенную нагрузку испытывают и групповые маршрутизаторы, и каналы передачи данных.

Доставка группового трафика в режиме SPARSE

Режим DENSE целесообразно использовать в тех случаях, когда подавляющее большинство абонентов сети заинтересовано в приеме группового трафика. В остальных случаях должен применяться более эффективный и экономичный режим SPARSE.

В режиме SPARSE дерево распространения маршрутной информации формируется в направлении, противоположном распространению группового трафика — от "листьев" к "корню". В данном случае маршрутизатор начинает принимать групповой трафик только после формирования специального сообщения.

Очевидно, что при использовании этого метода построения маршрута пропускная способность каналов передачи данных используется гораздо более экономно.

Применение процедуры RPF

Групповые маршрутизаторы, функционирующие в режиме DENSE или SPARSE, должны использовать специальные процедуры, исключающие возможность перемещения группового трафика по циклическим маршрутам. Поскольку маршрутизатор в режиме SPARSE должен сам искать источник группового трафика, то в дополнение к этим процедурам он должен применять специальные алгоритмы, упрощающие процедуру поиска этого источника.

В сетях, использующих режим групповой адресации, применяются специальные протоколы маршрутизации. Основной особенностью этих протоколов является то, что в противоположность протоколам одноадресной маршрутизации, они предназначены для поиска пути к источнику информации, а не к ее приемнику. Поэтому в маршрутных таблицах, формируемых протоколами групповой маршрутизации, размещаются не адреса сетей назначения, а адреса источников группового трафика. В таблице групповой маршрутизации источник группового трафика имеет два адреса, обозначаемых S и G:

- S — обычный IP-адрес класса (A-C) этого источника в сети Интернет;
- G — адрес класса D группы, для которой этот источник формирует трафик.

Первый адрес протоколы групповой маршрутизации используют для построения дерева распространения трафика, а второй используют в качестве ключа для поиска первого. Как правило, при построении маршрута протоколы групповой маршрутизации достаточно тесно интегрируются с обычными протоколами маршрутизации, поскольку при этом обеспечивается возможность полного или частичного использования имеющихся баз маршрутной информации.

Для построения маршрута распространения группового трафика протоколы групповой маршрутизации могут применять режимы DENSE или SPARSE. Ранее уже было отмечено, что протоколы групповой маршрутизации DENSE должны использовать специальные процедуры для того, чтобы предотвратить появление циклических маршрутов.

Классической мерой борьбы с этим явлением является ограничение времени жизни дейтаграмм в сети. Эта универсальная мера, однако, не может обеспечить достаточной оперативности реакции на возникновение петли. Поэтому в протоколах групповой маршрутизации для противодействия возникновению циклических маршрутов используется специальный алгоритм, который называется *алгоритмом RPF* (Reverse Path Forwarding).

Применяя эту процедуру, групповой маршрутизатор использует таблицу протокола одноадресной маршрутизации и определяет номер интерфейса, на который возможен прием группового трафика NG от источника из искомой сети. Если кратчайший маршрут в искомую сеть проходит через этот интерфейс, дейтаграммы принимаются для дальнейшей обработки. В том случае, если дейтаграммы прибывают на несоответствующий интерфейс, маршрутизатор уничтожает их без формирования каких-либо дополнительных сообщений. Некоторые из протоколов групповой маршрутизации используют дополнительные алгоритмы и процедуры, применение которых обеспечивает возможность построения дерева распространения группового трафика, имеющего оптимальную структуру.

Протокол групповой маршрутизации PIM

Протокол групповой маршрутизации — протокол *PIM* (Protocol Independent Multicast) использует таблицы маршрутизации, которые построены алгоритмами одноадресной маршрутизации для создания на их основе деревьев доставки многоадресного трафика до его приемников. Поэтому характерной особенностью этого протокола маршрутизации является его независимость от типа протокола одноадресной маршрутизации, который используется в сети.

Протокол групповой маршрутизации PIM может применяться в двух основных режимах — SPARSE и DENSE.

Использование протокола PIM в режиме DENSE

Протокол PIM при его использовании в режиме DENSE строит дерево распространения группового трафика от источника G, используя периодические затопления всего дерева этим трафиком. В том случае, если в некоторой ветви отсутствуют потребители трафика G, групповой маршрутизатор PIM, образующий эту ветвь, должен передать сообщение об отказе от приема трафи-

ка данной группы — PRUNE вышестоящему маршрутизатору. Существенное отличие состоит в том, что протокол PIM не усекает дерево распространения группового трафика на стадии его создания. Поэтому задача построения дерева в данном случае решается только со стороны приемника трафика с использованием процедуры RPF. Вследствие этого построенное таким образом дерево распространения группового трафика будет заведомо неоптимальным, поскольку маршрутизаторы будут передавать полученный групповой трафик через все свои интерфейсы, за исключением того, с которого этот трафик был получен. Следовательно, построенное дерево наверняка будет содержать дублирующие ветви передачи группового трафика. Корректировка структуры дерева в данном случае выполняется уже на стадии передачи трафика с использованием сообщений отказа от приема — PRUNE и восстановления приема — GRAFT.

Как уже было указано, для определения RPF-интерфейсов групповых маршрутизаторов применяется маршрутная таблица используемого в сети протокола одноадресной маршрутизации. Сообщения ASSERT в протоколе PIM-DM предназначены для определения поставщика группового трафика в сегмент сети с множественным доступом.

Применение протокола PIM в режиме SPARSE

Наиболее широко, однако, используется другой режим протокола PIM — режим SPARSE. Как уже было выше отмечено, этот режим является существенно более экономичным и требует значительно меньше сетевых ресурсов для реализации. Особенностью протокола PIM-SM является то, что в нем для передачи группового трафика наравне с деревьями кратчайших путей (Shortest Path Tree) могут быть использованы разделяемые деревья (Shared Tree). Разделяемое дерево образует виртуальную магистраль, предназначенную для передачи группового трафика, возможно, от нескольких источников.

Информационный обмен в данном случае организуется с использованием специальных групповых маршрутизаторов, которые выполняют функцию "Rendezvous Point (RP)" — точка встречи. Назначением этих маршрутизаторов является накопление информации об Unicast-адресах зарегистрированных источников группового трафика и передача ее по запросам, которые RP-маршрутизаторы получают от маршрутизаторов, непосредственно подключенных к приемникам группового трафика (Last hop router). После получения Unicast-адреса источника группового трафика Last hop router может построить дерево доставки группового трафика непосредственно от источника этого трафика.

После получения сообщения Join корневой маршрутизатор констатирует, что построение дерева завершено, и в том случае, если RP принимает групповой

трафик NG, начинает процесс доставки группового трафика по дереву RP. В том случае, если корневой маршрутизатор в текущий момент не принимает групповой трафик, он формирует сообщение `Join` в адрес одного из зарегистрированных источников этой группы. Процесс регистрации источника инициируется ближайшим к нему групповым маршрутизатором. Для регистрации источника на корневом маршрутизаторе формируется сообщение `Register`, которое источник передает по известному ему адресу корневого маршрутизатора RP. Назначением этого сообщения является передача Unicast-IP-адреса источника группового трафика NG корневому маршрутизатору. Сообщением `Register Stop` корневой маршрутизатор подтверждает, что регистрация источника завершена успешно.

Таким образом, корневой маршрутизатор играет ключевую роль при выполнении всех процедур организации доставки группового трафика протокола PIM-SM, являясь посредником между всеми источниками и приемниками группового трафика сети.

Следовательно, для надежного функционирования протокола PIM в режиме SPARSE должно обеспечиваться динамическое назначение и надежное резервирование самих RP-маршрутизаторов. Это динамическое назначение и резервирование может быть выполнено с использованием двух режимов:

- режима Auto-RP;
- режима Bootstrap.

В режиме Auto-RP один или несколько маршрутизаторов конфигурируются для передачи анонсов о зарегистрированных источниках группового трафика. Для передачи этих анонсов используется выделенная группа 224.0.1.39. Эти анонсы предназначены для обработки на маршрутизаторах-агентах, которые выполняют функцию определения RP-маршрутизатора. Определение RP-маршрутизатора выполняется параллельно всеми агентами по единому алгоритму, в соответствии с которым среди равных выбирается маршрутизатор, который имеет максимальный IP-адрес. Выбор RP осуществляется независимо для каждой передающей группы, этот процесс называется *mapping*. Информация о сделанном выборе передается для всех членов группы 224.0.1.40, в которую входят все остальные маршрутизаторы сети. Поскольку все агенты используют один и тот же алгоритм выбора, информация о выбранных маршрутизаторах RP, сформированная разными агентами, является идентичной. Вследствие этого обеспечивается надежность функционирования всей системы в целом.

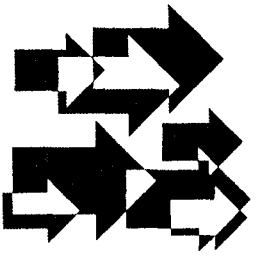
В режиме Bootstrap один или несколько маршрутизаторов конфигурируются в качестве RP-кандидатов. Эти же или другие несколько маршрутизаторов конфигурируются в качестве Bootstrap-кандидатов. Последние начинают периодически (один раз в минуту) передавать всем членам группы 224.0.0.13

содержимое таблицы соответствия группового адреса и адреса RP-маршрутизатора. Кроме этого передается адрес самого Bootstrap-кандидата. Информация распределяется по сети в соответствии с классическими алгоритмами "затопления" с блокированием дублирующих ветвей функцией Reverse Path Forwarding (*RPF*). В соответствии с этой функцией пакет, который принят на интерфейс, находящийся на кратчайшем пути до его источника, должен быть передан через все остальные порты маршрутизатора. Если пакет придет на какой-либо другой порт, то он должен быть уничтожен. Так обеспечивается передача информации всем маршрутизаторам сети и исключается дублирование передаваемой информации. Маршрутизаторы, которые являются RP-кандидатами, в одноадресном режиме передают информацию о зарегистрированных источниках группового трафика непосредственно BS-кандидату, который имеет наибольший адрес. Все остальные маршрутизаторы сети принимают сообщения, сформированные BS-кандидатами, и формируют на их основе свои внутренние таблицы соответствия групповых адресов и адресов RP-маршрутизаторов. Для каждой записи этой таблицы устанавливается период времени, в течение которого эта запись считается актуальной. В том случае, если до истечения этого периода информация не будет подтверждена очередным сообщением, полученным от Bootstrap-кандидата, запись аннулируется. В листинге 11.4 приведен вариант настройки режима PIM-SM на коммутаторе Cisco Systems.

Листинг 11.4. Настройка режима PIM-SM на коммутаторе Cisco Systems

```
    1. Переход в режим изменения настройки коммутатора
3750# conf t
    2. Определение списка групп, для которых коммутатор может выполнять
       функцию RP
3750(config)# access-list 11 permit 239.0.0.0 0.255.255.255
    3. Настройка коммутатора в качестве кандидата на выполнение
       функций RP для выделенных групп
3750(config)# ip pim send-rp-announce gigabitethernet1/0/1 group-list 11
```

ГЛАВА 12



Управление трафиком приложений мультисервисных ЛВС

Управление трафиком абонентских приложений осуществляется для того, чтобы повысить эффективность использования сетевых ресурсов и обеспечить требуемые значения параметров информационного обмена в ЛВС. Поскольку главным ресурсом ЛВС, как уже было отмечено, является пропускная способность каналов передачи данных, управление трафиком приложений состоит в реализации оптимального распределения пропускной способности портов ЛВС между исполняемыми приложениями. Для некоторых приложений может дополнительно потребоваться нормирование и других характеристик информационного обмена. Кроме того, управление трафиком клиентских приложений может быть организовано для предотвращения перегрузки компонентов ЛВС при возникновении аварийной ситуации.

Однотипные абонентские приложения, как правило, имеют похожие требования к ресурсам ЛВС и поэтому могут объединяться в группы одинакового уровня обслуживания. Уровнем обслуживания в этом случае называется обобщенная характеристика параметров ресурсов ЛВС, выделяемых для выполнения абонентского приложения или группы приложений. Более высокому уровню обслуживания при этом соответствуют лучшие значения характеристик ЛВС, например, более высокая пропускная способность канала или меньшая задержка при обработке блока данных.

В зависимости от характера требований, которые предъявляются к нормируемым параметрам, и возможностей активного оборудования ЛВС по реализации этих требований, для управления трафиком приложений могут быть использованы разнообразные схемы, методы и средства. В частности, задача управления трафиком группы приложений может быть решена глобально (объединенное управление трафиком), в рамках всей сети в целом, путем закрепления сетевых ресурсов за этой группой приложений на каждом промежуточном узле ЛВС. Задача управления трафиком может быть решена и ло-

кально (распределенное управление трафиком), в том случае, если на каждом из промежуточных узлов ЛВС будет реализовано несколько типовых уровней обслуживания, с каждым из которых впоследствии можно будет связать ту или иную группу приложений.

В первом разделе данной главы приведены определения основных терминов и понятий, которые используются в системах управления трафиком абонентских приложений.

Во втором разделе на примере протокола RSVP рассматриваются основные принципы организации систем объединенного управления трафиком абонентских приложений (IntServ).

Третий раздел посвящен рассмотрению способов разделения трафика и основных компонентов систем распределенного управления трафиком абонентских приложений (DiffServ).

В заключительном разделе главы кратко рассмотрены особенности управления трафиком абонентских приложений в нестандартных ситуациях.

Элементы систем управления трафиком

Сложность задачи управления трафиком состоит в ограниченности распределяемого ресурса, поэтому удовлетворение потребностей одной группы приложений почти всегда влечет за собой снижение уровня обслуживания остальных групп приложений.

К сожалению, наиболее популярные на настоящий момент сетевые технологии: протокол сети Интернет — на сетевом уровне и Ethernet/IEEE 802.3 — на канальном, изначально одинаково плохо приспособлены для управления трафиком абонентских приложений. В этих условиях резко вырастает потребность в дополнительных процедурах и технологиях, позволяющих расширить возможности современных сетей для обеспечения оптимальной интеграции разнородного сетевого трафика.

В общем случае задача управления трафиком абонентских приложений включает в себя следующие компоненты:

- планирование трафика приложений;
- определение политики управления;
- выбор метода и схемы управления.

Задача планирования трафика представляет собой поиск оптимального распределения ресурсов ЛВС между абонентскими приложениями. При выполнении этой задачи должны быть проанализированы, учтены и согласованы требования приложений и характеристики ЛВС.

После того, как схема оптимального распределения будет найдена, определяются основные принципы ее практической реализации. Они составляют модель или политику, в соответствии с которой взаимодействуют узлы мультисервисной сети в процессе совместного управления трафиком абонентских приложений.

На следующем этапе должны быть определены инструменты управления трафиком приложений — схемы и методы, которые будут использоваться для реализации выбранных классов обслуживания для каждой группы приложений.

Планирование трафика приложений

Современные вычислительные сети активно используются для передачи по ним голосового и видеотрафика. Для эффективной передачи этих разновидностей трафика к параметрам сети предъявляются жесткие специфические требования. Дело в том, что аудио- и видеотрафик имеет ярко выраженный потоковый характер и поэтому плохо приспособлен для передачи по сетям с коммутацией блоков данных.

Для нормального функционирования потоковых приложений сеть должна обеспечивать заданный уровень качества обслуживания — QoS (Quality of Service): гарантированную ширину полосы пропускания и стабильную минимальную задержку передаваемых блоков данных.

Определение

Качеством обслуживания (QoS — Quality of Service) называют способность ЛВС обеспечивать заданные значения сетевых параметров для передачи выбранного типа трафика.

На рис. 12.1 приведены примеры передачи потокового трафика через ЛВС без обеспечения заданного уровня качества обслуживания. В том случае, когда эта ЛВС располагает ресурсом, необходимым для нормального функционирования приложения, абонент не замечает отсутствия сервиса QoS. В приведенном примере для нормального приема видеопотока с сервера S1 требуется выделение пропускной способности 6 Мбит/сек. Такая потребность легко может быть реализована при отсутствии других приложений в данной ЛВС, поскольку пропускная способность задействованных этим приложением каналов имеет достаточный ресурс. Эта ситуация представлена на рис. 12.1, *а* — коммутаторы SW1 и SW2 связаны потоком 100 Мбит, неиспользованный ресурс которого составляет 94 Мбит/сек. В то же время неиспользуемый ресурс на канале между коммутаторами SW2 и SW3 составляет всего 4 Мбит/сек, поэтому при появлении в данной ЛВС еще одного прило-

жения нормальное функционирование первого приложения может быть нарушено.

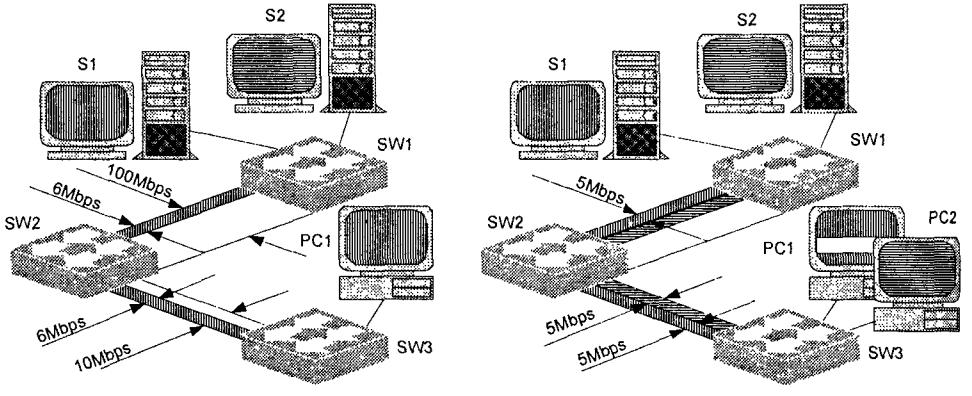


Рис. 12.1. Схема информационного обмена протокола RSVP

Такая ситуация представлена на рис. 12.1, *б* — вследствие отсутствия службы обеспечения заданного уровня качества обслуживания, пропускная способность канала между коммутаторами SW2 и SW3 будет разделена поровну (по 5 Мбит/сек) между двумя активными приложениями. Поэтому при подключении к коммутатору SW3 абонента PC2, который принимает видеопоток с сервера S2, абонент PC1 отметит значительное ухудшение качества приема своего видеопотока.

В общем случае потоковые приложения предъявляют требования к следующим характеристикам ЛВС:

- *Bandwidth* — пропускная способность, скорость передачи данных;
- *Delay* — среднее или максимальное значение временной задержки передаваемого блока данных;
- *Delay variation* — максимальное значение изменения величины временной задержки передаваемого блока данных.

Наиболее часто в качестве основной характеристики мультисервисной ЛВС рассматривается именно пропускная способность используемых каналов передачи данных, поскольку остальные параметры качества имеют вторичное значение и являются более сложными для управления.

Модели управления клиентским трафиком

На мультисервисные сети возлагается задача обеспечения оптимальной интеграции разнородного трафика в условиях ограниченности сетевого ресурса.

Для решения этой задачи могут быть использованы две различные модели обеспечения качества обслуживания:

- *модель IntServ* (Integrated Service Model) — модель объединенного обслуживания;
- *модель DiffServ* (Differentiated Service Model) — модель раздельного обслуживания.

При использовании модели IntServ весь трафик, передаваемый в системе, считается изначально однородным. Заданный уровень качества обслуживания в данном случае обеспечивается путем применения специальных механизмов динамического резервирования ресурсов для выделенной части передаваемого трафика. Такой механизм может быть, в частности, реализован при использовании протокола RSVP (Resource Reservation Protocol).

Использование модели DiffServ предполагает неоднородность трафика, передаваемого в системе, и включает несколько последовательных этапов преобразования данных.

На первом этапе выполняется классификация трафика, проходящего через устройство. При этом в соответствии с реализуемой политикой обеспечения QoS, весь трафик разбивается на *классы обслуживания* — CoS (Class of Service), для каждого из которых устанавливается уровень качества обслуживания, в виде совокупности установленных требований к характеристикам производительности сети. В качестве критериев принадлежности трафика к некоторому классу может быть использовано значение поля IP PRECEDENCE или любого другого поля дейтаграммы (адрес источника, порт назначения и т. д.). В качестве признака принадлежности блока данных к определенному классу также может быть использована специальная метка, передаваемая по сети вместе с блоком.

В зависимости от типа функций, выполняемых сетевым устройством, на следующем этапе может выполняться регулирование трафика. Применение регулирования обеспечивает реализацию заданных значений QoS для каждого из установленных классов обслуживания. Для регулирования трафика устройство может использовать *жесткий метод* — policing ("ограничение"), при котором блоки данных, выходящие за лимит сетевого ресурса своего класса, просто уничтожаются. Также может быть использован более *мягкий метод* регулирования трафика — shaping ("формирование"). При использовании этого метода сверхлимитные блоки данных задерживаются в специальных буферах — отстойниках, дожидаясь там разрешения на использование сетевого ресурса.

Объединенное управление трафиком (IntServ)

Аппарат объединенного управления трафиком абонентских приложений предполагает наличие и использование сигнальных механизмов для резервирования требуемых сетевых ресурсов перед началом информационного обмена. Эта модель управления качеством обслуживания не является новой. Похожий механизм используется, например, для аналогичных целей в технологии ATM. В современных ЛВС для реализации объединенного управления трафиком обычно используется протокол динамического резервирования ресурсов — протокол RSVP: (IETF RFC 2205: Resource Reservation Protocol: September 1997: Status: PROPOSED STANDARD).

Протокол RSVP

Протокол RSVP используется для резервирования сетевых ресурсов с целью обеспечения заданного уровня QoS в системах объединенного обслуживания — IntServ. При помощи протокола RSVP конечный узел может запрашивать определенные уровни QoS для выделенных групп источников поступающего к нему трафика. Протокол RSVP может одинаково успешно обеспечивать резервирование ресурсов, необходимых для передачи одноадресного и группового трафика. Для обеспечения резервирования сетевых ресурсов протокол RSVP использует информацию о маршрутах, получаемую от протоколов Unicast- и Multicast-маршрутизации.

Механизмы управления трафиком протокола RSVP

Протокол RSVP позволяет определить и реализовать политику обеспечения качества обслуживания для групп блоков данных, проходящих по некоторому маршруту и называемых потоками. Для управления потоками протокол RSVP использует следующие функциональные модули и механизмы:

- Packet classifier — классификатор пакетов;
- Packet scheduler — планировщик пакетов;
- Admission controller — контроллер ресурса;
- Policy controller — контроллер политики.

Информационный обмен между узлами сети, использующими протокол RSVP для резервирования сетевых ресурсов, осуществляется при помощи специальных сообщений. Сообщения протокола RSVP могут быть сформированы источником потока данных, приемником (или приемниками) этого потока, а также промежуточными узлами сети.

Сообщение "Запрос резервирования" (Reservation Request) используется для распространения по сети информации о потребности в сетевых ресурсах для некоторого информационного потока. Элементарный запрос резервирования включает в себя две спецификации:

- Flow specification — спецификация потока;
- Filter specification — спецификация фильтра.

Спецификация потока содержит значения запрашиваемых параметров сетевых ресурсов и предназначается для настройки модулей планировщиков пакетов. В состав спецификации потока входят два набора цифровых параметров.

1. RSpec (Reserve Specification) — запрашиваемые параметры QoS;
2. TSpec (Traffic Specification) — описание потока данных.

Спецификация фильтра содержит информацию, необходимую для настройки классификатора, — критерии принадлежности трафика к выделенной группе.

Схема организации информационного обмена при использовании протокола RSVP приведена на рис. 12.2.

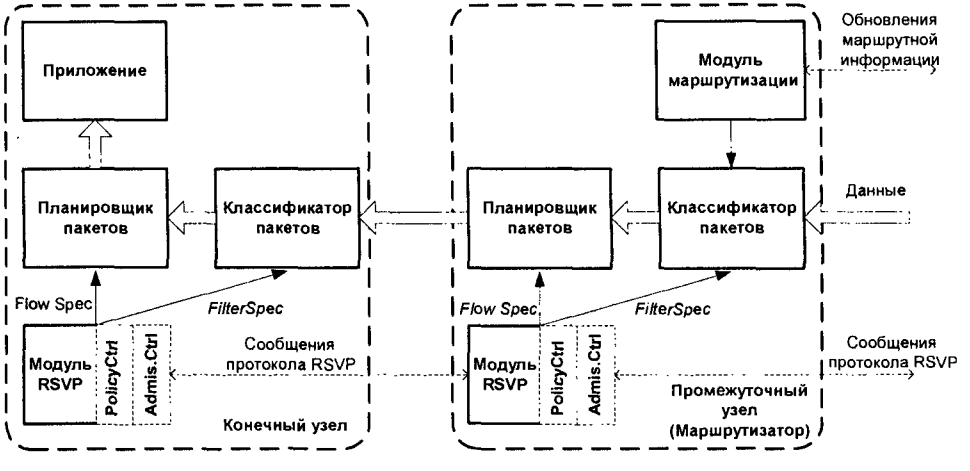


Рис. 12.2. Схема информационного обмена протокола RSVP

Управление информационным потоком, направление которого указано утолщенными стрелками, осуществляется двумя типами модулей — модулями протокола RSVP и модулями маршрутизатора. Инициатором информационного взаимодействия выступает узел, заинтересованный в приеме потока данных. Для определения политики обеспечения качества обслуживания этот узел и маршрутизаторы, через которые пролегает путь, связывающий его с источником потока данных, обмениваются сообщениями протокола RSVP.

Этот обмен производится по классическому принципу "hop-by-hop". В результате обмена сообщениями на узле и маршрутизаторах осуществляется настройка исполняющих модулей обеспечения качества обслуживания.

При приеме RSVP-сообщения на промежуточный узел выполняются следующие действия:

- закрепление ресурса канала за выделенным потоком;
- формирование последующего RSVP-сообщения.

В свою очередь процесс закрепления канального ресурса включает в себя две предварительные контрольные стадии. На первой из них устанавливается наличие у источника запроса полномочий на выполнение процедур резервирования на данном узле. В ходе выполнения второй процедуры устанавливается практическая возможность выделения данным узлом запрашиваемых ресурсов. В том случае, если обе описанные ранее процедуры были осуществлены успешно, на промежуточном узле выполняются действия, обеспечивающие закрепление требуемых ресурсов за выделенным потоком. При этом, в зависимости от типа используемого протокола канального уровня, резервирование может быть выполнено с использованием специфических алгоритмов упорядочивания.

Назначение классификатора состоит в определении принадлежности к тому или иному классу блоков данных входящего информационного потока. В зависимости от реализуемой политики определение принадлежности к тому или иному классу может производиться на основании анализа значений таких параметров информационного потока, как адрес источника, адрес назначения, тип протокола сетевого и транспортного уровня и т. д. Управление классификатором производится от модуля протокола RSVP и модуля маршрутизации. При этом модуль маршрутизации обеспечивает поступление необходимой маршрутной информации, а модуль RSVP направляет информацию, необходимую для обеспечения собственно процедуры классификации.

Назначение планировщика пакетов состоит в определении порядка прохождения на обработку блоков данных сетевого уровня, принадлежащих к различным классам входного потока. Управление планировщиком производится от модуля RSVP, при этом планировщику передается информация о значениях разрешенных для каждого класса потоков параметров сетевых ресурсов.

Формы и методы резервирования ресурсов

Особенностью протокола RSVP является возможность обеспечения резервирования сетевых ресурсов для передачи группового трафика. Как известно, для передачи трафика этого типа в сети при помощи протоколов групповой маршрутизации создаются виртуальные структуры — деревья распростране-

ния группового трафика. Для повышения эффективности использования сетевого ресурса процедура резервирования, реализуемая протоколом RSVP, располагает возможностью объединения (merging) резервов сетевых ресурсов, обеспечивающих передачу одного и того же группового трафика в точках разветвления. Собственно резервирование состоит в определении значений пары связанных величин — адреса источника трафика (S) и пропускной способности, требуемой для передачи этого трафика (Q).

Протокол RSVP обеспечивает возможность использования нескольких стилей для формулирования политики резервирования и формирования спецификации фильтра:

- Wildcard-Filter (WF) — стиль резервирования с неопределенным фильтром;
- Fixed-Filter (FF) — стиль резервирования с фиксированным фильтром;
- Shared Explicit (SE) — разделяемый стиль с явным указанием источников.

При использовании стиля резервирования с неопределенным фильтром для формулирования политики управления качеством обслуживания приложение или промежуточный маршрутизатор определяет только требование к значению пропускной способности сети (Q) – WF (*{Q}). Создаваемый таким образом резервированный канал обеспечивает передачу всего группового трафика. В том случае, если промежуточный маршрутизатор получает несколько последовательных запросов резервирования WF (*{Q}), он формирует итоговый запрос, передаваемый в направлении источника трафика, используя принцип поглощения меньшего запроса большим запросом:

$$\{WF\ (*\{Q_i\})\}\ i = (1..n) \Rightarrow WF\ (*\{\ \max(Q_i)\})\}$$

На рис. 12.3 представлена схема формирования запросов при использовании стиля Wildcard-Filter.

В данном случае параметр Q запросов, формируемых маршрутизаторами ГМ1 и ГМ4, соответствует максимальному значению Q среди всех запросов на резервирование сетевого ресурса, принятых данными маршрутизаторами, и никак не зависит от типа запрашиваемого трафика.

При использовании стиля резервирования с фиксированным фильтром для формулирования политики управления качеством обслуживания приложение или промежуточный маршрутизатор явно определяют требования к значению пропускной способности сети для передачи конкретного вида группового трафика FF (S{Q}). Создаваемый таким образом резервированный канал обеспечивает передачу всего группового трафика. В том случае, если промежуточный маршрутизатор получает несколько последовательных запросов резервирования FF (S{Q}), он формирует итоговые запросы, передаваемые в направлении источника трафика, используя принцип поглощения меньшего

запроса большим запросом отдельно для каждого источника группового трафика:

$$\{FF\ (S_j\{Q_i\})\}\ i = (1..n) \Rightarrow FF_j\ (S\{\ max(Q_i)\})\}$$

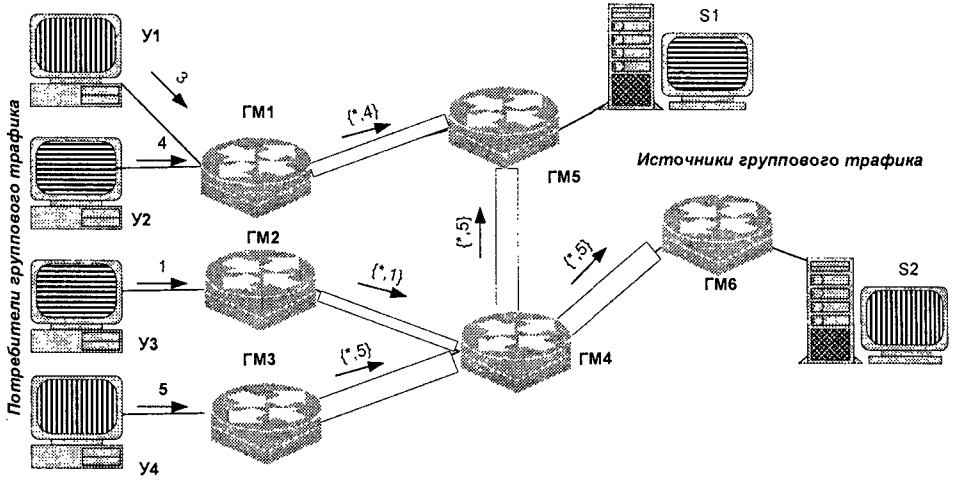


Рис. 12.3. Схема формирования запросов протокола RSVP при использовании стиля Wildcard-Filter

На рис. 12.4 представлена схема формирования запросов при использовании стиля резервирования Fixed-Filter.

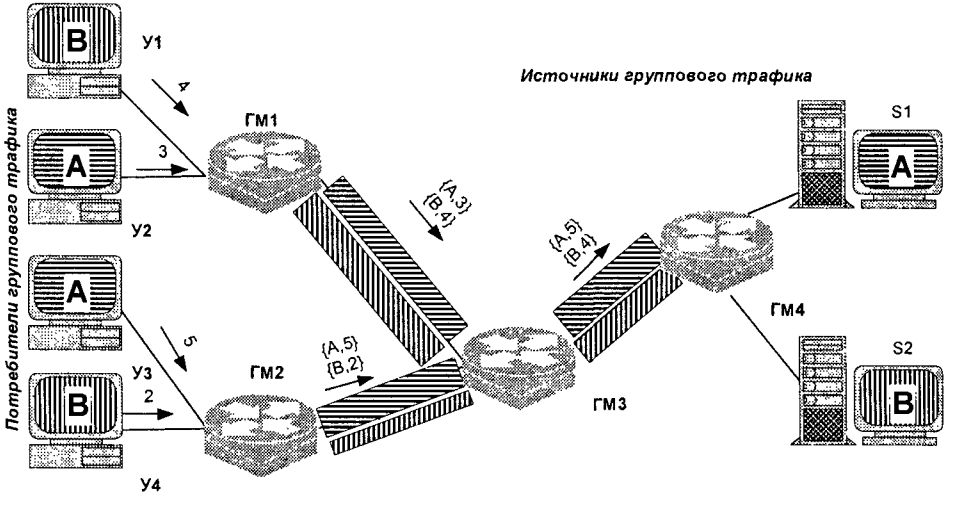


Рис. 12.4. Схема формирования запросов при использовании стиля резервирования Fixed-Filter

При использовании этого стиля резервирования промежуточный маршрутизатор ГМ3 формирует суммарный запрос, в котором для источников A и B резервируются максимальные значения соответствующих ресурсов сети (5 и 4 соответственно).

При использовании разделяемого стиля с явным указанием источников приложение или промежуточный маршрутизатор определяют единое требование к значению пропускной способности сети для передачи группового трафика нескольких явно определенных источников SE (S_1...S_j{Q}).

Этот стиль резервирования незначительно отличается от стиля резервирования WF. Отличие состоит в том, что при использовании стиля SE информация об источниках группового трафика накапливается в последующих запросах резервирования по принципу снежного кома. При этом требования к сетевому ресурсу определяются стандартным образом — результирующее требование формируемого запроса соответствует максимальному требованию из числа принятых запросов.

На рис. 12.5 представлена схема формирования запросов при использовании стиля резервирования Shared Explicit.

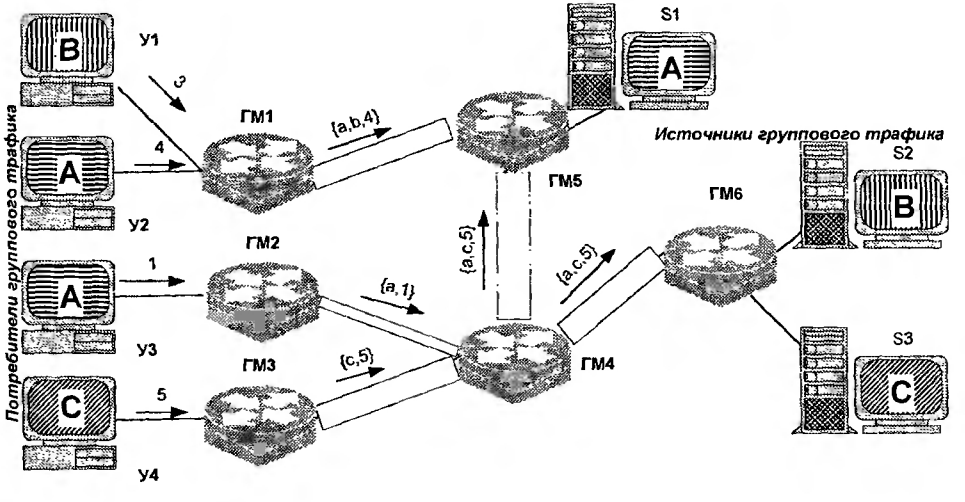


Рис. 12.5. Схема формирования запросов при использовании стиля резервирования Shared Explicit

Сообщения протокола RSVP

Для обеспечения информационного обмена между компонентами в протоколе RSVP используются следующие типы сообщений:

- `Reservation-Request` — сообщения запросов резервирования;
- `Path` — сообщения о формировании пути;
- `Error` — сообщения об ошибках;
- `Confirmation` — сообщения подтверждения;
- `Teardown` — сообщения о разрывании пути.

Каждый конечный или промежуточный узел RSVP, принимающий групповой или одноадресный трафик, должен принимать, обрабатывать и формировать сообщения `Reservation-Request`, а также передавать сформированные сообщения в направлении источников этого трафика. Сообщения `Reservation-Request` передаются по пути, проложенному сообщениями `Path`. Для передачи сообщений `Reservation-Request` должен быть использован Unicast-адрес ближайшего узла или маршрутизатора. При получении сообщения `Reservation-Request` промежуточный маршрутизатор переходит в состояние резервирования соответствующего сетевого ресурса. Это состояние является динамическим в том случае, если маршрутизатор в течение установленного интервала времени не получит сообщений `Reservation-Request` и `Path`, подтверждающих необходимость резервирования данного ресурса, он автоматически перейдет в исходное состояние.

Сообщения `Path` формирует каждый источник трафика, а также любой промежуточный узел RSVP, передающий этот трафик по инстанции. Для передачи сообщений `Path` должен быть использован тот же адрес, который применяется для передачи потока данных. Передача сообщений `Path` предшествует передаче сообщений `Reservation-Request`. При получении сообщения `Path` маршрутизатор переходит в состояние хранения пути передачи данных соответствующего источника. Впоследствии этот путь будет использован для передачи по нему потока данных и сообщений `Reservation-Request`.

В протоколе RSVP используются два сообщения об ошибках:

- `ResvErr` — сообщение об ошибке резервирования;
- `PathErr` — сообщение об ошибке маршрута.

К сожалению, существует достаточно много самых разнообразных причин, вызывающих формирование сообщения `ResvErr`. Такое сообщение может быть сформировано в том случае, если полученный запрос резервирования не может быть удовлетворен на данном узле из-за существующих ограничений сетевого ресурса. К аналогичному результату может привести отсутствие у автора запроса надлежащих прав на выполнение операций резервирования на данном маршрутизаторе. К появлению подобного сообщения могут также привести конфликты между несколькими последовательными запросами, поступившими на маршрутизатор.

Сообщения об ошибке маршрута PathErr передаются в направлении источника потока данных по принципу "hop-by-hop".

Требование подтверждения применения резервирования может быть включено в любой передаваемый приемником запрос резервирования. При наличии такого требования в запросе резервирования источник потока данных должен получить подтверждение о применении резервирования от того узла, на котором этот запрос закончил свой путь по сети. Обычно такое сообщение передает узел, выполнивший операцию слияния запросов.

Сообщение Teardown формируется для обеспечения немедленного изменения существующего состояния маршрутизатора, хранящего информацию о пути передачи потока данных или резервировании сетевых ресурсов для передачи этого потока.

Для выполнения таких изменений используются сообщения PathTear и ResvTear соответственно. Эти сообщения могут быть сформированы любым узлом, находящимся на пути распространения потока данных и распространяются по принципу "hop-by-hop".

Формат сообщений протокола RSVP

Структура сообщения протокола RSVP представлена в табл. 12.1.

Таблица 12.1. *Структура сообщения протокола RSVP*

Номер поля	Наименование и содержание поля	Значение	Длина поля (байт)
1	VERSION — номер версии протокола RSVP	2	0,5
2	FLAGS — зарезервировано для размещения управляющих признаков	1	0,5
3	TYPE — тип сообщения RSVP	1—255	1
4	CHECKSUM — контрольная сумма информационной части сообщения RSVP	1—255	2
5	LENGTH — длина сообщения RSVP, выраженная в байтах	1—255	2
6	RESERVED — зарезервировано для дальнейшего использования	0/1/2	1
7	TTL — время жизни сообщения в сети	1—255	1
8	MESSAGE ID — индивидуальный идентификатор сообщения		2
9	RESERVED — зарезервировано для дальнейшего использования		28,128

Таблица 12.1 (окончание)

Номер поля	Наименование и содержание поля	Значение	Длина поля (байт)
10	MF — порядок текущего фрагмента сообщения		0,125
11	FRAGMENT OFFSET — смещение текущего фрагмента сообщения		2

Поле VERSION предназначено для размещения номера использованной версии протокола RSVP. В настоящее время используется первая версия протокола RSVP.

Поле FLAGS зарезервировано для размещения управляющих признаков протокола RSVP.

В поле TYPE размещается признак типа используемого сообщения протокола RSVP. Перечень сообщений протокола RSVP и их назначение приведены в табл. 12.2.

Таблица 12.2. Типы сообщений протокола RSVP

Тип	Тип сообщения	Назначение
1	PATH	Формирование пути передачи трафика
2	RESERVATION-REQUEST	Запрос резервирования сетевого ресурса
3	PATH-ERROR	Ошибка пути передачи трафика
4	RESERVATION-REQUEST ERROR	Неверный запрос резервирования сетевого ресурса
5	PATH-TEARDOWN	Разрывание пути передачи трафика
6	RESERVATION-TEARDOWN	Снятие запроса резервирования сетевого ресурса
7	RESERVATION-REQUEST ACKNOWLEDGMENT	Подтверждение запроса резервирования сетевого ресурса

В поле CHECKSUM размещается 16-разрядная контрольная сумма сообщения протокола RSVP.

В поле LENGTH размещается выраженная в байтах длина данного сообщения.

Значение, размещенное в поле TTL, определяет максимальную величину временного интервала, в течение которого данное сообщение может существовать в сети.

Значение, размещенное в поле MESSAGE ID, предназначено для обеспечения восстановления исходного сообщения, прошедшего процедуру фрагментации. В этом случае все фрагменты исходного сообщения должны иметь одинаковое значение поля MESSAGE ID.

В поле MF размещается признак, указывающий на положение текущего фрагмента в исходном сообщении. У последнего фрагмента сообщения этот признак устанавливается равным 0.

Значение, размещенное в поле FRAGMENT OFFSET, определяет смещение текущего фрагмента относительно начала исходного сообщения.

Распределенное управление трафиком (DiffServ)

Модель DiffServ наиболее часто используется для управления трафиком в современных ЛВС. Это вызвано, с одной стороны, относительной простотой реализации компонентов модели DiffServ на активном оборудовании современных ЛВС, а с другой — универсальностью этой модели. Универсальность распределенного управления трафиком заключается в том, что элементы этой модели могут быть реализованы на активном оборудовании как сетевого, так и канального уровня OSI ISO 7498. Простота администрирования и невысокая требовательность к используемым ресурсам объясняется отсутствием у DiffServ единой сигнальной и управляющей схемы, поскольку информация о классовой принадлежности содержится в каждом блоке передаваемых данных. Каждый из участников DiffServ реализует свою политику управления трафиком клиентских приложений независимо от остальных участников путем соответствующего распределения пропускной способности своих каналов между различными классовыми группами.

Реализация распределенного управления трафиком современных локальных сетей включает в себя следующие основные этапы анализа и обработки трафика клиентских приложений:

- классификацию — разделение и маркирование трафика клиентских приложений;
- нормирование — выравнивание и упорядочивание трафика клиентских приложений.

На этапе классификации производится разделение трафика клиентских приложений на классы эквивалентного обслуживания в соответствии с признаками классовой принадлежности, которые находятся в передаваемых блоках данных. Эти признаки, впрочем, не могут иметь глобального значения. Очевидно, что трафик одних и тех же приложений может иметь разные приоритеты с точки зрения администраторов различных ЛВС, поэтому согласован-

ные политики DiffServ могут выполняться только внутри ограниченных областей, которые называются *QoS-доменами*.

Определение

QoS-доменом называется группа связанных узлов ЛВС, в пределах которой используются единые правила классификации трафика клиентских приложений.

В том случае, если блоки передаваемых данных не содержат признаков классовой принадлежности, формирование этих признаков — маркирование трафика выполняется по основным параметрам блоков данных канального, сетевого или транспортного уровней OSI ISO 7498. Обычно процедура маркирования реализуется на граничном узле QoS-домена.

Нормирование выполняется для классифицированного трафика с целью достижения требуемого соотношения скоростей информационных потоков для соответствующих классов обслуживания. На промежуточном узле, находящемся в пределах QoS-домена, нормирование может быть выполнено как для принимаемого, так и для передаваемого трафика. Тип процедур, которые используются для реализации нормирования трафика, обычно определяется классом обслуживаемого трафика и возможностями промежуточного узла ЛВС.

Способы разделения трафика приложений

При использовании модели распределенного управления трафиком (DiffServ) заданный уровень качества обслуживания QoS обеспечивается независимо каждым из промежуточных узлов ЛВС, через которые проходит этот трафик. При этом каждый из узлов должен выполнять следующие функции:

- разделение входного трафика на группы с одинаковыми требованиями QoS — классы обслуживания CoS (Class of Service);
- обеспечение требуемого уровня QoS для трафика каждого класса.

Для определения принадлежности трафика к классу CoS используются дополнительные признаки, которые специально для этих целей размещаются в заголовках блоков данных протоколов сетевого (IP) и канального (Ethernet) уровней.

Примечание

Следует учитывать, что само по себе наличие в блоке данных признака принадлежности к привилегированному классу обслуживания не означает автоматического выполнения для него соответствующих процедур обеспечения QoS на всех промежуточных узлах ЛВС. Для того чтобы эти процедуры были выполнены, необходимы наличие аппаратов реализации согласованных политик на этих промежуточных узлах.

Классификация по признакам канального уровня

Изначально в блоке данных канального уровня — кадре Ethernet отсутствовало поле, в котором можно было бы поместить признак принадлежности трафика к определенному классу (см. *главу 6*). Это объясняется особенностями становления технологии Ethernet, которая изначально обеспечивала информационный обмен по среде с множественным доступом абонентов (общая шина).

В дальнейшем, по мере развития технологии, разработчики спецификации IEEE 802.3 постарались скомпенсировать отмеченный недостаток путем введения специального поля CoS в состав метки VLAN. Эта доработка обеспечивает возможность реализации согласованных политик управления трафиком на канальном уровне для коммутаторов, соединенных друг с другом через маркирующие порты (см. *главу 7*).

В метке VLAN для указания класса CoS используются 3 бита (биты 8, 7 и 6 первого байта метки), при помощи которых можно определить принадлежность кадра к одному из 8 различных классов обслуживания. Значение "000" = 0 при этом должно быть использовано для обозначения кадров наименее приоритетного класса, и, соответственно, значение "111" = 7 используется для указания принадлежности к классу с наивысшим приоритетом.

Основными недостатками классификации трафика на канальном уровне являются невозможность разделения трафика, поступающего на демаркирующий порт коммутатора, и потеря признака принадлежности к классу (вместе с меткой VLAN) при передаче трафика через этот порт. Отмеченные недостатки усугубляются тем, что именно через такие порты обычно производится подключение абонентов в ЛВС. Таким образом, становится принципиально невозможной реализация единой политики (от сервера к абоненту через ЛВС) для управления трафиком на канальном уровне.

Классификация по признакам сетевого уровня

В четвертой версии протокола IPv4 (IETF RFC 791, STD 5) для указания рекомендованного типа обслуживания — *TOS* (Type of Service) использовалось одноименное восьмибитовое поле заголовка пакета. Три старших бита этого поля образовывали дополнительное поле IP Precedence — IP_PREC. Содержимое этого поля определяет тип приложения, которое использовано для формирования полезной нагрузки пакета. В табл. 12.3 приведены значения поля IP_PREC для основных типов приложений.

По замыслу авторов, значения остальных битов поля TOS должны были использоваться для указания требований источника данного пакета к характеристикам каналов передачи данных, по которым этот пакет будет передан.

Значения битов этого поля должен был анализировать каждый маршрутизатор при наличии нескольких альтернативных маршрутов для передачи помеченного пакета. В табл. 12.4 приведены назначения битов поля TOS. Во всех случаях значение 0 бита поля TOS указывает на отсутствие повышенных требований источника данного пакета к соответствующей характеристике канала.

Таблица 12.3. *Значения поля IP_PREC для основных типов приложений*

IP_PREC	Тип приложения	Назначение
0	ROUTINE	Стандартная процедура (наименьший приоритет)
1	PRIORITY	Приоритетная процедура
2	IMMEDIATE	Неотложная процедура
3	FLASH	Срочная процедура
4	FLASH-OVERRIDE	Чрезвычайная процедура
5	CRITICAL	Критическая процедура
6	INTERNET	Межсетевое управление
7	NETWORK	Процедура управления ЛВС (наивысший приоритет)

Таблица 12.4. *Значения битов поля TOS*

Номер бита поля TOS	Характеристика канала	Назначение
3	DELAY	Задержка распространения сигнала в канале
4	THROUGHPUT	Пропускная способность канала передачи данных
5	RELIABILITY	Надежность канала передачи данных
6	MONETARY	Стоимость использования канала передачи данных
7	RESERVED	Зарезервирован для дальнейшего использования

Основные принципы построения и методы реализации модели DiffServ для управления трафиком, передаваемым по сети Интернет, изложены в документах:

- Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (IETF RFC 2474 : December 1998: Standards Track);
- An Architecture for Differentiated Services (IETF RFC 2475: December 1998: Informational).

Эти документы предусматривают использование битов 7—2 поля TOS заголовка пакета для размещения в них значения, определяющего принадлежность к выделенному классу — *DSCP* (Differentiated Services Code Point). Поле DSCP, в свою очередь, также разделено на два поля:

- CLASS SELECTOR — указатель класса;
- DROP PRECEDENCE — очередность удаления (при перегрузке).

В соответствии с принятой схемой, пакеты, помеченные большими значениями указателя класса, имеют преимущество при отправке и обработке по сравнению с пакетами, помеченными меньшими значениями указателя класса. По этой же схеме, пакеты, помеченные большими значениями поля DROP PRECEDENCE, имеют преимущество при удалении в случае возникновения перегрузки по сравнению с пакетами, помеченными меньшими значениями DROP PRECEDENCE.

В этих документах определяются также основные схемы поведения промежуточных узлов — *PHB* (Peer Hop Behavior), которые могут быть использованы при обработке трафика DiffServ в сети Интернет:

- Assured Forwarding — гарантированная передача;
- Expedited Forwarding — срочная передача.

Основные принципы реализации гарантированной и срочной передачи трафика DiffServ на промежуточных узлах в сети Интернет приведены в следующих документах, соответственно:

- Assured Forwarding PHB Group (IETF RFC 2597: June 1999: Standards Track);
- An Expedited Forwarding PHB (IETF RFC 2598: June 1999: Standards Track).

В табл. 12.5 показаны характеристики классов обслуживания, соответствующие значениям поля DSCP. Поле DROP PRECEDENCE определяет относительную возможность удаления блоков данных данного класса при возникновении перегрузки канала. Таким образом, внутри каждого класса обслуживания могут быть организованы три дополнительных класса с индивидуальными уровнями обслуживания.

Таблица 12.5. *Значения битов поля DSCP*

Номер	Характеристика COS для канала	Class Selector	Поле DROP PRECEDENCE	Двоичное значение	Десятичное значение
1	AF11	1	Low	001010_2	10_{10}
2	AF12	1	Medium	001100_2	12_{10}
3	AF13	1	High	001110	14_{10}

Таблица 12.5 (окончание)

Номер	Характеристика COS для канала	Class Selector	Поле DROP PRECEDENCE	Двоичное значение	Десятичное значение
4	AF21	2	Low	010010_2	18_{10}
5	AF22	2	Medium	010100_2	20_{10}
6	AF23	2	High	010110_2	22_{10}
7	AF31	3	Low	011010_2	26_{10}
8	AF32	3	Medium	011100_2	28_{10}
9	AF33	3	High	011110_2	30_{10}
10	AF41	4	Low	100010_2	34_{10}
11	AF42	4	Medium	100100_2	36_{10}
12	AF43	4	High	100110_2	38_{10}
13	EF	—	—	101110_2	46_{10}
14	EF/RESERVED	—	—	$xxxx01_2$	—

Основные принципы маркирования трафика мультисервисных ЛВС

Особенность мультисервисных ЛВС состоит в том, что передаваемый через них трафик содержит множество разнородных информационных потоков, для обработки которых требуется использование индивидуальных уровней QoS. Поскольку большинство таких потоков не присутствует в ЛВС постоянно, задача выделения им необходимой полосы пропускания для обеспечения требуемого уровня QoS должна решаться в реальном масштабе времени.

В листинге 12.1 приведена структура кадра Ethernet, который используется для передачи Multicast-трафика в мультисервисной сети. Данный листинг получен с использованием программного анализатора протоколов SoftPerfect Network Protocol Analyzer компании SoftPerfect Research. Анализируемый кадр содержит данные потока, передаваемого от группового сервера 192.168.255.2 для абонентов Multicast-группы 239.255.0.16. Для обеспечения требуемого уровня качества обслуживания у этого кадра установлен признак QoS сетевого уровня в формате IPprec = 4.

Листинг 12.1. Кадр Ethernet, используемый для передачи Multicast-трафика

```
1. Заголовок канального уровня (Ethernet)
   Destination: 01:00:5E:7F:00:10
```

```
      Source: 00:12:01:27:09:7F
      Type: 0x0800 Internet Protocol
   2. Заголовок сетевого уровня (IPv4)
      Version: 4 (IP, Internet Protocol)
      Header length: 5 (20 bytes)
      Type of service: 0x80              // Установленное значение IPPREC
            100..... (Flash Override) // соответствует DSCP = AF40
            ...0.... (Normal delay)
            ....0... (Normal throughput)
            .....0.. (Normal relibility)
            ......0. (Normal monetary cost)
            .......0 (Reserved flag is not set)
      Total length: 1344 bytes
      Identification: 51566
      Flags: 0x4000
            DF .1..... (Don't fragment)
            MF ..0..... (Last fragment)
      Fragment offset: 0
      Time to live: 2 hops (seconds)
      Protocol: UDP (0x11)
      Header checksum: 0xFA03 (Correct)
      Source IP: 192.168.255.2
      Destination IP: 239.255.0.16
      No options
   3. Заголовок транспортного уровня UDP
      Source port: 32946
      Destination port: 1234
      Length: 1324 bytes
      Checksum: 0x95AA (Correct)
Data: 1316 bytes
```

Для упрощения процедуры классификации могут быть использованы различные способы, среди которых в первую очередь следует выделить:

- включение источников трафика в QoS-домен;
- применение автоматической классификации.

При использовании первого способа формирование признака QoS выполняется непосредственно на источнике абонентского трафика и, следовательно, на граничный узел QoS-домена поступает уже соответствующим образом помеченный трафик. Это позволяет существенно понизить нагрузку и сократить время выполнения операций по обеспечению качества обслуживания на наиболее загруженных граничных узлах QoS-домена. Главным недостатком этого способа является потеря управления маркированием на граничном узле и неконтролируемое расширение границ QoS-домена.

В листинге 12.2 приведен фрагмент конфигурационного файла коммутатора Cisco Systems, сформированного для включения источников трафика в QoS-домен в части доверия к признаку IPprec.

Листинг 12.2. Обеспечение доверия к признаку IPprec на порту коммутатора Cisco Systems

```
    1. Переход в режим настройки интерфейса
Interface f0/1
    2. Организация на интерфейсе режима доверия к признаку IPprec
mls qos trust ip-precedence
```

Суть процедуры автоматической классификации состоит в том, что для всего трафика, который поступает от абонента на определенный порт коммутатора, автоматически назначается один класс обслуживания. Очевидно, что применение этой процедуры также существенно упрощает реализацию классификации на граничном узле QoS-домена. Недостатки автоматической классификации проявляются в том случае, если трафик абонента не является однородным, а содержит в себе несколько потоков с различными требованиями к уровню QoS. Примером такого абонента является IP-телефон, совмещающий в себе функции коммутатора. Через Ethernet-интерфейс такого IP-телефона будут передаваться два вида трафика — оцифрованный голосовой трафик VoIP и обычный трафик сети передачи данных от рабочей станции, подключенной к IP-телефону через интерфейс расширения.

Для автоматической настройки параметров QoS в подобных ситуациях на порту коммутатора Cisco Systems может быть использован специальный режим Auto QoS VoIP. Особенность этого режима заключается в том, что помимо автоматической настройки параметров QoS для передачи двух видов трафика, этот режим обеспечивает управляемое включение функции доверия к признакам QoS принимаемого трафика.

В листинге 12.3 приведен фрагмент конфигурационного файла коммутатора Cisco Systems, сформированного для включения функции автоматического конфигурирования параметров QoS. В данном случае функция доверия к признакам QoS принимаемого трафика будет автоматически активизирована только в том случае, если к порту коммутатора будет подключен VoIP-телефон компании Cisco Systems.

Листинг 12.3. Обеспечение доверия к признаку IPprec на порту коммутатора Cisco Systems

```
    1. Переход в режим настройки интерфейса
Interface f0/1
    2. Включение функции автоматического конфигурирования параметров QoS
auto qos voip cisco-phone
```

Реализация классификации в ЛВС

Основная особенность задачи классификации DiffServ состоит в том, что она обрабатывает все входные блоки данных и, следовательно, должна выполняться всякий раз, когда очередной такой блок поступает на устройство. Поэтому для сохранения требуемого темпа обработки данных на этом устройстве необходимо, чтобы для решения этой задачи требовалось как можно меньше времени и вычислительных ресурсов центрального процессора. Эта задача решается относительно просто при наличии признака классовой принадлежности в обрабатываемом блоке данных — на внутренних узлах QoS-домена. Выполнение классификации на пограничных узлах домена QoS осложняется тем, что именно на этих узлах производится реализация алгоритма назначения меток классовой принадлежности. Этот алгоритм обычно выполняется при помощи списков управления доступом — ACL (Access Control List), и его сложность определяется характером формируемой политики QoS.

Аппаратная реализация списков доступа в узлах ЛВС обычно выполняется по тем же принципам и в тех же блоках, что и аппаратная маршрутизация, но имеет свои особенности. Особенность аппаратной реализации списков доступа состоит в том, что параллельный характер ее выполнения в некоторых случаях может нарушить заданный администратором порядок следования правил. В таких ситуациях производители телекоммуникационного оборудования предлагают администраторам использовать специальные дополнительные параметры команд, которые указывают порядок применения правил в тех случаях, когда это необходимо. Примером подобного параметра является Match-Order Config, который может быть использован при построении списков доступа на оборудовании 3COM.

Для реализации классификации DiffServ на активном оборудовании современных ЛВС обычно используются списки доступа как сетевого, так и канального уровня. В *главе 7* был приведен пример создания списка доступа сетевого уровня на коммутаторе Cisco Systems (см. листинг 7.5). В листинге 12.4 приведен пример создания списка доступа канального уровня на коммутаторе 3COM. Правило этого списка выделяет кадры с MAC-адресами назначения в диапазоне с 0100-5e00-0000 по 0100-5e7f-ffff, которые используются для передачи трафика Multicast-приложений. Сформированный таким образом список доступа в дальнейшем может быть использован для выполнения любых задач, связанных с реализацией выбранной политики DiffServ на данном коммутаторе.

Листинг 12.4. Создание списка доступа канального уровня на коммутаторе 3COM

```
1. Переход в режим изменения конфигурации системы
<4500>system-view
System View: return to User View with Ctrl+Z
```

```
   2. Создание нумерованного списка доступа канального уровня
[4500]acl number 4001
   3. Создание правила, которое выделяет кадры Multicast-приложений из
      общего потока
[4500-acl-ethernetframe-4001] rule 1 permit destination 100-5e00-0000
0000-007f-ffff
   4. Возвращение в исходный режим
[4500]quit
<4500>
```

Методы и способы нормирования трафика приложений

В современных ЛВС одним из наиболее распространенных способов обеспечения требуемого уровня QoS является управляемое нормирование — ограничение трафика клиентских приложений. Механизм ограничения является, по сути, единственным доступным средством для обеспечения требуемого уровня качества обслуживания, поскольку технологии Ethernet и Интернета не имеют собственных встроенных инструментов для решения подобных задач.

Применение этого механизма обычно заключается в том, чтобы уменьшить загрузку канала передачи данных трафиком менее приоритетных приложений, обеспечив тем самым необходимое расширение полосы пропускания канала для передачи трафика более приоритетных приложений.

Для этого на активном оборудовании ЛВС могут быть использованы два основных метода:

- административное ограничение клиентского трафика (Traffic Policing);
- регулирование параметров клиентского трафика (Traffic Shaping).

Основное отличие между ними состоит в том, что при использовании первого метода трафик, поступающий с нарушением установленных соглашений, подлежит уничтожению. Регулирование параметров позволяет сглаживать пульсации клиентского трафика и тем самым снижать вероятность потери передаваемых данных при нормировании.

Алгоритм Leaky Bucket

Большинство методов, которые используются для ограничения и регулирования трафика, основано на применении алгоритма "дырявого ведра" (Leaky Bucket).

В этом алгоритме используются следующие понятия:

- согласованное значение информационной скорости — *CAR* (Committed Access Rate) или *CIR* (Committed Information Rate);

- согласованное значение объема передаваемых данных — *Bc* (Burst Committed);
- интервал измерения объема передаваемых данных — *T*.

Если рассматривать аналогию с ведром, то значение Bc определяет объем этого ведра. Значение CIR соответствует скорости, с которой вода должна вытекать из ведра, чтобы за интервал T вылить весь его объем Bc полностью. Очевидно, что используемые в этом алгоритме понятия связаны следующим соотношением:

$$CAR = Bc / T.$$

Модель Leaky Bucket можно использовать для описания функционирования порта, через который производится нормированная отправка трафика клиентских приложений. Значение CAR в этом случае соответствует информационной скорости порта, а значения Bc и T выбираются таким образом, чтобы обеспечить требуемую схему обработки поступающего трафика. Например, если значение CAR составляет 1 Мбит/сек, а значение T равно 1 сек, то величина Bc должна составлять 1 Мбит. Таким образом, если усредненное за секунду значение скорости поступления данных на порт не будет превышать 1 Мбит/сек, то перегрузка на порту возникать не будет, и все полученные данные будут отправлены. В том случае, если данные на порт будут поступать с большей скоростью, например 1,1 Мбит/сек, то возникнет состояние перегрузки порта, в котором за каждую секунду будет теряться 0,1 Мбит входного трафика. В описанной выше модели это соответствует ситуации, когда поступающая слишком сильным потоком вода начинает переливаться через верхний край ведра.

Таким образом, значение Bc соответствует максимальному объему принимаемых на порт данных, передача которого через порт может быть гарантирована при установленных значениях CAR и T. В некоторых схемах регулирования трафика допускается кратковременное превышение этого объема на величину согласованного превышения допустимого объема — Be, но при этом для обработки дополнительного трафика используются специальные процедуры, позволяющие обеспечить для него независимый уровень обслуживания.

Административное ограничение клиентского трафика

Административное ограничение представляет собой строгую процедуру нормирования, при использовании которой часть клиентского трафика, поступающая с нарушением установленных ограничений, подлежит уничтожению. Процедуры административного ограничения, как правило, относительно просты для реализации, поскольку в данном случае администратор определяет только согласованное значение информационной скорости для выбранного

порта или класса обслуживания. Правила административного ограничения клиентского трафика могут быть использованы для управления информационными потоками, как на входном, так и на выходном интерфейсах.

Наиболее простым методом административного ограничения является фиксирование скорости передачи и (или) приема данных для порта на физическом уровне. При этом для всех потоков, передаваемых или принимаемых через данный порт, устанавливается предельное суммарное значение информационной скорости, которое не может быть превышено ни при каких обстоятельствах.

Примечание

Установленные значения скоростей, разумеется, не могут превышать текущие значения скорости информационного обмена, установленные для данного интерфейса.

В листинге 12.5 приведен пример установки административного ограничения до 6 Мбит/сек скорости передаваемых данных на коммутаторе AT-9724TS компании Allied Telesyn.

Листинг 12.5. Ограничение скорости передаваемых данных на коммутаторе Allied Telesyn

```
AT-9724TS:4# config bandwidth_control 1:1 tx_rate 6
Command: config bandwidth_control 1:1 tx_rate 6
Success.
AT-9724TS:4#
```

Описанный ранее метод административного ограничения клиентского трафика на физическом уровне имеет ряд существенных недостатков, главным из которых является отсутствие возможности реального управления трафиком. Правило этого метода действует одинаково на любой компонент трафика вне зависимости от того, к какому классу обслуживания этот компонент принадлежит. Вместе с тем, использование данного метода будет целесообразным в тех случаях, когда ограничение трафика выполняется для предотвращения возникновения аварийных ситуаций.

Для организации действительно управляемого административного ограничения клиентского трафика администратор должен определить предельную скорость информационного потока для всех или нескольких классов обслуживания передаваемого трафика.

В листинге 12.6 приведен фрагмент конфигурационного файла коммутатора компании 3COM, в котором выполняется административное ограничение скорости принимаемого трафика. В данном случае ограничение обеспечивает

уменьшение до указанного значения скорости передачи через интерфейс 1/0/1 трафика, который принимается на канальном уровне в режимах Unicast и Broadcast.

Листинг 12.6. Создание списка доступа канального уровня на коммутаторе 3COM

```
   1. Переход в режим изменения конфигурации системы
<4500>system-view
System View: return to User View with Ctrl+Z
   2. Создание нумерованного списка доступа канального уровня
[4500]acl number 4002
   3. Создание правил, которые выделяет кадры Multicast-приложений из
      общего потока
[4500-acl-ethernetframe-4002] rule 1 deny destination 100-5e00-0000 0000-
007f-ffff
[4500-acl-ethernetframe-4002] rule 2 permit destination 0-0-0 0-0-0
   4. Переход в режим изменения конфигурации интерфейса
[4500]interface Ethernet 1/0/1
   5. Административное ограничение скорости обработки поступающего на
      интерфейс не Multicast-трафика до 3,2 Мбит/сек
[4500-Ethernet1/0/1] traffic-limit inbound link-group 4002 3200
   6. Возвращение в исходный режим
[4500-Ethernet1/0/1] quit
<4500>
```

Регулирование параметров клиентского трафика

Методы регулирования параметров клиентского трафика позволяют обеспечить более эффективное и гибкое управления информационными потоками клиентских приложений. Это обеспечивается благодаря использованию всех компонентов модели Leaky Bucket, применению буферных запоминающих устройств и специальных методов для выравнивания трафика. Применение методов регулирования трафика позволяет предотвратить возникновение перегрузок на каналах передачи данных, сократив при этом до минимума вероятность потери нормируемого трафика.

Для того чтобы обеспечить регулирование параметров клиентского трафика, администратор для выделенной группы абонентов определяет значения всех параметров модели Leaky Bucket — CAR, Bc, Be и T. В листинге 12.7 приведен пример настройки и проверки выполнения регулирования параметров клиентского трафика на маршрутизаторе Cisco Systems. Пункты 1 и 2 листинга отображают процесс создания правила для разделения абонентского трафика. Пункты 3 и 4 листинга отображают процесс настройки параметров вы-

равнивания для выбранной части трафика: значение согласованной информационной скорости CAR выбрано равным 50 Кбит/сек, величины разрешенного и превышающего объема трафика составляют в данном случае 8 Кбит. Последний параметр команды определяет максимальное количество буферов, разрешенных к использованию при выполнении данной процедуры выравнивания.

Листинг 12.7. Регулирование параметров клиентского трафика на маршрутизаторе Cisco Systems

```
   1. Переход в режим создания расширенных //проверяющих адрес
      назначения и адрес источника пакета //списков доступа
Ip access-list extended 128
   2. Создание нумерованного правила
access-list 128 deny ip any  224.0.0.0 15.255.255.255
access-list 128 permit ip any any
   3. Переход в режим настройки интерфейса
Interface f0/1
   4. Установка параметров регулирования клиентского трафика //CAR =
      50 Кбит/сек, Bc = Be= 8 Кбит
traffic-shape group 128 50000 8000 8000 1000
   5. Проверка текущих настроек процедуры выравнивания на маршрутизаторе
ST-2811#sh traffic-shape
...
Interface   Fa0/1
      Access Target     Byte   Sustain   Excess    Interval  Increment
VC    List   Rate       Limit  bits/int  bits/int  (ms)      (bytes)
Active
-     124    10000      2000   8000      8000      800       1000      -
-     128    50000      2000   8000      8000      160       1000      -
-     122    128000     1984   7936      7936      62        992       -
-     120    10000      2000   8000      8000      800       1000      -
-     126    128000     1984   7936      7936      62        992       -
   6. Отображение статистических данных выполнения процедуры
      выравнивания
ST-2811#sh traffic-shape statistics
                Acc. Queue Packets   Bytes      Packets   Bytes      act
I/F             List Depth                     Delayed   Delayed
Active
Fa0/0             144 0     9730408  11769225 31019806  2110050095 no
Fa0/1             124 0     0        0        0         0          no
Fa0/1             128 15    9347789  825660953 3887677  208264537  yes
Fa0/1             122 0     0        0        0         0          no
Fa0/1             120 0     62       4717     0         0          no
Fa0/1             126 0     0        0        0         0          no
```

```
   7. Отображение состояния очередей, которые используются для
      выравнивания абонентского трафика
ST-2811#sh traffic-shape queue
...
Traffic queued in shaping queue on FastEthernet0/1
 Traffic shape group: 128
  Queueing strategy: weighted fair
  Queueing Stats: 3/1000/64/10268 (size/max total/threshold/drops)
     Conversations  1/16/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 50 kilobits/sec
...
ST-2811#
```

Пункты 5, 6 и 7 листинга 12.7 отображают результаты контроля выполнения выравнивания на данном маршрутизаторе.

В некоторых случаях в дополнение к регулированию параметров клиентского трафика администратору предоставляется возможность определить тип акции, применяющейся к той части трафика, которая будет передана с нарушением установленных ограничений. Примером подобной акции может быть, например, перевод этой части трафика в группу с пониженным уровнем приоритета.

В листинге 12.8 приведен пример настройки регулирования параметров клиентского трафика на коммутаторе Cisco Systems. Для выделения группы входного трафика в данном случае применяется такой же ACL 128, который был использован в предыдущем примере. В соответствии с правилами сформированной политики, для той части трафика, которая превысит установленный лимит скорости, будет выполнено понижение приоритета.

Листинг 12.8. Регулирование параметров клиентского трафика на коммутаторе Cisco Systems

```
   1. Определение группы абонентского трафика, в которую входят все
      не-Multicast-приложения
3750(config)# class-map NOMULT
3750(config-cmap)# match access-group 128
3750(config-cmap)# exit
   2. Создание политики для реализации заданных правил нормирования
      трафика
3750(config)# policy-map newone
3750(config-pmap)# class NOMULT
3750(config-pmap-c)# police 50000 8000 exceed-action policed-dscp-transmit
```

```
3750(config-pmap-c)# exit
3750(config-pmap)# exit
   3. Применение политики на интерфейсе коммутатора
3750(config)# interface f0/1
3750(config-if)# service-policy input newone
```

Управление нормированием абонентского трафика

Методы нормирования абонентского трафика основаны на применении разнообразных механизмов упорядочивания (Queuing) трафика. Для каждого из классов обслуживания (CoS) создается очередь (Queue), в которую помещаются поступившие на обработку блоки данных этого класса. В классовых очередях блоки данных одного класса обычно обслуживаются по принципу *FIFO* (First In — First Out — "первый пришел — первый ушел"). Относительный порядок и способ обслуживания классовых очередей, в свою очередь, определяются приоритетом соответствующего класса и выбранным способом нормирования трафика абонентских приложений. Для обслуживания классовых очередей могут использоваться две разновидности алгоритмов:

- алгоритмы строгой очереди приоритетов — *SPQ* (Strict Priority Queuing);
- циклические алгоритмы взвешенного выбора — *WRR* (Weighted Round Robin).

При использовании алгоритмов SPQ абсолютное преимущество при обслуживании имеют блоки данных, которые находятся в очереди с более высоким приоритетом. Пока в наиболее приоритетной очереди находится хотя бы один блок данных, очереди с меньшими значениями приоритетов просто не обслуживаются. Очевидно, однако, что применение алгоритмов SPQ может привести к неконтролируемому увеличению задержек передачи и к потерям данных пониженного приоритета.

Алгоритмы WRR используют более гибкую схему нормирования, которая обеспечивает обслуживание очередей с низким уровнем приоритета даже в том случае, если очереди более высокого приоритета обслужены не полностью. Управление нормированием абонентского трафика в данном случае состоит в том, чтобы определить долю пропускной способности канала, которая закрепляется за каждой из классовых очередей. В листинге 12.9 приведен пример настройки схемы нормирования трафика абонентских приложений на коммутаторе Cisco Systems.

Листинг 12.9. Регулирование параметров клиентского трафика на коммутаторе Cisco Systems

```
   1. Переход в режим конфигурирования параметров интерфейса f0/1
3750(config)# interface f0/1
```

2. Ограничение до 10% предельной доли пропускной способности интерфейса, которая может быть использована для обслуживания очереди 1

```
3750(config-if)# srr-queue bandwidth shape 10 0 0 0
```

3. Распределение пропускной способности интерфейса между очередями 1, 2, 3 и 4 в следующем соотношении 1, 2 – 10%, 3 - 30%, 4 - 50%

```
3750(config-if)# srr-queue bandwidth share 1 1 3 5
```

Рекомендации по управлению трафиком приложений

Применение модели с распределенным управлением в мультисервисных ЛВС, однако, вовсе не гарантирует, что установленная система приоритетов будет повсеместно соблюдена, и соответствующие приложения получат в свое распоряжение требуемые ресурсы сети. Дело в том, что схема организации классового обслуживания не может учитывать фактических значений нормируемых параметров ЛВС в каждый момент времени.

Применения описанных ранее методов и процедур может оказаться недостаточно, например, для обеспечения гарантированного значения задержки доставки блоков данных. Особенно сильно величина этой задержки влияет на выполнение мультимедийных приложений. В частности установлено, что для нормального функционирования приложений технологии VoIP величина задержки не должна превышать значение 0,15 сек. Для того чтобы обеспечить гарантированное выполнение этого требования в условии, когда мультимедийный трафик конкурирует за право обладания сетевым ресурсом с трафиком локальной вычислительной сети, должен применяться метод Fragmentation (дробление больших дейтаграмм).

Целесообразным может также оказаться увеличение запаса пропускной способности и производительности центральных процессоров на магистральных узлах ЛВС.

Постоянный мониторинг состояния каналов передачи данных и управление возникающими в них перегрузками также позволят существенно повысить качество передачи данных в мультисервисной ЛВС.

Управление трафиком в чрезвычайных ситуациях

В предыдущем разделе было отмечено, что для гарантированного обеспечения качества обслуживания каналы передачи данных, используемые при по-

строении ЛВС, должны иметь достаточный резерв пропускной способности. Однако в некоторых случаях применение высокоскоростных каналов может привести к возникновению перегрузок в мультисервисных ЛВС. При возникновении перегрузки коммутатор ЛВС обрабатывает поступающие данные на предельной для себя скорости при полном использовании ресурсов интерфейса или управляющего процессора. Подобные ситуации могут быть вызваны ошибками проектирования, несогласованными изменениями конфигурации или неправильными действиями оператора. При возникновении перегрузки на порту происходит потеря большого объема трафика абонентских приложений и, в некоторых случаях, временное прекращение обслуживания.

Поэтому, во избежание возникновения чрезвычайных ситуаций в будущем, целесообразно организовать надлежащую защиту от них в ЛВС заблаговременно.

Предотвращение перегрузок на порту коммутатора

Предотвращение возникновения перегрузок на порту коммутатора выполняется с целью обеспечения автоматической адаптации трафика абонентских приложений. Для предотвращения возникновения перегрузок на порту коммутатора могут быть использованы две различные стратегии:

- отсечение излишков принимаемого трафика — *TD* (Tail Drop);
- предупредительное уничтожение некоторых из его компонентов — *WRED* (Weighted Random Early Detect).

При использовании стратегии TD для каждой из классовых очередей на коммутаторе может быть определено одно или несколько пороговых значений. В случае увеличения длины очереди за пределы установленного ограничения излишний трафик будет удален. Основным недостатком стратегии TD является то, что она, как правило, применяется уже после возникновения перегрузки, что существенно снижает эффективность ее использования.

В отличие от предыдущей стратегии, WRED может начать свое действие задолго до возникновения перегрузки, поскольку ее использование предполагает случайное удаление компонентов передаваемых данных после того, как скорость их поступления превысит установленное пороговое значение. Факт потери данных укажет приложению на то, что используемая им пропускная способность близка к предельной, после чего достигнутая скорость не будет увеличиваться. В листинге 12.10 приведен фрагмент конфигурационного файла коммутатора компании 3COM, созданный для ограничения трафика абонентских приложений с использованием стратегии WRED.

Листинг 12.10. Ограничение трафика абонентских приложений с использованием стратегии WRED на коммутаторе 3COM

```
   1. Переход в режим изменения конфигурации системы
<4500>system-view
System View: return to User View with Ctrl+Z
   2. Переход в режим изменения конфигурации интерфейса
[4500]interface Ethernet 1/0/1
   3. Применение стратегии WRED для трафика, передаваемого через
      интерфейс со скоростью свыше 32 Кбит/сек.
      Вероятность уничтожения — 50%
[4500-Ethernet1/0/1]wred 0 32 50
   4. Возвращение в исходный режим
[4500-Ethernet1/0/1] quit
<4500>
```

Предотвращение широковещательных штормов

Наиболее опасным последствием возникновения перегрузки является то, что она делает сеть неуправляемой. Например, при возникновении широковещательного "шторма" в неподготовленной к нему ЛВС все подключенные к ней коммутаторы могут оказаться недоступными не только для удаленного, но и для локального управления. Все это может крайне затруднить процесс локализации и устранения неисправности. Наиболее простым способом, который может быть использован для предотвращения подобных ситуаций, является административное ограничение скорости передаваемого через порт трафика в сочетании с автоматически выполняемым действием в момент ее возникновения.

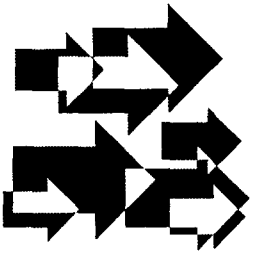
В листинге 12.11 приведен пример настройки и проверки состояния системы предотвращения перегрузок на коммутаторе Cisco Systems.

Листинг 12.11. Пример настройки и проверки состояния системы предотвращения перегрузок на коммутаторе Cisco Systems

```
2950_ST#sh run int f0/2
Building configuration...

Current configuration : 135 bytes
!
interface FastEthernet0/2
 switchport access vlan 100
// На порту установлен уровень включения действия, соответствующий
// 30-процентной загрузке интерфейса широковещательным трафиком
 storm-control broadcast level 30.00 10.00
```

```
// Тип установленного действия - выключение интерфейса при возникновении
// аварийной ситуации
 storm-control action shutdown
end
// Проверка параметров системы предотвращения перегрузок, установленных
// для порта fastEthernet 0/2
2950_ST#sh storm-control fastEthernet 0/2
Interface  Filter State   Trap State     Upper    Lower    Current  Traps
Sent
---------  -------------  -------------  -------  -------  -------  -----
Fa0/2      Forwarding     inactive       30.00%   10.00%    0.00%       0
2950_ST#
```



ЧАСТЬ III

Структура и компоненты мультисервисных ЛВС

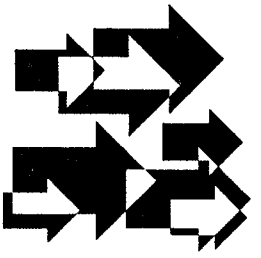
Глава 13. Способы и схемы построения мультисервисных ЛВС

Глава 14. Построение магистральных соединений мультисервисных ЛВС

Глава 15. Организация подключения абонентов к оборудованию мультисервисных ЛВС

Глава 16. Программные компоненты мультисервисных ЛВС

ГЛАВА 13



Способы и схемы построения мультисервисных ЛВС

Структура ЛВС определяется совокупностью использованных при ее построении способов организации информационного обмена и схем соединения активных компонентов (коммутаторы, маршрутизаторы, каналообразующая аппаратура) с абонентами ЛВС (серверы и рабочие станции). Выбор структуры во многом определяется характером и особенностями тех процессов передачи данных в ЛВС, для организации которых и создается локальная сеть. Следует отметить, что схема взаимного соединения компонентов — топология ЛВС, как правило, тесно связана с технологией, которая используется для передачи данных. И наоборот, выбор технологии передачи данных в ЛВС зачастую однозначно определяет тип схемы соединения активных компонентов этой сети.

Большое влияние на выбор топологии построения ЛВС оказывает относительное расположение абонентов. Абоненты локальных сетей прежних лет, как правило, размещались на ограниченном пространстве — в пределах одного или нескольких зданий, что делало эти сети действительно локальными. Специфика современных мультисервисных сетей состоит в том, что абоненты этих ЛВС могут находиться как в отдельном здании (офис небольшой организации), так и быть распределены на площади крупного городского района (клиентская сеть мультисервисного провайдера). В этой ситуации при проектировании следует особенно внимательно учитывать особенности конкретной реализации каждой из топологий при построении ЛВС с тем, чтобы обеспечить максимальную эффективность технических решений.

В первом разделе данной главы рассматриваются наиболее распространенные варианты топологии построения ЛВС — шинная, иерархическая и кольцевая. Более подробно в этом разделе рассматриваются особенности шинной и иерархической организации ЛВС.

Второй раздел данной главы посвящен рассмотрению разнообразных технологий, которые применяются при построении кольцевых топологий ЛВС. В этом разделе, в частности, кратко рассматриваются особенности таких технологий, как Token Ring и FDDI и, более подробно, технологии построения кольцевых пакетных магистралей SRP/RPR.

Типы и разновидности топологий ЛВС

Как уже было отмечено во вступлении к данной главе, способ взаимного соединения активных компонентов и абонентов принято называть топологией ЛВС. Наиболее распространенными вариантами топологии построения ЛВС являются:

- *шинная топология*;
- *иерархическая топология*;
- *кольцевая топология*.

Шинная топология ЛВС имела наибольшее распространение при построении ЛВС на основе ранних технологий Ethernet/IEEE 802.3. Последующее развитие этих технологий и необходимость существенного повышения скорости информационного обмена привело к широкому внедрению коммутируемых сетей Ethernet/IEEE 802.3, которые имеют иерархическую топологию "многоуровневая звезда". Отдельного рассмотрения заслуживают ЛВС, построенные с использованием кольцевой топологии соединения компонентов. Несмотря на то, что основные принципы построения таких сетей были разработаны в конце прошлого века, многие из этих принципов не теряют своей актуальности и при построении современных ЛВС.

При анализе и сравнении различных вариантов построения топологии ЛВС обычно используют следующие критерии:

- обеспечение требуемой производительности;
- обеспечение требуемого уровня информационной безопасности;
- устойчивость к возникновению отказа;
- возможность масштабирования;
- стоимость реализации.

Шинная топология ЛВС

Тип топологии ЛВС во многом определяется типом используемой среды передачи данных. Так, например, наиболее эффективно шинная топология ЛВС может быть реализована только на средах передачи данных, допускающих

множественный доступ абонентов — типичным примером такой среды является коаксиальный кабель.

Характерными чертами сетей, построенных по шинной топологии, являются равные возможности и отсутствие управления доступом абонентов к общим ресурсам ЛВС.

Принципы построения ЛВС шинной топологии

Сети, построенные с использованием шинной топологии на основе коаксиального кабеля в качестве среды передачи данных, обеспечивают передачу информационного сигнала на расстояние 200—500 м без использования усилителей (репитеров). Именно по этой причине ЛВС с шинной топологией являются наиболее дешевыми, обеспечивая возможность информационного обмена без использования активных компонентов ЛВС. Такие сети легко масштабируются, причем к одному сегменту одновременно может быть подключено от 30 до 100 рабочих станций. Как размер сегмента, так и количество одновременно подключенных к нему абонентов ЛВС могут увеличиваться при использовании сетевых повторителей — репитеров.

Локальные сети с шинной топологией могут быть построены и на сегментах типа "неэкранированная витая пара" — *UTP* (Unshielded Twisted Pair), однако из-за особенностей передачи данных Ethernet в среде этого типа, к физическому сегменту в данном случае может быть подключено не более 2 абонентов.

На рис. 13.1 представлены варианты подключения абонентов к физическому сегменту ЛВС, имеющей шинную топологию.

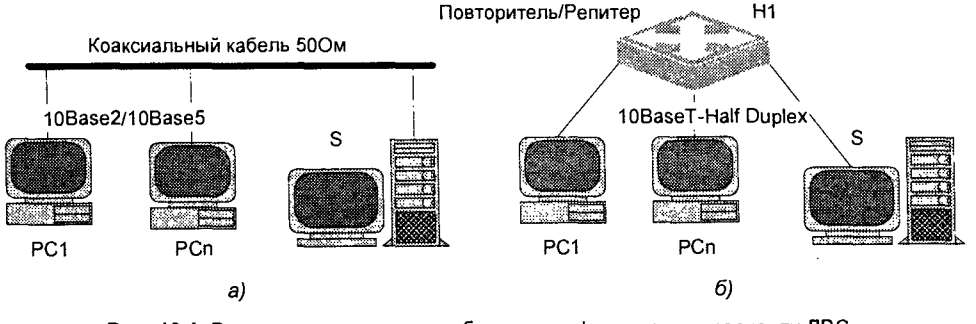


Рис. 13.1. Варианты подключения абонентов к физическому сегменту ЛВС, имеющей шинную топологию

В данном случае для подключения абонентов к ЛВС по первому варианту (рис. 13.1, *а*) используется коаксиальный кабель. Локальная сеть, представленная на рис. 13.1, *б*, основана на использовании UTP в качестве среды пе-

редачи данных. В последнем случае физическая неисправность одного абонента не приводит к нарушению функционирования ЛВС в целом, но при этом максимальный размер сегмента не должен превышать 100 м.

Особенности ЛВС с разделяемой средой передачи данных

Основными недостатками ЛВС, построенных с использованием шинной топологии, являются:

- низкая устойчивость к возникновению отказов;
- невозможность управления полосой пропускания в сегменте;
- ограниченность пропускной способности.

Возникновение неисправности у любого из абонентов, подключенного к сегменту ЛВС, приводит, как правило, к отказу всего сегмента в целом. Все абоненты, подключенные к единому сегменту, разделяют между собой его пропускную способность (обычно 10 Мбит/сек). В локальных сетях, которые имеют топологию *общей шины* (ОШ), невозможно реализовать вариант, когда один из абонентов, например, сервер S, имеет большую скорость передачи данных, чем остальные, к примеру, рабочие станции PCn. В дополнение к этому следует отметить, что ЛВС, имеющие топологию ОШ, как правило, используют полудуплексный режим информационного обмена, что еще больше снижает скорость передачи данных. Все эти причины в совокупности делают нецелесообразным применение топологии ОШ при построении современных мультисервисных ЛВС.

Иерархические структуры ЛВС

От большинства недостатков, которые свойственны локальным сетям с топологией ОШ, свободны локальные вычислительные сети (ЛВС), имеющие иерархическую топологию.

Иерархическими называются структуры ЛВС, которые разделены на несколько уровней таким образом, что непосредственно взаимодействовать могут только устройства соседних уровней. Поэтому иерархические структуры ЛВС, как правило, представляют собой пирамиды, на нижнем уровне которых размещаются наименее производительные устройства, которые и обеспечивают непосредственное подключение абонентов. На последующих, более высоких уровнях действуют более производительные устройства, обеспечивающие информационный обмен между устройствами нижнего уровня.

В дальнейшем будет использована терминология, применяемая многими компаниями-производителями коммуникационного оборудования, например, Cisco Systems, при описании иерархических структур ЛВС. В соответствии

с установившейся терминологией и практикой проектирования, в иерархических ЛВС принято выделять три уровня обработки данных:

- *уровень доступа* (Access Layer);
- *уровень распределения* (Distribution Layer);
- *уровень ядра ЛВС* (Core Layer).

Трехуровневая иерархическая структура ЛВС позволяет наиболее экономично и эффективно реализовать основные требования, которые предъявляются к характеристикам современных мультисервисных сетей. В последующих разделах назначение и функции каждого из этих уровней будут рассмотрены более подробно.

Задачи, решаемые на уровне доступа

Уровень доступа является самым нижним уровнем в иерархической ЛВС. Активное оборудование, размещенное на этом уровне, обеспечивает решение следующих задач, которые выполняются на физическом и канальном уровнях OSI ISO 7498:

- непосредственное подключение абонентов ЛВС;
- надежное подключение к активному оборудованию уровня распределения;
- разделение абонентов на функциональные группы;
- обеспечение требуемого уровня качества обслуживания для каждой функциональной группы;
- защита от несанкционированного подключения;
- невысокая стоимость оборудования.

На уровне доступа непосредственное подключение абонентов современных ЛВС выполняется, как правило, отрезками кабеля UTP, с использованием технологий IEEE 802.3 10/100BaseT или 1000BaseT. Особенность информационного взаимодействия в современных мультисервисных ЛВС состоит в том, что большая часть (примерно 80%) совокупного трафика всех абонентов, подключенных на уровне доступа, принимается от внешних, по отношению к этому уровню, источников. Поэтому подключение активного оборудования уровня доступа к активному оборудованию уровня распределения выполняется, как правило, через специальные высокоскоростные магистральные порты. Для магистрального подключения активного оборудования уровня доступа к устройствам ЛВС последующего уровня в зависимости от конфигурации конкретной ЛВС могут быть использованы различные технологии:

- IEEE 802.3 1000BaseT;
- IEEE 802.3 1000Base SX;
- IEEE 802.3 1000Base LX.

В некоторых случаях для этой цели могут быть использованы технологии из комплекса IEEE 802.3 10GBase X.

Примечание

Более подробное описание указанных выше технологий и особенности их использования приведены в *главе 14* настоящего издания.

При выборе технологии, используемой для магистрального подключения, следует, с одной стороны, учитывать особенности относительного расположения активного оборудования уровня доступа, а с другой — принимать во внимание специфические требования к организации информационного обмена в конкретной группе подключаемых абонентов. Так, если вещание для абонентов мультисервисной ЛВС выполняется в одноадресном режиме, например, по протоколу HTTP, групповой сервер должен будет сформировать по одному потоку для каждого из подключенных абонентов. В этом случае магистральный порт коммутатора Ethernet, установленного на уровне доступа, должен обеспечивать передачу суммарного потока от сервера к абонентам. На рис. 13.2 приведена схема информационных потоков на уровне доступа мультисервисной ЛВС при использовании одноадресного режима вещания.

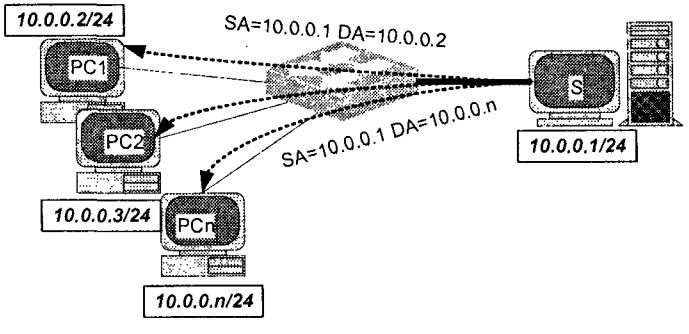


Рис. 13.2. Варианты подключения абонентов к физическому сегменту ЛВС, имеющей топологию ОШ и при одноадресном режиме вещания

Если принять во внимание, что для организации одного видеопотока требуется информационная скорость порядка 8 Мбит/сек, то легко можно определить, что магистральное соединение в ЛВС, схема которой приведена на рис. 13.2, должно обеспечивать передачу данных со скоростью n × 8 Мбит/сек, где n — количество подключаемых абонентов. Следовательно, при использовании магистрального соединения для связи с сервером 1000 Мбит/сек максимальное число подключаемых к нему абонентов не должно превышать 125. Это ограничение, впрочем, достаточно легко можно преодолеть, если использо-

вать на сервере режим многоадресного (Multicast) вещания. Схема информационных потоков, формируемых в мультисервисной ЛВС при использовании многоадресного режима вещания, представлена на рис. 13.3.

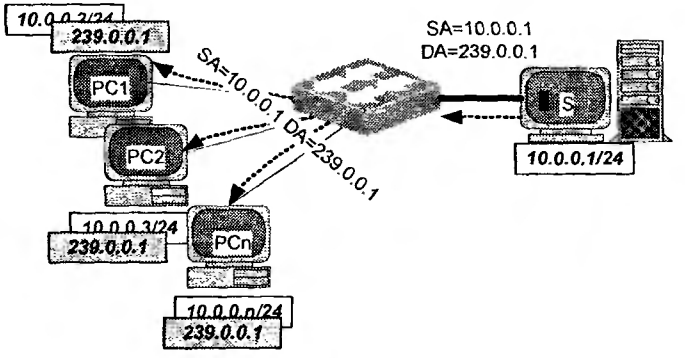


Рис. 13.3. Варианты подключения абонентов к физическому сегменту ЛВС, имеющей топологию ОШ и при многоадресном режиме вещания

В этом случае, независимо от числа подключенных абонентов, сервер формирует только один поток для каждой из групп абонентов (в представленном на рисунке примере эта группа имеет адрес 239.0.0.1). Таким образом, при определении требований к характеристикам магистрального соединения коммутатора, который расположен на уровне доступа ЛВС, в равной степени должны быть учтены и количество подключаемых абонентов, и особенности информационного взаимодействия с ними.

Разделение абонентов на функциональные группы и обеспечение требуемого уровня качества обслуживания для каждой функциональной группы выполняется на коммутаторе доступа Ethernet путем использования аппарата виртуальных сетей IEEE 802.1Q. Передаваемые через коммутатор кадры Ethernet каждой группы помечаются соответствующей меткой, что позволяет осуществлять взаимную изоляцию передаваемых информационных потоков для обеспечения требуемого уровня информационной безопасности. Распределение абонентов между функциональными группами выполняется, как правило, статически, при этом для каждой из функциональных групп может быть также определен относительный уровень качества обслуживания (значение поля PRIORITY метки IEEE 802.1Q). Кадры Ethernet, которые помечены меткой большего приоритета, обслуживаются в первую очередь на всех коммутаторах мультисервисной ЛВС.

Примечание

Более полно вопросы обеспечения информационной безопасности и качества обслуживания абонентов мультисервисных ЛВС рассмотрены в *главах 7 и 12* настоящего издания, соответственно.

На коммутаторах уровня доступа также реализуется защита от несанкционированных подключений абонентов к оборудованию мультисервисной ЛВС. Эта защита выполняется с использованием специальных функций, ограничивающих количество разрешенных подключений к порту коммутатора доступа (Port Security или аналогичные ей процедуры).

Таким образом, активное оборудование, используемое на уровне доступа в иерархической ЛВС, выполняет основные требования, которые возникают при подключении абонентов к мультисервисной ЛВС — обеспечение требуемой пропускной способности, информационной безопасности и установленного уровня качества обслуживания.

Функции, выполняемые на уровне распределения

Уровень распределения является промежуточным уровнем в иерархической ЛВС. Активное оборудование, размещенное на этом уровне, предназначено для решения задач управления информационным обменом между функциональными группами абонентов мультисервисной ЛВС.

Активное оборудование уровня распределения мультисервисной ЛВС обеспечивает решение следующих основных задач, выполняемых на сетевом и канальном уровне OSI ISO 7498:

- информационный обмен между абонентами функциональных групп и серверным оборудованием мультисервисной ЛВС;
- обеспечение информационной безопасности и требуемых параметров информационного обмена на сетевом уровне;
- ограничение распространения по ЛВС невостребованного трафика;
- обеспечение заданного уровня надежности информационного обмена в ЛВС.

При этом один коммутатор уровня доступа иерархической ЛВС, как правило, используется для подключения нескольких коммутаторов уровня распределения. Для повышения надежности информационного обмена в иерархической ЛВС рекомендуется дублировать коммутаторы уровня распределения. На рис. 13.4 приведена схема организации связи между компонентами иерархической ЛВС.

Символами SW-A и SW-D на приведенном рисунке отмечены коммутаторы уровня доступа и уровня распределения соответственно. Для повышения надежности информационного обмена в представленной ЛВС выполнено дублирование коммутаторов уровня распределения и каналов, которыми эти коммутаторы связаны с коммутаторами уровня доступа. Для сокращения возможного простоя ЛВС после выхода из строя одного из коммутаторов уровня распределения, групповые серверы могут быть снабжены дополни

тельными сетевыми интерфейсами, которые обеспечивают их одновременное подключение к основному и резервному коммутаторам распределения.

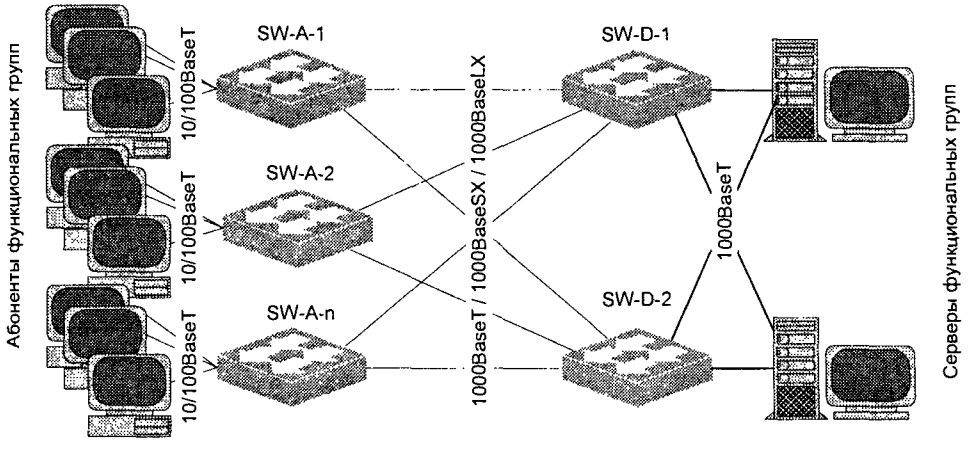


Рис. 13.4. Схема организации связи между компонентами иерархической ЛВС

Повышение эффективности использования основного и резервного оборудования может быть обеспечено благодаря применению таких технологий резервирования, как подробно рассмотренные в *главе 8* многоплановый Spanning Tree протокол MSTP (Multiple Spanning Tree Protocol) и протокол резервирования маршрутизаторов VRRP (Virtual Router Redundancy Protocol), позволяющие обеспечивать динамическое выравнивание нагрузки основных и резервных компонентов ЛВС.

Вследствие того, что каждая функциональная группа ЛВС представляет собой независимый сегмент канального уровня *OSI ISO 7498*, информационный обмен между абонентами различных групп и серверным оборудованием мультисервисной ЛВС может быть выполнен только на сетевом уровне OSI ISO 7498 при помощи маршрутизации. Специфика маршрутизации, которая осуществляется на активном оборудовании уровня распределения в иерархической ЛВС, состоит в том, что обработка пакетов должна выполняться на очень высокой скорости. Поэтому маршрутизация на коммутаторах распределения реализуется аппаратным способом в виде шаблонной или потоковой коммутации.

Применение технологий многоуровневой коммутации на уровне распределения в иерархической ЛВС позволяет на гигабитных скоростях поступления пакетов не только выполнять их маршрутизацию между функциональными группами — виртуальными сетями (VLAN), но и осуществлять фильтрацию этих пакетов с использованием списков управления доступом (ACL) для реа-

лизации политики информационной безопасности. В общем случае политика информационной безопасности, реализуемая на уровне распределения мультисервисной ЛВС, представляет собой перечень правил организации информационного обмена между абонентами функциональных групп и правил доступа абонентов к сетевым ресурсам этой ЛВС.

Ограничение распространения невостребованного трафика на уровне распределения иерархической ЛВС достигается при помощи блокирования широковещательных информационных потоков. Применение маршрутизации автоматически ограничивает область распространения подобных потоков размерами функциональной группы — виртуальной сети. Дополнительная экономия пропускной способности магистрального канала, связывающего коммутатор уровня распределения с коммутатором уровня доступа, может быть достигнута путем блокирования на этом канале кадров тех функциональных групп, которые не имеют абонентов, подключенных к данному коммутатору доступа.

Назначение активного оборудования ядра ЛВС

Активное оборудование, размещенное на уровне ядра ЛВС, обеспечивает управление информационным обменом между всеми абонентами мультисервисной вычислительной сети, а также взаимодействие абонентов ЛВС с внешними сетями и системами. В качестве отдельной группы устройств уровень ядра присутствует только в достаточно крупных ЛВС, где должно быть обеспечено перекрестное соединение нескольких групп коммутаторов уровня распределения. В вычислительных сетях небольшого и среднего размера функции ядра, как правило, могут быть реализованы на коммутаторах уровня распределения. На рис. 13.5 приведена схема организации связи с использованием коммутаторов уровня ядра в иерархической ЛВС.

Основной задачей, которая возлагается на коммутаторы уровня ядра, является высокоскоростная многоуровневая коммутация передаваемых блоков данных. Уровень ядра представляет собой единую высокоскоростную магистраль, которая связывает в единое целое все компоненты ЛВС. Для обеспечения требуемой пропускной способности на каналах, которые связывают коммутаторы ядра ЛВС с коммутаторами уровня распределения, должны быть использованы высокоскоростные технологии передачи данных, например, технологии из группы 10GBase, которые осуществляют передачу данных со скоростью 10 Гбит/сек. Так же, как и на уровне распределения, требуемый уровень надежности информационного обмена на уровне ядра ЛВС обеспечивается при помощи дублирования коммутаторов и канального оборудования. Дополнительное повышение эффективности использования оборудования и скорости передачи данных на уровне ядра ЛВС может быть достигнуто

благодаря применению технологий горячего резервирования активного оборудования и агрегирования каналов ЛВС.

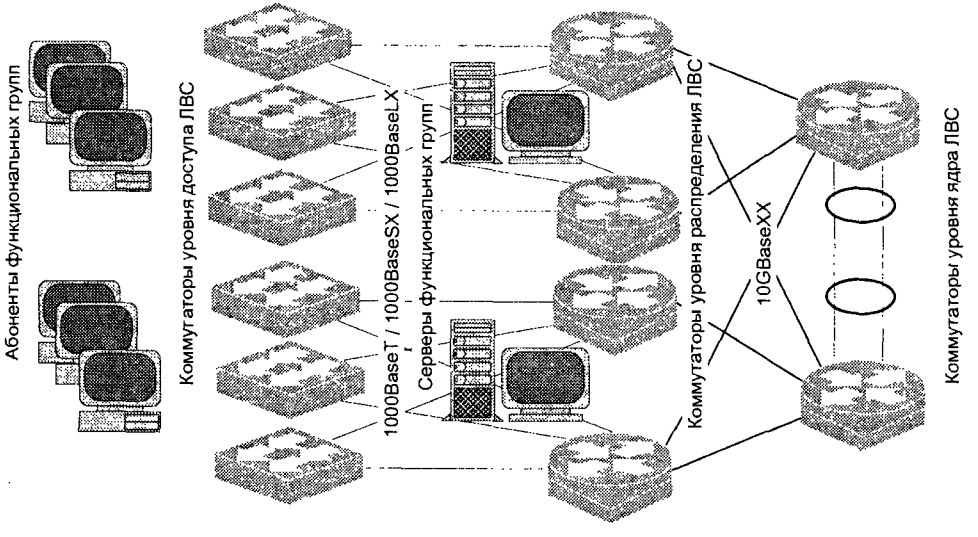


Рис. 13.5. Схема организации связи с использованием коммутаторов уровня ядра иерархической ЛВС

Применение иерархических технологий при построении мультисервисных ЛВС

В настоящее время наиболее распространенными являются локальные сети, которые имеют иерархическую топологию соединения компонентов. Как уже было отмечено, именно такая топология обеспечивает возможность организации надежного и эффективного информационного обмена между абонентами ЛВС.

Разделение всего комплекса оборудования ЛВС на функциональные уровни позволяет применять на каждом из этих уровней специализированные коммутаторы, что в свою очередь, повышает эффективность использования коммуникационного оборудования. Так, например, коммутаторы, которые предназначены для использования на уровне доступа, должны иметь достаточное количество портов для подключения абонентов функциональных групп и магистральные порты для подключения к коммутаторам уровня распределения. Поддержка таких функций, как многоуровневая коммутация или агрегирование каналов для этих коммутаторов, не является обязательной.

В табл. 13.1 приведены обобщенные характеристики коммутаторов каждого из уровней иерархической структуры ЛВС.

Таблица 13.1. Характеристики коммутаторов иерархической структуры ЛВС

Функция/Характеристика	Уровень доступа	Уровень распределения	Уровень ядра
Порты 10/100 Base T	Да	Нет	Нет
Порты 1000 Base XX	Да	Да	Да
Порты 10G Base XX	Нет	Да	Да
Многоуровневая коммутация/маршрутизация	Нет	Да	Да
Управление подключением абонента к порту	Да	Нет	Нет
Списки управления доступом (ACL)	Да	Да	Нет
Агрегирование портов (LACP IEEE 802.3AD)	Да	Да	Да
Виртуальные сети (VLAN IEEE 802.1Q)	Да	Да	Нет
Поддержка качества обслуживания (QoS IEEE 802.1Q)	Да	Да	Да
Многоплановый протокол (MSTP IEEE 802.1S)	Да	Да	Нет
Протокол динамического резервирования VRRP	Нет	Да	Да
Прослушивание сообщений протокола IGMP	Да	Да	Нет

Кольцевые топологии ЛВС

Иерархическая организация, бесспорно, позволяет осуществлять эффективное и надежное управление информационными потоками ЛВС. В то же время сетям с иерархической топологией присущ ряд серьезных недостатков, которые могут существенно ограничить возможность использования этой топологии при построении распределенных мультисервисных сетей. Среди этих недостатков в первую очередь следует выделить:

- высокую стоимость оборудования;
- необходимость применения специальных процедур для реализации горячего резервирования;
- радиальный характер построения сети доступа.

Последний из отмеченных недостатков при построении разветвленных сетей абонентского доступа является наиболее существенным. Дело в том, что при построении таких сетей для передачи данных с узла доступа на оборудование центрального узла, как правило, используется волоконно-оптический кабель. При этом обычно один многожильный волоконно-оптический кабель применяется для подключения нескольких узлов доступа, которые образуют от-

дельную ветвь. Нетрудно заметить, что при увеличении длины этой ветви будет уменьшаться эффективность использования оптического кабеля. В том случае, например, когда ветвь соединяет 4 узла, расстояние между ними, измеренное по кабелю, составляет 500 м, коэффициент полезного использования кабеля (16 волокон) будет равен $(16 \times 500 + 12 \times 500 + 8 \times 500 + 4 \times 500)/16 \times 2000 = 0{,}625$. В том случае, если ветвь будет соединять 8 узлов, то коэффициент полезного использования кабеля снизится до 0,56. Таким образом, при использовании свойственного иерархической топологии радиального построения сети доступа около половины всех волокон оказываются неиспользованными.

Очевидно, что с целью повышения эффективности использования кабеля было бы целесообразно для организации сети доступа применять кольцевое соединение, при котором непосредственно связанными оказываются только ближайшие узлы доступа. Кроме того, кольцевому каналу передач данных изначально свойственна избыточность, поскольку такой канал сочетает в себе как минимум два возможных маршрута передачи данных. Эта избыточность может быть использована для повышения надежности передачи данных.

Применение кольцевых топологий при построении сетей передачи данных имеет достаточно богатую историю. В разные периоды развития сетей передачи данных активно применялись и широко использовались технологии, основанные на кольцевом соединении абонентов. Среди этих технологий, в первую очередь, следует отметить технологии SONET/SDH, FDDI/CDDI и Token Ring. Перспективные комплексы передачи данных по кольцевым структурам, к которым следует отнести RPR/IEEE 802.17, успешно сочетают в себе положительные качества отмеченных выше технологий с последними достижениями в области построения высокопроизводительных сетей с коммутацией пакетов.

Технологии Token Ring/IEEE 802.5

В истории развития технологии Token Ring/IEEE 802.5 много общего с историей возникновения Ethernet. Начало технологии Token Ring/IEEE 802.5 было положено частной компанией — в данном случае это была компания IBM. Для обеспечения дальнейшего развития и промышленного использования данной технологии в институте IEEE был создан специальный комитет, который получил наименование 802.5. В процессе дальнейшего совершенствования технологии комитетом IEEE 802.5 был подготовлен ряд спецификаций, которые определяют основные принципы построения сетей Token Ring (TR) различного назначения. В последних спецификациях комитета IEEE 802.5 наряду с классическим методом маркерного доступа — протоколом *TKP* (Token Passing Protocol), предлагается использовать протокол непосредствен-

ной передачи — *TXI* (Transmit Immediate Protocol), что позволяет существенно повысить скорость информационного обмена.

В табл. 13.2 приведены основные характеристики технологий Token Ring.

Таблица 13.2. *Основные характеристики технологий Token Ring*

Функция/Характеристика	IEEE 802.5	IEEE 802.5t	IEEE 802.5v
Скорость передачи данных (Мбит/сек)	4 или 16	4, 16, 100	4, 16, 100, 1000
Среда передачи данных	UTP	UTP/STP/ MMF	UTP/STP/ MMF/SMF
Метод доступа	TKP	TKP/TXI	TKP/TXI
Логическая топология сети	Кольцо	Кольцо/LL	Кольцо/LL

Организация информационного обмена в сети Token Ring

Управление передачей данных в классической сети Token Ring/IEEE 802.5 выполняется при помощи специального блока данных — маркера (token), циклически перемещаемого по кольцевой среде передачи, которая соединяет все станции ЛВС. Станция, получающая маркер и имеющая информацию для передачи, преобразует маркер в информационный пакет и отправляет его в сеть. Если станция, которая приняла маркер, не имеет информации для передачи, она просто транслирует маркер дальше по сети. Станция-получатель принимает информацию и отправляет кадр далее по сети. Когда переданный блок данных возвращается передающей станции, она отделяет информацию от маркера, после чего движение маркера по сети возобновляется до момента следующей передачи.

На физическом уровне сети Token Ring/IEEE 802.5 построены по схеме "звезда". Все станции в сети подключаются к концентраторам Token Ring через порты, реализующие функцию подключения абонентских станций — *TCU* (Trunk Coupling Unit). Эти порты выполняют последовательную передачу маркера на подключенные станции или другие концентраторы ЛВС, что обеспечивает логическое объединение в единое кольцо всех компонентов сети Token Ring (TR).

Важным положительным качеством сети TR является то, что она обеспечивает возможность использования системы приоритетов, которая позволяет отдельным станциям передавать данные чаще, чем другим. Для обеспечения этого режима в маркере размещается специальное поле, которое содержит информацию о приоритете передаваемых данных. Таким образом, управлять распределением полосы пропускания сети между приложениями в сети TR можно путем изменения приоритета передаваемого маркера.

В сети TR применяются несколько механизмов для того, чтобы обеспечить локализацию и устранение возникающих неисправностей. Одним из таких механизмов является функция активного монитора, которая выполняется одной из выбранных станций ЛВС. Основной задачей этой станции является обнаружение и устранение из кольца тех кадров, которые по какой-либо причине не были удалены их передатчиками. Если активный монитор обнаруживает такой циркулирующий кадр, он должен уничтожить этот кадр и сформировать новый маркер.

Функция обнаружения неисправной станции также предназначена для автоматического устранения неисправностей в сети TR. Эта функция выполняется устройством TCU и позволяет оперативно исключать из кольца станции, которые не могут нормально передавать принимаемый маркер.

Структура кадра TR

В сети Token Ring (TR) используются два типа кадров: информационные кадры, которые применяются для выполнения информационного обмена между компонентами сети, и управляющие кадры, предназначенные для обеспечения этого обмена.

В табл. 13.3 представлена структура информационного кадра Token Ring.

Таблица 13.3. *Структура информационного кадра Token Ring*

Номер поля	Наименование и содержание поля	Длина поля (байт)
1	START DELIMITER — признаки начала кадра	1
2	ACCESS CONTROL — управление доступом к среде передачи данных	1
3	FRAME CONTROL — признак типа кадра	1
4	DESTINATION ADDRESS — адрес станции назначения кадра	6
5	SOURCE ADDRESS — адрес формирователя кадра	6
6	DATA — полезная нагрузка кадра	>0
7	CRC — контрольная сумма	4
8	END DELIMITER — признаки завершения кадра	1
9	FRAME STATUS — состояние обработки кадра	1

Во многом, например, в части форматов адресов и контрольной суммы, структура кадра Token Ring (TR) напоминает структуру кадра Ethernet. Основное отличие между этими структурами состоит в том, что минимальная длина информационного кадра в сети TR не определена, поскольку в сетях

маркерного типа невозможно возникновение коллизий. Максимальная длина кадра TR может превышать аналогичный параметр кадра Ethernet.

Последовательность сигналов, которая размещается в поле START DELIMITER, предназначена для распознавания начала приема информационного или управляющего кадра TR на вход станции. Эта последовательность имеет уникальное кодирование, что позволяет однозначно выделить данную кодировку на фоне обычных информационных сигналов.

Информационный код, который размещается в поле ACCESS CONTROL, указывает на уровень приоритета, соответствующего данному информационному или управляющему кадру. В этом поле размещается также monitor bit, который используется активным монитором для выявления циркулирующих кадров. В этом поле также размещается признак маркера — token bit, позволяющий отличать маркерные кадры от информационных или управляющих кадров.

В поле FRAME CONTROL содержится признак типа кадра. В зависимости от значения этого признака кадр будет признан информационным или управляющим.

Форматы и назначение полей с 4 по 7 кадра TR полностью соответствуют назначению одноименных полей кадра Ethernet.

Кодировка, которая размещается в поле END DELIMITER, указывает на завершение передаваемого кадра. В этом поле также размещаются признак нарушения информационной структуры кадра и порядковый номер кадра в логической последовательности.

Признаки, размещенные в поле FRAME STATUS кадра TR, кодируют информацию об особенностях обработки этого кадра на приемнике данных. Так, например, признак "A" формируется приемником в том случае, если данный кадр был адресован именно ему. В том случае, если приемник выполнил операцию копирования полезной нагрузки кадра в свое запоминающее устройство, в поле FRAME STATUS формируется признак копирования "C" (Copy).

Управляющие кадры выполняют служебные функции в сети TR и обеспечивают поддержание установленной дисциплины информационного обмена. Кадр маркера (Token) представляет собой обычный информационный кадр, который не содержит поле передаваемых данных и поэтому имеет длину 3 байта: START DELIMITER, ACCESS CONTROL, END DELIMITER.

Использование технологии Token Ring при построении ЛВС

Такие специфические особенности технологического комплекса Token Ring/IEEE 802.5, как управление полосой пропускания канала и кольцевое подключение абонентов ЛВС, делают весьма привлекательным применение этой

технологии при построении мультисервисных ЛВС. Однако при выборе окончательных проектных решений следует учитывать, что высокоскоростные варианты Token Ring, например, IEEE 802.5v, в первую очередь ориентированы на подключение абонентов по индивидуальным выделенным линиям — LL (Leased Line), а не через кольцевые структуры. Кроме того, компоненты Ethernet, которые обеспечивают аналогичные характеристики информационного обмена, как правило, имеют существенно более низкую стоимость.

Технология FDDI

Спецификация построения распределенной оптической магистрали — *FDDI* (Fiber Distributed Data Interface) была разработана американским национальным комитетом ANSI в середине 1980-х годов. Эта технология была предназначена для объединения сегментов локальных сетей Ethernet/IEEE 802.3 и Token Ring/IEEE 802.5 с помощью надежных высокоскоростных каналов. После завершения подготовки спецификации FDDI она была представлена в ISO и получила статус международного стандарта.

Спецификация FDDI определяет принципы построения магистрального канала, который обеспечивает передачу данных со скоростью 100 Мбит/сек. Технология FDDI в качестве среды передачи данных использует оптический кабель и обеспечивает информационное взаимодействие между компонентами с применением процедуры маркерного доступа. Основные принципы и технические решения, положенные в основу сети FDDI, во многом напоминают решения и схемы, применяемые в технологии Token Ring/IEEE 802.5. Основное отличие двух этих технологий состоит в том, что для обеспечения большей надежности передачи данных в сети FDDI используются дублированные каналы. Таким образом, в сети, построенной по этой технологии, для передачи данных могут быть применены два информационных кольца — основное (primary ring) и дополнительное (secondary ring).

Еще одно отличие технологии FDDI от классической технологии IEEE 802.5 заключается в типе используемой среды передачи данных. Для обеспечения информационного взаимодействия компонентов в сети FDDI используется одномодовый и многомодовый оптический кабель.

Представление данных в сети FDDI

Для линейного кодирования передаваемых данных в сети FDDI применяется метод, который впоследствии был использован в технологиях 100Base X. В соответствии с принятыми в FDDI правилами кодирования, передаче "1" соответствует изменение фазы сигнала, отсутствие изменения соответствует передаче "0". Для того чтобы обеспечить достаточное для взаимной синхронизации тактовых генераторов передатчика и приемника количество единиц в

выходном коде, в FDDI используется избыточное кодирование по схеме 4B5B. Вследствие того, что только четыре из каждых пяти передаваемых бит обеспечивают передачу данных, частота сигнала, поступающего в линию, должна быть увеличена на четверть. Таким образом, для того чтобы обеспечить скорость передачи данных 100 Мбит/сек, сигнал в линии должен меняться со скоростью 125 МГц (при этом один бит передается за 8 нсек). Из 32 возможных кодировок только 16 используются для передачи данных. Эти кодировки выбраны таким образом, чтобы в символе не встречалось более двух последовательных нулей. Оставшиеся символы либо используются в качестве служебных и управляющих, например, в качестве символов начала и конца кадра FDDI, либо являются запрещенными. Прием запрещенного символа однозначно указывает на наличие ошибки в канале передачи данных.

Структура кадров, используемых для передачи данных по магистрали FDDI, имеет очень много общего со структурой кадра TR, которая была подробно рассмотрена в предыдущем разделе данной главы. По сравнению с кадром TR, у кадра FDDI добавлено одно поле (1) и немного изменен формат двух других (9 и 10). Структура информационного кадра FDDI представлена в табл. 13.4.

Таблица 13.4. *Структура информационного кадра FDDI*

Номер поля	Наименование и содержание поля	Длина поля (байт)
1	PRE — преамбула кадра	>2
2	START DELIMITER — признаки начала кадра	1
3	ACCESS CONTROL — управление доступом к среде передачи данных	1
4	FRAME CONTROL — признак типа кадра	1
5	DESTINATION ADDRESS — адрес станции назначения кадра	6
6	SOURCE ADDRESS — адрес формирователя кадра	6
7	DATA — полезная нагрузка кадра	>0
8	CRC — контрольная сумма	4
9	END DELIMITER — признаки завершения кадра	0,5
10	FRAME STATUS — состояние приема кадра	1,5

Поле PRE имеет длину два или более байтов и предназначено для обеспечения взаимной синхронизации тактовых генераторов передатчика и приемника данных до начала приема информационной части кадра. В данном поле размещаются служебные кодировки типа Idle — все "1".

Кодировка, которая размещается в поле END DELIMITER, указывает на завершение передаваемого кадра. В этом поле размещается служебный символ "T" в том случае, если кадр является полным. Отсутствие этого символа в поле указывает на то, что последовательность, которая размещена в поле DATA данного кадра, не представляет собой завершенный блок данных протокола верхнего уровня.

В поле FRAME STATUS размещаются три индикатора, которые определяют статус передаваемого кадра. Нормальными значениями для данных индикаторов являются кодировки S (Set) или R (Reset). В момент первоначального формирования кадра передатчик формирует индикаторы значением R. В процессе передачи кадра по сети FDDI могут возникнуть проблемы. Для того чтобы указать последующим станциям на эти проблемы, первоначальное содержимое этих полей может быть изменено транслирующими станциями на символ S. Для обозначения проблем используются следующие символы-индикаторы "E", "A" и "C". Индикаторы "A" и "C" в поле FRAME STATUS кадра FDDI имеют такое же значение, как одноименные индикаторы в поле FRAME STATUS кадра TR.

Индикатор "E" — ошибка (Error) устанавливается в том случае, если в процессе приема или ретрансляции кадра была обнаружена ошибка. Например, когда рассчитанное значение контрольной суммы не совпало с передаваемым значением FCS. Если у принятого кадра в поле индикатора E находится любой другой символ кроме R, такой кадр считается ошибочным и не принимается к рассмотрению.

Организация информационного обмена по магистрали FDDI

Поскольку технология FDDI изначально была предназначена для построения надежных магистральных соединений, многие технические решения этой технологии ориентированы на обеспечение надежной передачи данных, автоматическое обнаружение и парирование неисправностей.

Для реализации и обслуживания процесса передачи по магистрали FDDI используются три типа кадров:

- *кадр управления каналом* (MAC-frame);
- *информационный кадр* (LLC-frame);
- *кадр управления станцией* (SMT-frame).

Кадры MAC-типа используются для управления процессом информационного обмена на уровне доступа к среде передачи. В сети FDDI используются два типа кадров данного типа — кадры требования и сигнальные кадры. Примером сигнального кадра FDDI является кадр JAM.

Структура информационного поля кадра LLC полностью соответствует структуре поля DATA кадра IEEE 802.3 (SAP). Единственное отличие заклю-

чается в том, что общая длина информационного поля у кадра FDDI составляет 4473 байтов.

Кадры SMT используются на магистрали FDDI для реализации функции управления станцией (Station Management). Эта функция обеспечивает взаимодействие компонентов сети, обнаружение и устранение нарушений информационного взаимодействия, сбор статистики и т. д. Кадр SMT, который размещается в поле данных кадра FDDI, состоит из двух компонентов: заголовка (SMT Hdr.) и информационной части (SMT Info). Эти две части в совокупности образуют блок данных канального уровня кадра SMT.

Технология FDDI обеспечивает независимую передачу по информационной магистрали двух типов трафика:

- синхронного трафика;
- асинхронного трафика.

Синхронный трафик образуют такие приложения, для которых критичным является наличие временной задержки при передаче данных — передача голоса или видеоинформации. Остальные данные, которые передаются по сети, образуют асинхронный трафик. Для обеспечения гарантированных значений задержки при передаче данных, которые относятся к синхронному трафику, в сети FDDI используется резервирование полосы пропускания канала в сочетании с применением механизма приоритетов.

Обеспечение устойчивости к отказам компонентов сети FDDI

Для обнаружения неисправностей и автоматического изменения конфигурации сети при возникновении отказов на магистрали FDDI применяется ряд специальных механизмов и технических решений.

Вспомогательное кольцо является одним из решений, которые обеспечивают устойчивость к отказам сети FDDI. На рис. 13.6, *а* представлен вариант первоначальной структуры информационной магистрали, связывающей четыре группы абонентов. Коммутаторы доступа FDDI на этом рисунке представлены в виде пронумерованных квадратов. При отказе канала, который связывал коммутаторы доступа FDDI 1 и 4, происходит автоматическое изменение первоначальной структуры сети.

Коммутаторы 1 и 4, которые зафиксировали неисправность, соединяют на своих интерфейсах основное и дополнительное кольцо FDDI (см. рис. 13.6, *б*). Кольцо меняет конфигурацию — становится одинарным, однако при этом связность системы в целом не нарушается. Примерно таким же образом производится изменение конфигурации системы при отказе одного из коммутаторов доступа FDDI.

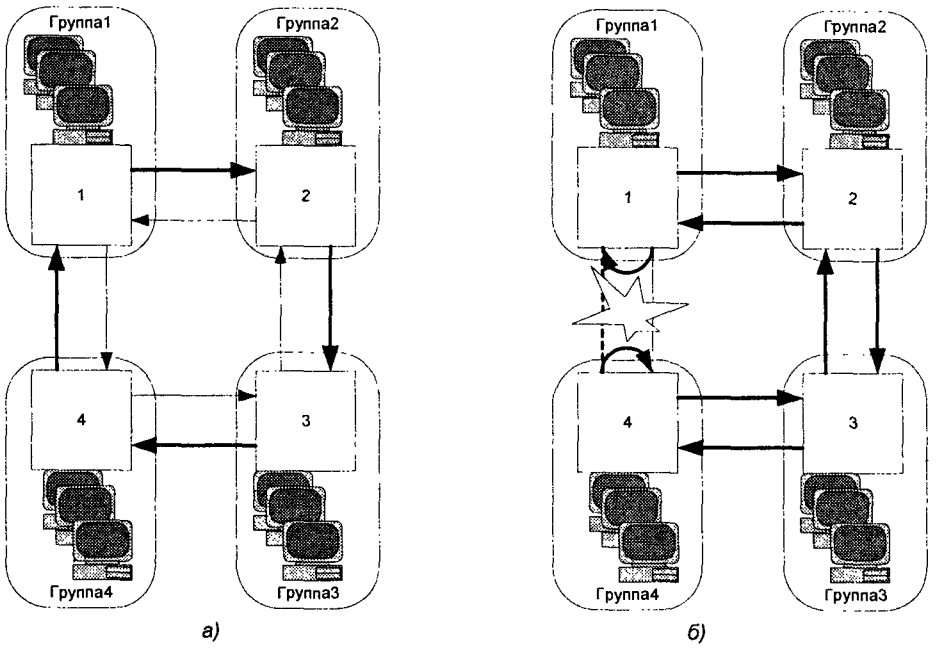


Рис. 13.6. Изменение конфигурации информационной магистрали FDDI при отказе канала

Для обеспечения возможности автоматической реконфигурации системы применяются специальные алгоритмы управления соединением на физическом уровне FDDI. Так, например, каждая станция в сети FDDI выполняет процедуру управления физическим соединением — *FDDI-PCM* (FDDI — Physical Connection Management). Эта процедура выполняется на каждом порту, который используется для подключения абонентского устройства к сети FDDI.

Для каждого подключения выполняется комплекс предварительных процедур PCM, которые в реальном масштабе времени обеспечивают:

- определение совместимости типов подключенных портов;
- определение качества физического контакта.

Для определения качества физического контакта применяется процедура *LCT* (Link Confidence Test). Продолжительность выполнения LCT определяется перед началом выполнения проверки и может в зависимости от качества соединения составлять от 50 мсек до 50 сек. В ходе выполнения проверки станции обмениваются установленными кодировками и проверяют качество принятого сигнала. Только в том случае, если качество контакта отвечает предъявляемым требованиям, соединение считается установленным. После установления соединения соответствующие порты включаются в маршрут

перемещения маркера по сети FDDI (token path) и начинают использоваться для передачи данных.

Применение технологий FDDI при построении ЛВС

Относительно высокая стоимость компонентов FDDI является фактором, который сдерживает ее более широкое внедрение в локальные сети пользователей. В то же время практически повсеместно для передачи данных в этих локальных сетях используются экранированные и неэкранированные медные пары, которые также способны обеспечивать передачу данных со скоростью до 100 Мбит/сек.

Поэтому в 1990 году в ANSI был образован комитет, который в 1994 году подготовил спецификацию, обеспечившую функционирование протоколов канального уровня FDDI при использовании в качестве среды передачи данных кабелей с неэкранированными витыми парами категории 5 или экранированными витыми парами. Однако дальнейшее развитие комплекса технологий Ethernet, в частности появление спецификаций 1000Base X и 10GBASE X, привело к существенному повышению требований, которые предъявляются к пропускной способности магистральных соединений ЛВС. Относительно небольшая, по современным меркам, скорость передачи данных и высокая стоимость компонентов существенно снижают возможность использования технологий FDDI и CDDI в современных мультисервисных ЛВС.

Магистральные технологии второго поколения

Технологиям передачи данных в кольцевых сетях, которые были рассмотрены в предыдущих разделах, свойственен ряд существенных недостатков, главным из которых является недостаточная пропускная способность. Вместе с тем нельзя не отметить, что кольцевая топология среды передачи данных практически идеально подходит для организации распределенных сетей доступа.

При разработке этих технологий основные изменения были направлены на увеличение реальной пропускной способности кольцевой среды передачи данных, а также повышение надежности и устойчивости к отказам кольцевой магистрали. Главные отличия этих технологий от кольцевых технологий первого поколения состоят в том, что при их реализации выполняются:

- отказ от маркерного принципа управления процессом передачи данных;
- извлечение из кольца принятого кадра данных;
- введение ограничения времени существования кадра в кольце;
- введение процедуры обеспечения качества обслуживания.

Кольцевые пакетные технологии Cisco Systems

Один из первых протоколов второго поколения, обеспечивающий передачу данных в пакетных сетях по кольцевым магистралям, был разработан специалистами компании Cisco Systems (IETF RFC: 2892 "The Cisco SRP MAC Layer Protocol" August 2000 Category — Informational). Этот протокол определяет основные принципы управления передачей данных в пакетном формате через распределенное кольцевое магистральное соединение — протокол *SRP* (Spatial Reuse Protocol). Общая схема построения такого магистрального соединения SRP приведена на рис. 13.7. Квадратами на этой схеме обозначены устройства доступа к магистрали SRP. Каждое из таких устройств имеет непосредственное соединение с парой соседних магистральных устройств. В схеме, представленной на рис. 13.7, восточным соседом устройства доступа 1 является устройство доступа 2, а западным соседом устройства доступа 1 является устройство доступа 0. Для организации каждого из таких соединений используются два волокна волоконно-оптического кабеля — одно для передачи данных непосредственному соседу, другое для приема данных, которые этот сосед передает по магистрали.

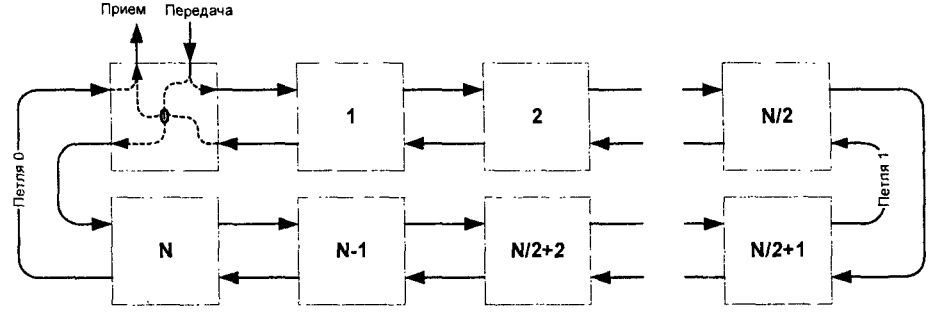


Рис. 13.7. Схема построения магистрального соединения SRP

Таким образом, все устройства доступа SRP оказываются соединенными двумя кольцевыми магистралями, которые принято именовать петлями (SRP Ringlet). Магистральная петля, в которой данные передаются по часовой стрелке, имеет номер 0 (SRP Ringlet0), петля, по которой данные передаются во встречном направлении, имеет номер 1(SRP Ringlet1). Для передачи данных по магистрали SRP используются кадры специального формата. Заголовок кадра содержит адрес станции назначения для данного кадра и адрес станции, которая сформировала данный кадр. Устройство доступа к магистрали SRP анализирует заголовки каждого кадра, принимаемого от восточного и западного соседа. В том случае, если адрес назначения кадра совпадает с MAC-адресом одной из подключенных к данному устройству абонентских станций, кадр передается на внутренний приемный интерфейс. Все остальные

кадры, принятые от восточного соседа, передаются западному соседу, и, наоборот, кадры, принятые от западного соседа, передаются восточному.

Исключение составляют кадры, сформированные теми абонентскими станциями, которые непосредственно подключены к данному устройству доступа. Кадры, формируемые данными станциями, устройство доступа отправляет своим непосредственным соседям через магистральные соединения. Когда эти кадры, пройдя полную петлю, возвращаются на то устройство доступа, с которого они были впервые переданы в магистраль, они должны быть уничтожены. Следовательно, общая магистраль SRP оказывается разделенной на сегменты, в пределах которых могут быть организованы независимые информационные потоки. На рис. 13.8 приведена схема информационного взаимодействия между двумя парами (группами) абонентов, связанных кольцевой пакетной магистралью SRP.

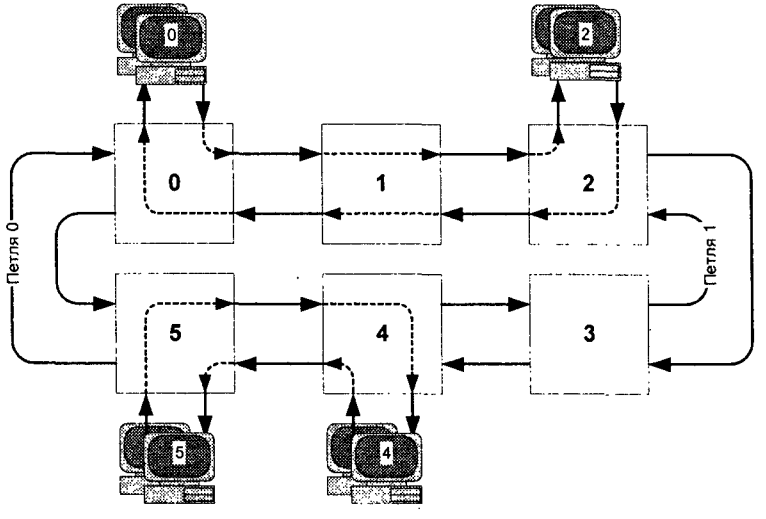


Рис. 13.8. Схема взаимодействия между группами абонентов, связанных магистралью SRP

В данном случае передача данных между группами абонентов 0 и 2 выполняется по маршруту, который не проходит через устройства доступа 5 и 4. Поэтому для информационного обмена между обеими парами взаимодействующих групп может быть использована полная пропускная способность магистрали SRP.

Примечание

Очевидно, именно эта особенность информационного обмена на кольцевой магистрали определила название протокола SRP. Сочетание "Spatial Reuse" означает возможность повторного использования транспортного объема магистрали.

Гарантированное исключение кадров, которые прошли полный цикл передачи по магистрали, достигается благодаря ограничению общего времени передачи кадра в петле. Для этого каждый кадр снабжается меткой, определяющей длину пройденного им пути. Значение этой метки модифицируется каждый раз, когда кадр транслируется через очередное устройство доступа. В том случае, если длина пути, пройденного кадром, превысит максимальное значение, которое установлено для данной магистрали, этот кадр также подлежит уничтожению.

Описанные выше процедуры и технические решения повышают эффективность использования пропускной способности и исключают возможность бесконечной циркуляции кадров в петлях магистрали без применения маркерного доступа, что позволяет отнести SRP ко второму поколению протоколов организации кольцевых магистральных соединений в пакетных сетях.

Технология IEEE 802.17 (RPR)

Описанные выше принципы организации резервированного магистрального соединения SRP получили дальнейшее развитие при разработке технологического комплекса построения кольцевых пакетных магистралей — *RPR* (Resilient Packet Ring). Комплекс протоколов RRP включает в себя одноименные технологии, одна из которых была подготовлена комитетом IEEE 802.17 "Resilient packet ring (RPR) access method and physical layer specifications", а другая — специалистами Cisco Systems, для применения в магистральных маршрутизаторах.

Технологии RPR позволяют организовать надежные высокоскоростные кольцевые пакетные магистрали, которые обладают следующими характеристиками:

- *возможностью использования всех режимов информационного обмена при передаче блоков данных канального уровня.* Для адресации абонентов кольцевой магистрали могут применяться адресные диапазоны Unicast, Multicast и Broadcast;
- *обеспечением нескольких уровней качества обслуживания для групп трафика, передаваемого по кольцевой магистрали.* Так, в частности, уровень обслуживания по типу Class A в дополнение к гарантиям размера пропускной способности обеспечивает заданный диапазон изменения задержки распространения сигнала в магистрали. Этот уровень может быть использован для передачи трафика, чувствительного к временным задержкам, например VoIP. Обслуживание по типу Class C может быть использовано для управления передачей обычного трафика ЛВС, поскольку для этого типа трафика обычно не требуется нормированных характеристик. Обслуживание по классу Class B может быть использовано для всех проме-

жуточных категорий трафика, например, для передачи сжатых видеопотоков;

- *повышением эффективности использования пропускной способности кольцевой магистрали.* Это свойство обеспечивается автоматическим удалением из кольцевой магистрали пакетов невостребованного трафика, перераспределением неиспользуемого ресурса пропускной способности кольцевой магистрали между активными информационными потоками;
- *равными возможностями доступа к ресурсам для всех абонентов, подключенных к магистрали RPR. Автоматическим определением кратчайшего маршрута между устройствами доступа по кольцевой магистрали;*
- *автоматическим диагностированием магистральных каналов, обнаружением отказов и изменением топологии магистрали для их устранения.* Время автоматического восстановления работоспособности кольцевой магистрали после обнаружения отказа при этом не будет превышать 50 мсек;
- *применением разветвленной системы управления трафиком для предотвращения потерь пакетов при перегрузках на кольцевой магистрали;*

Для управления передачей данных по магистрали RPR применяются несколько типов кадров:

- *информационные кадры* (RPR Data Frame) используются для непосредственной передачи данных по кольцевой магистрали;
- *управляющие кадры* (RPR Control Frame) используются для диагностирования каналов передачи данных и общего управления передачей данных по кольцевой магистрали;
- *выравнивающие кадры* (RPR Fairness Frame) применяются для динамического перераспределения ресурсов пропускной способности информационной магистрали RPR между активными абонентами;
- *технологические кадры* (RPR Idle Frame) обеспечивают взаимную синхронизацию тактовых генераторов абонентов RPR при отсутствии информационных кадров.

Структура информационного кадра RPR представлена в табл. 13.5.

Таблица 13.5. *Структура информационного кадра RPR*

Номе поля	Наименование и содержание поля	Длина поля (байт)
1	TTL — время жизни кадра	1
2	BASE.CONTROL — признаки базового управления	1
3	DA — адрес станции назначения кадра	6

Таблица 13.5 (окончание)

Номе поля	Наименование и содержание поля	Длина поля (байт)
4	SA — адрес формирователя кадра	6
5	TTL.BASE — исходное значение времени жизни данного кадра	1
6	EXTENDED.CONTROL — признаки расширенного управления	1
7	HEC — контрольная сумма заголовка кадра	2
8	PROTOCOL.TYPE — тип или длина полезной нагрузки кадра	2
9	SERVICE.DATA.UNIT — полезная нагрузка кадра	>0
10	FCS — контрольная сумма кадра	4

В поле TTL (Time To Live) кадра RPR помещается значение времени жизни данного кадра. Это значение соответствует максимальной длине маршрута, который может пройти кадр по кольцевой магистрали. В процессе трансляции кадра по кольцевой магистрали это значение уменьшается на единицу при каждой последовательной передаче кадра через устройство доступа.

Поле BASE.CONTROL используется для размещения признаков, управляющих процессом передачи кадра по магистрали RPR. В этом поле, в частности, размещаются следующие признаки:

- идентификатор петли, в которую данный кадр был передан источником — RI (Ringlet Identifier);
- разрешение выполнения процедуры выравнивания для данного кадра — FE (Fairness Eligible);
- тип класса обслуживания, который был установлен для данного кадра — SC (Service Class);
- тип кадра — FT (Frame Type) — определяет принадлежность данного кадра к одной из четырех групп кадров RPR.

Поля адреса назначения кадра DA (Destination Address) и источника кадра SA (Source Address) имеют в кадре RPR такое же значение и кодирование, как и в кадре любой другой технологии канального уровня, например, Ethernet.

Поле TTL.BASE предназначено для размещения неизменяемого исходного значения времени жизни, которое было установлено при формировании данного кадра.

Поле EXTENDED.CONTROL используется для размещения признаков, управляющих процессом передачи кадра по магистрали RPR в расширенном режиме.

В поле HEC (Header Error Check) помещается контрольная сумма заголовка кадра RPR.

Поле PROTOCOL.TYPE используется для указания типа или длины полезной нагрузки данного кадра. Значение, большее чем 1 536, размещенное в данном поле, будет интерпретировано, как указание типа протокола. Значения, меньшие чем 1 536, используются для указания длины полезной нагрузки.

Поле SERVICE.DATA.UNIT имеет переменную длину и предназначено для размещения полезной нагрузки кадра RPR.

В поле FCS (Frame Check Sequence) помещается контрольная сумма кадра. Суммирование в данном случае выполняется с поля HEC до конца полезной нагрузки кадра.

Использование гибридных технологий для построения мультисервисных ЛВС

Технологии, описанные в предыдущих разделах данной главы, могут быть с разным успехом использованы при построении мультисервисных ЛВС. Вряд ли можно считать целесообразным, например, применение шинной топологии при построении распределенной мультисервисной ЛВС. В то же время, построение мультисервисной ЛВС с кольцевой топологией выглядит гораздо более обоснованным. Однако применение "штатных" кольцевых технологий может существенно повысить стоимость реализации проекта. Модули RPR, например, которые обеспечивают передачу данных на скорости в несколько гигабит в секунду, имеют стоимость, почти на порядок превышающую стоимость аналогичных интерфейсов Ethernet/IEEE802.3. В подобной ситуации могут быть использованы гибридные решения, которые обеспечивают достижения требуемых технических характеристик в условиях финансовых ограничений.

Соединение абонентов по схеме "Ромашка"

На рис. 13.9 приведен пример использования гибридных технологий при построении мультисервисной ЛВС. Топология, представленная на данном рисунке, обеспечивает построение распределенных сетей доступа на основе технологии Ethernet и имеет неофициальное наименование "Ромашка".

Подключение коммутаторов в данном случае выполняется по иерархически-кольцевой схеме, когда к одному коммутатору уровня распределения могут быть подключены несколько колец коммутаторов уровня доступа. Применение многопланового протокола Spanning Tree (MSTP) позволит повысить эффективность использования каналов передачи данных.

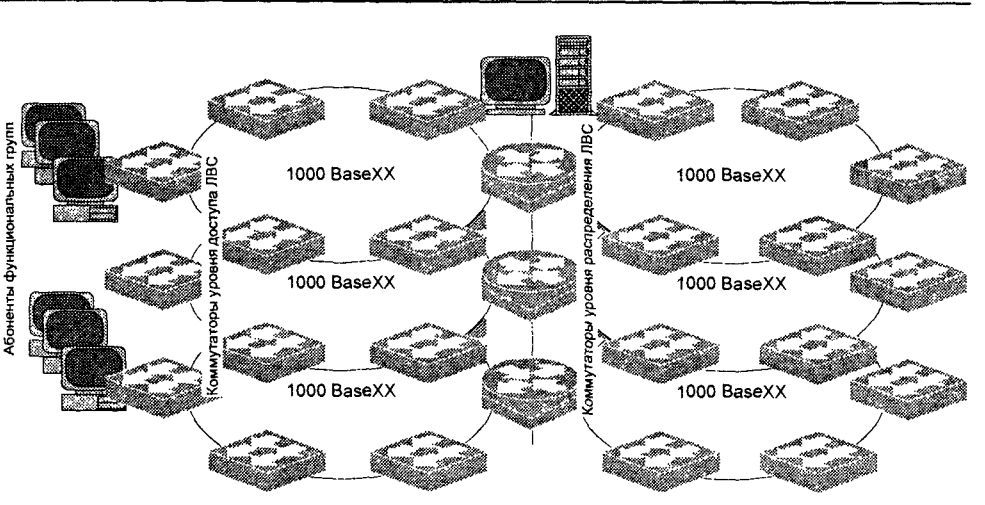


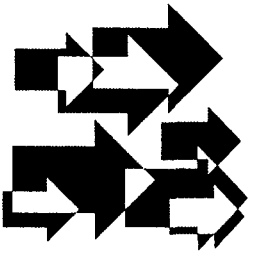
Рис. 13.9. Применение гибридных технологий при построении мультисервисной ЛВС

Рекомендации по выбору схемы построения ЛВС

При выборе той или иной структуры при построении ЛВС, наряду с особенностями применяемых технологий, следует тщательно учитывать особенности организации информационного обмена в проектируемой системе. Так, например, для эффективной реализации ЛВС, схема которой представлена на рис. 13.9, необходимо использование коммутаторов, поддерживающих протокол MSTP. Если данная ЛВС будет применяться для организации группового обмена, то в дополнение к этому на коммутаторах должна быть обеспечена поддержка протокола IGMP.

Некорректное применение технологии передачи данных или неправильный выбор топологии построения особенно сильно сказываются на характеристиках именно мультисервисных ЛВС, которым свойственны высокие требования к основным характеристикам сети.

ГЛАВА 14



Построение магистральных соединений мультисервисных ЛВС

Магистральные соединения предназначены для обеспечения высокоскоростной передачи данных между узлами мультисервисных сетей. Как уже было неоднократно отмечено, именно в мультисервисных ЛВС вопросам построения эффективных магистральных соединений придается очень большое значение. Во многом это связано с тем, что характерными признаками мультисервисных сетей являются большие объемы передаваемых данных и высокие требования к скорости и надежности их доставки.

Далее перечислены некоторые из наиболее существенных требований, которые предъявляются к характеристикам магистральных соединений современных мультисервисных ЛВС:

- скорость информационного обмена — 10^9—10^{10} бит/сек;
- достоверность и надежность: вероятность возникновения отказа в процессе передачи данных по магистральному соединению — 10^{-9}—10^{-12};
- автоматическая диагностика возникающих неисправностей.

В комплекс спецификаций IEEE 802.3 входят описания двух групп технологий, характеристики которых удовлетворяют большинству из перечисленных только что требований:

- группа технологий 1000 Base (Gigabit Ethernet);
- группа технологий 10G Base (10Gigabit Ethernet).

Первый раздел настоящей главы посвящен рассмотрению общих принципов и технологий построения магистральных соединений Gigabit Ethernet. В этом разделе представлены технологии 1000Base-SX, 1000Base-LX, 1000Base-CX и 1000Base-T.

Во втором разделе рассмотрены особенности организации высокоскоростных магистралей 10Gigabit Ethernet. В этом разделе рассматриваются общие прин-

ципы и особенности применения технологий 10GBase-X, 10GBase-R и 10GBase-W для построения магистральных соединений мультисервисных ЛВС.

Технологии Gigabit Ethernet

Для удобства описания протоколов информационного обмена в спецификации IEEE 802.3 применяется система, которая предполагает разбиение канального уровня информационного взаимодействия на несколько дополнительных уровней. Так же, как это принято в модели OSI ISO 7498, каждый из таких уровней выполняет строго определенные функции, что позволяет использовать при построении программного обеспечения универсальные функциональные блоки. Так, например, при описании спецификаций 1000Base X физический уровень информационного взаимодействия OSI ISO 7498 разделяется на несколько дополнительных уровней и интерфейсов:

- интерфейс, независимый от среды передачи данных — *интерфейс MII* (Media Independent Interface). Задачей этого интерфейса является обеспечение взаимодействия магистрального компонента с универсальными блоками канального уровня OSI. В свою очередь, интерфейсы MII являются общими и универсальными для нескольких разновидностей одной из магистральных технологий Ethernet;
- уровень физического кодирования — *уровень PCS* (Physical Coding Sub). На данном уровне обычно выполняются операции по преобразованию передаваемого и принимаемого кодов в соответствии с требованиями, которые определяются характеристиками среды передачи данных;
- уровень подключения к физической среде — *уровень PMA* (Physical Medium Attachment). На этом уровне обычно определяются основные требования к значениям характеристик используемой среды передачи данных и параметрам приемопередающих компонентов;
- уровень физической среды — *уровень PMD* (Physical Medium Dependent);
- интерфейс, определяемый средой передачи данных — *интерфейс MDI* (Medium Dependent Interface).

Алгоритмы обработки данных, реализуемые на этих уровнях и интерфейсах, могут быть универсальными для нескольких спецификаций. В некоторых случаях эти протоколы могут быть уникальными и предназначенными для использования только в одной технологии.

Магистрали Gigabit Ethernet обеспечивают передачу данных со скоростью 10^9 бит/сек и могут быть построены на основе различных типов кабеля (среды передачи данных). В табл. 14.1 показаны базовые характеристики технологий Gigabit Ethernet, представленных в спецификации IEEE 802.3/Ethernet.

Таблица 14.1. Базовые характеристики технологий Gigabit Ethernet

Наименование технологии	Среда передачи данных	PCS
1000Base-SX	Многомодовое оптическое волокно	8B/10B
1000Base-LX	Одномодовое или многомодовое оптическое волокно	8B/10B
1000Base-CX	Две специально подготовленные пары кабеля STP	8B/10B
1000Base-T	Четыре пары кабеля UTP категории 5	PAM-5

В описании магистральных технологий Gigabit Ethernet можно выделить две частично независимые группы спецификаций:

- 1000Base X;
- 1000Base T.

При создании группы спецификаций 1000Base X дальнейшее развитие получили общие принципы, в соответствии с которыми построено подавляющее большинство спецификаций Ethernet. Спецификация 1000Base T представляет собой комплекс технических решений, обеспечивающих передачу данных на скорости 1000 Мбит/сек по UTP категории 5.

Спецификации 1000Base X

Спецификации 1000Base X включают в себя группу технологий, которые могут быть использованы для построения магистральных соединений, обеспечивающих передачу данных со скоростью 1000 Мбит/сек по медному и волоконно-оптическому кабелю. В состав данной группы входят такие технологии, как 1000Base-SX, 1000Base-LX и 1000Base-CX.

Особенности организации информационного обмена 1000Base X

Применение технологий 1000Base X обеспечивает:

- обеспечение совместимости на уровне управления каналом CSMA/CD MAC;
- возможность применения регенераторов 1000 Мбит/сек;
- реализацию процедуры Auto-Negotiation (без применения FLP);
- скорость передачи данных 1000 Мбит/сек на уровне Gigabit MII (GMII);
- возможность использования в качестве среды передачи специально сбалансированного медного кабеля (150 Ом) или стандартных волоконно-оптических кабелей.

Примечание

Более подробно назначение и особенности использования процедуры Auto-Negotiation описаны в *главе 15* настоящего издания.

Специфика организации информационного обмена с использованием протоколов 1000Base X определяется применением схемы кодирования 8B/10B на уровне PCS.

Схема модуляции 8B10B является логическим продолжением алгоритма линейного кодирования 4B5B, который был использован в технологиях 100Base T(X). При использовании алгоритма линейного кодирования максимальное число кодировок, которые предназначены для передачи данных, меньше, чем общее число возможных кодировок. Наличие такого запаса позволяет выбрать информационные кодировки таким образом, чтобы обеспечить возможность взаимной синхронизации генераторов и, кроме того, обеспечить выполнение некоторых дополнительных условий, которые являются специфическими для используемой среды передачи данных. В случае 1000Base X таким требованием является необходимость обеспечения постоянства среднего уровня формируемого сигнала — для поддержания температурного режима излучателя.

Следует отметить, что использование схемы 8B10B, в первую очередь, было вызвано необходимостью обеспечения достаточного для устойчивой синхронизации тактового генератора приемника количества изменений передаваемого сигнала. Это требование в спецификациях 1000Base X реализуется за счет сокращения количества разрешенных к передаче кодовых комбинаций, что в свою очередь влечет за собой увеличение размера передаваемого символа. Кодирование передаваемого байта десятиразрядным символом обладает достаточным уровнем избыточности для того, чтобы обеспечить выбор необходимого количества разрешенных комбинаций передаваемого кода. Разрешенными считаются кодовые комбинации 8B/10B, каждая из которых имеет как минимум троекратное изменение сигнала. Так, например, комбинации 000010 0001 и 0001100 0000 не могут быть признаны разрешенными и не могут быть использованы для передачи данных с кодированием 8B/10B. В отличие от ранее приведенных кодовых комбинаций, такие комбинации, как 100111 0100 и 011101 0100, считаются разрешенными и применяются для передачи данных — комбинации "D0.0-" и "D0.1-" соответственно.

Применение избыточного кодирования 8B/10B не только обеспечивает устойчивую взаимную синхронизацию тактовых генераторов передатчика и приемника сигнала, но и позволяет реализовать оперативный контроль корректности принимаемого кода, а также возможность использования служебных комбинаций для управления процессом информационного обмена. Из общего количества 1024 различных комбинаций, которые могут быть пред-

ставлены десятиразрядным кодом, только 256 разрешенных комбинаций применяются для передачи данных, и еще несколько комбинаций применяются для управления процессом передачи данных. Остальные кодовые комбинации являются запрещенными и не используются в процессах информационного обмена 1000Base X.

Примечание

Информационная скорость 1000 Мбит/сек в данном случае может быть достигнута за счет увеличения до 1250 Мбит/сек частоты сигнала, передаваемого в линию.

Для обозначения кодовых комбинаций в технологическом комплексе 1000Base X применяется специальная система, в соответствии с которой каждый байт передаваемых данных представляется кодовой группой, которая разбита на две части: старшую — 3 бита и младшую — 5 бит. Принадлежность кодовой группы определяется первым символом имени этой группы:

- "D" — применяется для обозначения кодовых групп, которые используются для непосредственной передачи данных;
- "K" — применяется для обозначения кодовых групп, которые используются для управления процессом передачи данных.

Два последующих числа, разделенные точкой, определяют кодовое содержание группы, например имя "D10.0" используется для обозначения кода 000 01010.

Как уже было отмечено ранее, преобразование байтовых кодовых групп в десятибитные последовательности кода 8B/10B выполняется по специальным правилам, с тем, чтобы обеспечить требуемое соотношение нулей и единиц в результирующей десятиразрядной группе. Соответствие исходной восьмиразрядной кодовой группы и результирующего кода 8B/10B задано в спецификации 1000Base X в табличном виде. При этом результирующее десятиразрядное кодовое слово разбивается на два компонента:

- первое кодовое слово 8B/10B — биты "a b c d e i";
- второе кодовое слово 8B/10B — биты "f g h j".

Управляющие кодовые группы 8B/10B применяются для осуществления контроля над процессом информационного обмена между абонентами 1000Base X.

В табл. 14.2 приведены коды управляющих групп, которые используются в технологиях 1000Base X.

Управляющие кодовые группы IDLE 1 и IDLE 2 передаются в паузах между информационными кадрами и предназначены для обеспечения устойчивой

взаимной синхронизации тактовых генераторов передатчика и приемника данных при отсутствии информационного обмена между ними.

Таблица 14.2. *Коды управляющих групп, используемых в технологиях 1000Base X*

Имя	Назначение кода	Имена кодовых групп	Код первого слова 8B/10B	Код второго слова 8B/10B
I1	Незанятая линия IDLE 1	K28.5+D5.6	001111 1010	101001 0110
I2	Незанятая линия IDLE 2	K28.5+D16.2	001111 1010	011011 0101
R	Расширение кадровой группы	K23.7	111010 1000	
S	Разделитель начала кадра SPD	K27.7	110110 1000	
T	Разделитель конца кадра EPD	K29.7	101110 1000	
V	Сообщение об ошибке	K30.7	011110 1000	

Управляющие кодовые группы начала пакета — SPD (Start of Packet Delimiter) и конца пакета — EPD (End of Packet Delimiter) предназначены для указания начала и конца кадра, соответственно, в передаваемом информационном потоке.

Основное назначение кодовой группы расширения передаваемого кадра (Carrier_Extend) состоит во взаимном разделении нескольких последовательно передаваемых кадров, которые образуют единую группу (burst). В этом случае одна или две кодовых группы "R" используются также для обозначения начала и конца передаваемой кадровой группы.

Управляющие кодовые группы Error_Propagation применяются для сигнализации об ошибке, которая была зафиксирована в процессе передачи данных. Получение данной управляющей группы так же, как и прием неразрешенного кодового слова от удаленного абонента, свидетельствует о нарушении нормального процесса передачи данных, следствием которого должно стать формирование приемником сообщения об ошибке для объекта последующего уровня для аннулирования принятых данных.

Контроль паритета передаваемого кода

В дополнение к описанным ранее правилам формирования кодов, в спецификации 1000Base X для выравнивания характеристик передаваемых символов и проверки корректности принимаемых кодовых слов, используются специальные правила управления и контроля паритета (Parity) количества нулей и единиц в кодовых посылках 8B/10B. В соответствии с этими правилами по-

нятие текущего значения паритета формируемых кодов определяется следующим образом:

- кодовая группа, в которой содержится больше нулей, чем единиц, обладает отрицательным значением кодового паритета;
- кодовая группа, в которой содержится больше единиц, чем нулей, обладает положительным значением кодового паритета;
- кодовая группа, которая содержит одинаковое количество единиц и нулей, обладает нулевым значением кодового паритета.

Примечание

Приведенное ранее правило не распространяется на специфические кодовые группы 000111, 111000, 1100 и 0011. Кодовый паритет таких групп считается отрицательным в том случае, если такая группа заканчивается на "0", и положительным — в противном случае.

Эти дополнительные правила позволяют передатчику выравнивать среднее количество "0" и "1" в формируемых им кодовых группах. Спецификация 1000Base X предусматривает возможность использования двух альтернативных кодовых групп 8B/10B для кодирования каждого байта передаваемых данных в зависимости от текущего значения кодового приоритета. Для обеспечения однозначного определения начального уровня паритета после включения питания, он всегда считается отрицательным.

На рис. 14.1 приведены примеры вычисления кодового паритета при формировании кодовых групп 8B/10B.

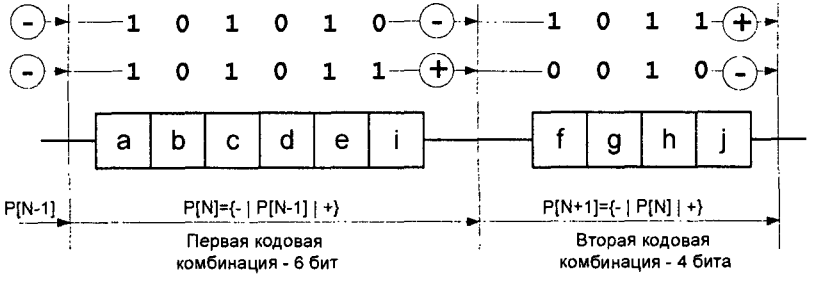


Рис. 14.1. Примеры вычисления кодового паритета при формировании кодовых групп 8B/10B

Верхний вариант значения первой кодовой группы имеет нулевой паритет, и поэтому кодовый паритет линии после передачи этой группы сохраняет свое исходное значение, в данном случае — отрицательное. Поскольку вторая комбинация верхней группы имеет положительный паритет, ее передача вызывает изменение общего паритета линии. Нижние значения первой и второй

кодовых групп приведены для иллюстрации другого сценария изменения паритета.

Очевидно, что представленные ранее правила вычисления паритета позволяют реализовать диагностику возникновения однократной ошибки при передаче кода. Признаком обнаружения ошибки в данном случае могут быть как прием недопустимой кодовой комбинации, так и нарушение паритета при ее передаче. В первом случае ошибка будет обнаружена немедленно, во втором — после приема следующей кодовой группы, которая будет ошибочно отклонена приемником из-за рассогласования его текущего паритета по отношению к передатчику кода.

Оптические варианты PMD 1000Base X

В спецификации 1000Base X определены два варианта протоколов подключения к *среде передачи данных — PMA* (Physical Medium Attachment):

- протокол 1000Base SX;
- протокол 1000Base LX.

Каждый из этих протоколов ориентирован на использование специфической *физической среды — PMD* (Physical Medium Dependent), которой в данном случае являлся волоконно-оптический кабель. Для организации одного оптического сегмента 1000Base X в ЛВС обычно применяются два волокна кабеля — по одному для приема и передачи оптического сигнала, при этом передающее волокно ближнего абонента ЛВС является приемным волокном для дальнего абонента. Спецификация 1000Base X устанавливает совокупность условий, которым должно удовлетворять установленное оптическое соединение для формирования признака начала приема — SIGNAL_DETECT:

- уровень принимаемого сигнала превышает минимально допустимый (минус 30dBm);
- зафиксирован прием допустимых кодовых групп от удаленного абонента.

При несоблюдении любого из данных условий оптическая линия признается неисправной и формируется признак "SIGNAL_DETECT = FAIL".

Спецификация 1000Base SX предполагает использование в качестве среды передачи данных сегментов многомодового волоконно-оптического кабеля с диаметром волокна 50 или 62,5 мкм. В качестве источников сигнала (передатчиков) в данной технологии обычно используются коротковолновые (Short-Wave) полупроводниковые лазеры или светодиоды — *LED* (Light Emission Diode) — с длиной волны 850 нм. Передатчики этого частотного диапазона достаточно просты в изготовлении, имеют относительно низкую стоимость, поэтому именно они применяются для воспроизведения записей бытовых компакт-дисков.

Многомодовые волоконно-оптические кабели также дешевле в изготовлении, чем одномодовые, и таким образом, совокупные затраты на построение сети 1000Base SX являются относительно небольшими. Недостатком данной технологии является не очень большая длина распространения сигнала по кабелю, которая определяется относительно высоким уровнем затухания этого сигнала в многомодовом оптическом кабеле.

Спецификация 1000Base LX обеспечивает возможность использования в качестве среды передачи данных одномодовых оптических волокон диаметром 8—10 мкм, допускается также возможность использования в данной технологии и многомодового кабеля.

Формирование сигнала в 1000Base LX осуществляется длинноволновыми (Long-Wave) лазерами, длина волны оптического излучения которых составляет около 1500 нм. Для передачи оптического сигнала этих лазеров могут быть использованы как многомодовые, так и одномодовые оптические кабели. Одномодовые компоненты — передатчики, приемники и кабели более сложны в изготовлении, чем многомодовые, и таким образом, совокупные затраты на построение сети 1000Base LX обычно несколько превышают затраты при построении сети на основе технологии 1000Base SX. Преимущество применения данной технологии заключается в возможности обеспечения более высокой скорости и большей дальности распространения сигнала по оптическому кабелю.

Основной характеристикой, которая определяет потенциальную пропускную способность оптического кабеля, является модальная скорость (Modal Bandwidth).

Определение

Модальной скоростью называется интегральная характеристика волоконно-оптического кабеля, которая определяет возможные соотношения скорости и дальности передачи оптического сигнала по этому кабелю.

Модальная скорость обычно вычисляется в мегагерцах на километр (МГц × км) и измеряется в том диапазоне длин волн оптического излучения, который предполагается использовать для передачи сигнала. Большее значение модальной скорости соответствует лучшему качеству оптического кабеля и, следовательно, более высокому уровню скорости передачи данных и большему размеру магистрального сегмента ЛВС.

В табл. 14.3 приведены размеры максимального сегмента для технологий 1000Base SX и 1000Base LX в зависимости от характеристик используемого многомодового волоконно-оптического кабеля.

Важной характеристикой качества волоконно-оптического сегмента ЛВС является ресурс или бюджет оптической мощности линии.

Таблица 14.3. *Размеры максимального сегмента для 1000Base SX и 1000Base LX*

Технология и размер сегмента	Модальная скорость на 850 нм (МГц × км)		Модальная скорость на 1300 нм (МГц × км)	
	62,5 мкм	50 мкм	62,5 мкм	50 мкм
1000Base SX — 220м	160	—	—	—
1000Base SX — 275м	200	—	—	—
1000Base SX — 500м	—	400	—	—
1000Base SX — 550м	—	500	—	—
1000Base LX — 550м	—	—	500	400, 500

Определение

Ресурс или *бюджет оптической мощности линии* представляет собой выраженное в децибелах (дБ) превышение минимального уровня мощности излучения оптического передатчика над минимально допустимым уровнем сигнала на входе оптического приемника.

Эта характеристика во многом определяется специфическими для используемой технологии значениями параметров информационного обмена и, в дополнение к этому, косвенно учитывает особенности передачи данных в конкретной среде.

Таким образом, значение технологического бюджета линии, с одной стороны, и модальной скорости используемого волоконно-оптического кабеля, с другой стороны, позволяют однозначно определить основные эксплуатационные характеристики проектируемых каналов передачи данных.

В табл. 14.4 представлены обобщенные характеристики технологий 1000Base SX и 1000Base LX, которые обеспечивают передачу данных со скоростью до 1000 Мбит/сек по магистральным волоконно-оптическим соединениям локальных вычислительных сетей, построенных на основе технологий Ethernet/IEEE 802.3.

Наличие в спецификации 1000Base X двух взаимно дополняющих технологий позволяет применять при проектировании магистральных соединений мультисервисных ЛВС взвешенные решения, основанные на достоинствах каждой из них. Так, например, проектные решения, основанные на технологии 1000Base SX, традиционно считаются более предпочтительными для построения относительно коротких высокоскоростных магистралей, радиус действия которых ограничивается отдельно стоящим зданием или одним из его этажей. Соответственно, технология 1000Base LX имеет безусловное преимущество при выборе технических решений для организации дальних магистральных соединений, которые призваны обеспечить высокоскоростной ин-

формационный обмен в пределах небольшого населенного пункта или городского района.

Таблица 14.4. *Обобщенные характеристики технологий 1000Base SX и 1000Base LX*

Характеристика	Технология				
	1000Base SX		1000Base LX		
	62,5 мкм	50 мкм	62,5 мкм	50 мкм	10 мкм
Диапазон длин волн излучателя (нм)	770—860		1270—1355		
Минимальное значение мощности оптического излучения (dBm)	–9,5		–11,5		–11,0
Минимальное значение мощности принимаемого сигнала (dBm)	–17		–19		
Бюджет оптической мощности линии (дБ)	7,5	7,5	7,5	7,5	8,0
Максимальная длина сегмента (м)	275	550	550	550	5000

Протокол физического уровня 1000Base CX

Спецификация 1000Base CX определяет основные принципы построения предельно коротких магистральных соединений между оборудованием внутри узла ЛВС. Эта спецификация предполагает реализацию основных принципов информационного обмена 1000Base X для построения высокоскоростных магистралей на основе специального подготовленного экранированного двухпарного медного кабеля в качестве среды передачи данных.

Так же, как и в остальных технологиях группы 1000Base X, в технологии 1000Base CX на уровне PCS применяется схема кодирования 8B/10B, использование которой обеспечивает возможность взаимной синхронизации тактовых генераторов и вызывает повышение до значения 1250 МГц частоты сигнала, передаваемого в линию. Очевидно, что такой высокочастотный сигнал достаточно сильно искажается и быстро затухает при его передаче по медному кабелю. Кроме того, на такой высокой частоте особенно трудно преодолеть неизбежные взаимные помехи, вызванные передачей сигнала по другой паре кабеля в режиме полного дуплекса. Именно поэтому, несмотря на предельно высокие требования, предъявляемые к характеристикам экранированного кабеля 1000Base CX, максимальный размер сегмента ЛВС, построенного с использованием этой технологии, ограничен значением 25 м.

Вследствие относительно невысоких эксплуатационных характеристик и высокой стоимости компонентов эта технология не получила достаточно широкого распространения.

Спецификация 1000Base T

Спецификация 1000Base T является наиболее революционной среди спецификаций построения гигабитных магистралей Ethernet, поскольку обеспечивает передачу данных на скорости 1000 Мбит/сек по магистральному соединению, построенному на основе UTP категории 5 на расстояние до 100 м.

Принципы организации информационного обмена 1000Base T

Применение технологий 1000Base T обеспечивает возможность:

- совместимости на уровне управления каналом CSMA/CD MAC;
- применения регенераторов 1000 Мбит/сек;
- использования UTP ANSI/EIA/TIA-568-A-1995 (Category 5);
- реализации стандартной процедуры Auto-Negotiation 10/100/1000Base T;
- обеспечения полнодуплексного информационного обмена со скоростью передачи данных 1000 Мбит/сек на расстоянии до 100 м.

Указанные технические характеристики достигаются благодаря применению нестандартных способов представления и кодирования данных, передаваемых через магистральное соединение. Так, в частности, четырехкратное увеличение информационной скорости достигается благодаря одновременному использованию всех четырех пар кабеля UTP для передачи данных в полнодуплексном режиме.

Магистральное соединение 1000Base T образуют четыре параллельных канала, каждый из которых используется для передачи данных со скоростью 250 Мбит/сек. Для организации одного такого канала применяется одна из четырех пар кабеля UTP. Полнодуплексный режим информационного обмена в данном случае обеспечивается применением алгоритма и схемных решений — *Echo Cancellation*. Суть этого алгоритма состоит в том, что оба абонента одновременно и независимо используют одну и ту же пару медного кабеля для организации информационного обмена друг с другом. При этом в каждый из моментов времени в линии действует суммарный сигнал двух передатчиков. Очевидно, что для выделения сигнала дальнего абонента, ближнему абоненту достаточно выполнить вычитание собственного передаваемого сигнала из суммарного сигнала линии. Эта задача несколько усложняется

вследствие наличия в линии эхо-сигналов, которые представляют собой отражения сигналов, переданных ближним абонентом от входных цепей приемника дальнего абонента. Эти эхо-сигналы обычно имеют достаточно высокий уровень и поэтому оказывают существенное влияние на принимаемый сигнал. Компенсация воздействия эхо-сигналов выполняется при помощи второго вычитания передаваемого сигнала, при котором этот сигнал специально задерживается и ослабляется с тем, чтобы наилучшим образом соответствовать компенсируемому сигналу.

На рис. 14.2 приведена схема организации магистрального соединения 1000Base T.

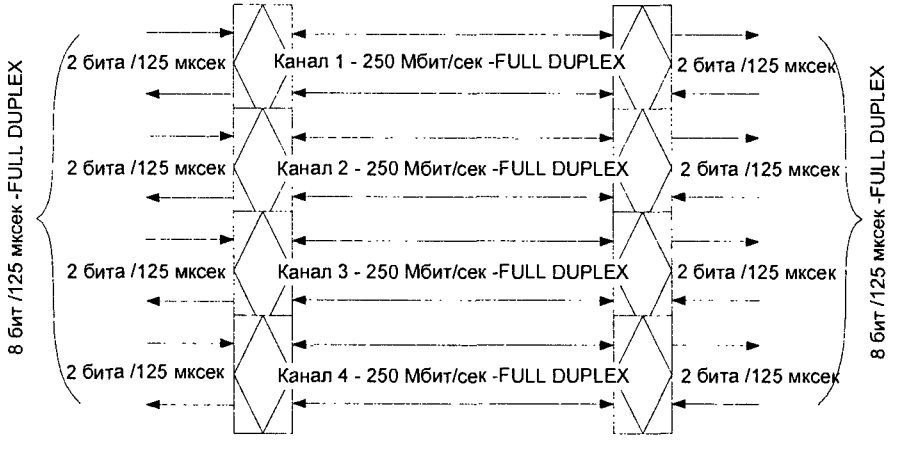


Рис. 14.2. Схема организации магистрального соединения 1000Base T

Информационная скорость 250 Мбит/сек в каждом из четырех параллельных каналов 1000Base T по витой паре категории 5 обеспечивается благодаря применению *многоуровневого амплитудно-импульсного кодирования — PAM5* (Five-level Pulse Amplitude Modulation). Применение многоуровневого кодирования PAM5 в данном случае обеспечивает требуемое значение информационной скорости в условиях ограничения максимальной скорости изменения сигнала в линии (символьной скорости) значением 125 МГц, что соответствует предельной частоте сигнала, передаваемого по UTP категории 5.

Передача n бит одним изменением параметров сигнала, передаваемого в линию, обычно реализуется при помощи многоуровневой амплитудной модуляции. Количество уровней в данном случае можно определить соотношением 2^n. В технологии 1000Base T применение пятиуровневого амплитудного кодирования обеспечивает кодовую избыточность, которая необходима для контроля и управления процессом передачи.

Избыточные коды PAM5 применяются для:

- ограничения начала и конца передаваемого блока данных;
- обеспечения устойчивой взаимной синхронизации тактовых генераторов передатчика и приемника данных;
- обнаружения искажений и потерь передаваемых данных.

Таким образом, процесс передачи данных по каналу 1000Base T представляет собой чередование последовательностей пятиуровневых символов {TA_n TB_n TC_n TD_n}, каждый из которых передается по отдельной паре кабеля UTP. В пределах одного такта изменения сигнала (8 нсек) каждый из таких символов кодируется одним из разрешенных уровней кодового напряжения:

- "–2" : –1,0 В;
- "–1" : –0,5 В;
- "0" : 0 В;
- "1" : 0,5 В;
- "2" : 1,0 В.

Легко подсчитать, что максимальное количество кодовых комбинаций в данном случае составляет 5^4 или 625 значений, в то время как для передачи одного информационного байта необходимо всего 256 комбинаций линейного кода. Более чем двукратная избыточность линейного кода 1000Base T, как уже было отмечено выше, используется для обеспечения обслуживания процесса формирования и приема кодовых групп. Основной задачей в данном случае, безусловно, является обнаружение ошибок при передаче кодовых последовательностей, поскольку передача модулированного сигнала на предельной для используемой среды передачи скорости практически неизбежно приводит к возникновению ошибок. Для уменьшения взаимного влияния формируемых сигналов и обеспечения требуемых частотных характеристик результирующей последовательности кодов поток входных байтов 1000Base T после многократного перемешивания (Scrambling) преобразуется в поток девятиразрядных символов $SD_n[0...8]$, каждый из которых кодируется одной из разрешенных комбинаций {TA_n TB_n TC_n TD_n}.

Особенности практической реализации 1000Base T

На первой стадии после включения питания каждый абонент ЛВС, который поддерживает спецификацию 1000Base T, должен выполнять стандартные требования по реализации процедуры *Auto-Negotiation*. Так же, как и при использовании технологии 1000Base T, эта процедура реализуется путем формирования и анализа последовательностей FLP. Небольшое отличие от стандартной процедуры в данном случае заключается в необходимости использо-

вания дополнительных кодовых страниц AN-MP и AN-UP для автоматического согласования параметров информационного обмена 1000Base T.

Примечание

Более полное описание процедуры Auto-Negotiation можно найти в *главе 15* настоящего издания.

Перед согласованием параметров информационного обмена 1000Base T с использованием процедуры Auto-Negotiation включается функция контроля состояния сигнала, которая предназначена для контроля стабильности сигнала, принимаемого от удаленного абонента. В том случае, если ближний абонент устойчиво принимает сигнал FLP (или NLP) от удаленного абонента, канал приема данных считается исправным и формируется сигнал "LINK_STATUS=OK".

Восстановление синхронизирующей последовательности из принятого сигнала в технологии 1000Base T выполняется независимо по каждой из четырех используемых пар кабеля UTP категории 5. Принятая последовательность синхроимпульсов должна быть достаточно стабильной для того, чтобы обеспечить требуемое значение вероятности возникновения ошибки в процессе приема кодового символа (SYMBOL ERROR RATIO < 10^{-10}).

Для обеспечения основных требований по организации информационного обмена при подключении устройств разного типа через интерфейс 1000Base T должно быть обеспечено перекрестное соединение линейных сигналов. Это перекрестное соединение может быть выполнено несколькими способами:

- использованием специального кабеля MDI/MDI-X 1000Base T — Crossover-кабеля;
- применением соединителя с альтернативным распределением сигналов. Спецификация 1000Base T рекомендует использование соединителей данного типа на многопортовых устройствах — репитерах и коммутаторах Ethernet. Обычно такой соединитель помечается символом "X"— (Crossover-порт);
- использованием функции автоматического определения типа подключенного устройства (MDI/MDI-X), как минимум, на одном из взаимодействующих устройств.

В табл. 14.5 приведена схема распределения линейных сигналов 1000Base T по контактам соединителя RJ-45 в зависимости от типа подключенного устройства.

Автоматическое определение типа подключенного устройства (MDI/MDI-X) не является обязательной функцией для абонентов ЛВС, поддерживающих

спецификацию 1000Base T. Вместе с тем, в данной спецификации определены основные положения, в соответствии с которыми такая процедура может быть реализована производителем коммуникационного оборудования. Так, в частности, предполагается, что автоматическое выполнение данной процедуры обеспечивает внутреннюю коммутацию линейных сигналов в соответствии со схемой, приведенной в табл. 14.5. Для устранения возможности возникновения циклических переходных процессов при выполнении процедуры автоматического определения типа порта подключенного устройства спецификацией 1000Base T рекомендуется использование в процессе принятия решений фиксированных временных задержек и генератора псевдослучайных чисел.

Таблица 14.5. *Распределение сигналов 1000Base T по контактам соединителя RJ-45*

Номер контакта RJ-45	Назначение сигнала	Порт MDI	Порт MDI-X — встроенный Crossover
1	Положительный полюс канала "A"	BI_DA+	BI_DB+
2	Отрицательный полюс канала "A"	BI_DA–	BI_DB–
3	Положительный полюс канала "B"	BI_DB+	BI_DA+
4	Положительный полюс канала "C"	BI_DC+	BI_DD+
5	Отрицательный полюс канала "C"	BI_DC–	BI_DD–
6	Отрицательный полюс канала "B"	BI_DB–	BI_DA–
7	Положительный полюс канала "D"	BI_DD+	BI_DC+
8	Отрицательный полюс канала "D"	BI_DD–	BI_DC–

В листинге 14.1 приведены результаты выполнения команд, которые используются для установки и контроля автоматического согласования типа интерфейса MDI/MDIX на коммутаторах Catalyst Cisco Systems.

Листинг 14.1. Установка и контроль автоматического согласования типа интерфейса MDI/MDIX на коммутаторах Catalyst Cisco Systems

```
    1. Переход в режим изменения конфигурации коммутатора
Switch# configure terminal
    2. Переход в режим изменения конфигурации интерфейса
Switch(config)# interface gigabitethernet1/0/1
    3. Установка режима автоматического согласования скорости
Switch(config-if)# speed auto
    4. Установка режима автоматического согласования дуплекса
Switch(config-if)# duplex auto
```

```
    5. Установка режима автоматического согласования типа интерфейса
Switch(config-if)# mdix auto
    6. Выход из режима изменения конфигурации коммутатора
Switch(config-if)# end
    7. Контроль состояния устройств управления интерфейсом
Switch# show controliers ethernet-controller gigabitethernet1/0/1 phy
Control Register                    :  0001 0001 0100 0000
Control STATUS                      :  0111 1001 0100 1001
Phy ID 1                            :  0000 0001 0100 0001
Phy ID 2                            :  0000 1100 0010 0100
Auto-Negotiation Advertisement      :  0000 0011 1110 0001
Auto-Negotiation Link Partner       :  0000 0000 0000 0000
Auto-Negotiation Expansion Reg      :  0000 0000 0000 0100
Next Page Transmit Register         :  0010 0000 0000 0001
...
Extended PHY Specific Status        :  1000 0100 1000 0000
Auto-MDIX                           :  On   [AdminState=1]
```

Технологии построения магистралей 10Gigabit Ethernet

Комплекс технологий 10Gigabit Ethernet предназначен для построения сверхвысокоскоростных магистральных соединений в сетях IEEE 802.3/Ethernet. Как следует из названия, технологии этого комплекса обеспечивают возможность передачи данных по магистральным соединениям ЛВС Ethernet на скорости 10 000 Мбит/сек.

В зависимости от особенностей реализации и предназначения, все технологии 10Gigabit Ethernet, определенные в спецификациях IEEE 802.3, могут быть условно разделены на три группы:

- технологии параллельной группы LAN (10GBase-X);
- технологии последовательной группы LAN (10GBase-R);
- технологии последовательной группы WAN (10GBase-W).

Основная особенность технологической группы 10GBase-X состоит в одновременном использовании четырех параллельных сегментов среды передачи для организации одного магистрального соединения. Эта технологическая особенность позволяет достичь десятикратного увеличения скорости при сохранении основных принципов, которые были использованы для организации информационного обмена в технологии 10Gigabit Ethernet.

В технологиях 10GBase-R и 10GBase-W, напротив, применяется новый принцип кодирования передаваемых данных на уровне PCS, что позволяет за счет

более эффективного использования пропускной способности среды передачи данных обеспечить десятикратное увеличение скорости информационного обмена в классической последовательной конфигурации среды передачи данных.

Параллельные магистрали 10GBase-X

В состав группы, которая имеет общее название 10GBase-X, входят технологии 10Gigabit Ethernet, обеспечивающие передачу данных со скоростью 10 000 Мбит/сек по параллельно-последовательным магистральным соединениям ЛВС Ethernet:

- 10GBase-LX4;
- 10GBase-CX4.

Основными особенностями технологического комплекса 1000Base-X являются:

- обеспечение совместимости с устройствами IEEE 802.3/Ethernet на уровне управления каналом CSMA/CD MAC;
- применение четырех независимых каналов передачи данных для построения единого магистрального соединения;
- обеспечение передачи данных в полнодуплексном режиме со скоростью 10 000 Мбит/сек на уровне интерфейса XGMII (10Gigabit Media Independent Interface);
- использование восстановленной из принимаемого сигнала синхронизирующей последовательности для обеспечения приема этого сигнала;
- возможность использования в качестве среды передачи сегментов специально сбалансированного медного кабеля (150 Ом) или стандартных одномодовых или многомодовых волоконно-оптических кабелей.

Организация информационного обмена 10GBase-X

Специфика организации информационного обмена в технологиях группы 1000Base-X определяется применением отработанной схемы кодирования 8B/10B на уровне PCS. Назначение и особенности практической реализации схемы кодирования 8B/10B достаточно подробно были описаны в предыдущих разделах этой главы. В данном случае следует отметить, что при использовании этого способа кодирования число кодировок, которые реально используются для передачи данных, существенно меньше, чем общее число возможных кодировок. Наличие такого запаса позволяет выбрать информационные кодировки таким образом, чтобы реализовать требования взаимной синхронизации тактовых генераторов и, кроме того, обеспечить выполнение

некоторых дополнительных условий, которые являются специфическими для используемой среды передачи данных.

Специфика применения алгоритма кодирования 8B/10B в магистральных технологиях группы 10GBase-X состоит в использовании четырех независимых каналов (lane) для передачи данных. При этом каждое передаваемое и принимаемое с уровня интерфейса XGMII 32-разрядное информационное слово (TXD[31:0] и RXD[31:0] соответственно) разбивается на 4 байта, а каждый такой байт снабжается управляющим признаком (TXC[3:0] и RXC[3:0] соответственно). Прямое и обратное преобразование информационных байтов XGMII в десятиразрядные кодовые группы выполняется по стандартным правилам, которые применяются в алгоритме 8B/10B. Каждая из десятиразрядных кодовых групп передается и принимается по отдельному и независимому информационному каналу.

В табл. 14.6 приведена схема распределения разрядов информационного слова по каналам 10GBase-X.

Таблица 14.6. *Распределение разрядов информационного слова по каналам 10GBase-X*

Номер канала (lane)	Передаваемые и принимаемые разряды TXD[31:0] и RXD[31:0]	Номер управляющего символа TXC и RXC	Разряды интегрального слова 8B/10B
0	Разряды с 7 по 0	0	Разряды с 9 по 0
1	Разряды с 15 по 8	1	Разряды с 19 по 10
2	Разряды с 23 по 16	2	Разряды с 29 по 20
3	Разряды с 31 по 24	3	Разряды с 39 по 30

Кодовые группы, передаваемые через интерфейс XGMII, разделены на две категории — управляющие и информационные. Признаком управляющей кодовой группы является ненулевое значение управляющего символа, сопровождающего данную группу. Информационные кодовые группы используются для организации информационного обмена через магистральное соединение, а управляющие кодовые комбинации, которые, как правило, включают в себя несколько управляющих символов, используются для контроля и управления процессом информационного обмена на интегральной магистрали 10GBase-X.

В дополнение к тем функциям контроля над процессом информационного обмена между абонентами, которые управляющие кодировки 8B/10B выполняют в технологиях 1000Base X, управляющие кодовые группы 10GBase-X

применяются для осуществления дополнительных задач, среди которых в первую очередь следует выделить:

- обнаружение и устранение временного рассогласования, которое вызвано независимостью синхронизации каждого из используемых компонентов интегрального канала передачи данных;
- сигнализацию о возникновении ошибок в процессе передачи и приема данных;
- формирование сообщений о состоянии интегрального канала передачи данных.

Так же, как и информационные данные, управляющие коды передаются независимо по каждому из компонентов магистрального канала, образуя вектор управляющего кода (Column). Таким способом передаются, например, управляющие коды незанятой линии — IDLE CODE. При формировании вектора управляющего кода особая роль предназначена базовому компоненту интегрального канала (Lane 0). Именно по этому каналу передается, в частности, управляющий символ начала вектора, который предваряет передачу кадра Ethernet по интегральной магистрали 10GBase-X.

Оптические WDM-магистрали 10GBase-LX4

Спецификация 10GBase-LX4 предполагает использование в качестве среды передачи данных сегментов многомодового волоконно-оптического кабеля с диаметром волокна 50 или 62,5 мкм или одномодовых оптических волокон диаметром 8—10 мкм. Формирование сигнала в 10GBase-LX4 осуществляется длинноволновыми (Long-Wave) лазерами, длина волны оптического излучения которых составляет около 1330 нм. Для передачи оптического сигнала этих лазеров могут быть использованы как многомодовые, так и одномодовые оптические кабели.

Для построения четырех независимых каналов передачи данных в магистральных соединениях 10GBase-LX4 применяется принцип волнового мультиплексирования.

Технологии *волнового мультиплексирования* — *WDM* (Wavelength Division Multiplexing) предназначены для повышения эффективности использования пропускной способности магистральных волоконно-оптических каналов, а также повышения дальности распространения сигнала в этих каналах.

Технологии волнового мультиплексирования основаны на возможности одновременного применения нескольких длин волн для передачи различных сигналов по одномодовому волоконно-оптическому кабелю. В том случае, если передаваемые сигналы будут размещены в непересекающихся частотных диапазонах, они не будут оказывать заметного влияния друг на друга и смогут независимо распространяться по виртуальным частотным каналам,

проложенным внутри волоконно-оптического кабеля. Возможность построения таких каналов объясняется тем, что области пониженной абсорбции — (окна) волоконно-оптического кабеля являются настолько широкими, что позволяют размещать в них несколько десятков независимых широкополосных сигналов.

В табл. 14.7 приведена схема распределения каналов 10GBase-LX4 по диапазонам волн излучения лазера.

Таблица 14.7. *Распределение каналов 10GBase-LX4 по диапазонам излучения*

Номер канала (lane)	Нижняя граница частотного диапазона (нм)	Верхняя граница частотного диапазона (нм)	Центральная длина волны (нм)
0	1269,0	1282,4	1275,7
1	1293,5	1306,9	1300,2
2	1318,0	1331,4	1324,7
3	1342,5	1355,9	1349,2

Реализация принципов частотного разделения при построении магистральных соединений позволяет использовать единую среду для передачи сигналов всех четырех компонентов интегрального канала 10GBase-LX4. Более того, при создании высокоскоростных магистралей в данном случае могут применяться сегменты многомодового — *MMF* (Multi Mode Fiber) и одномодового — *SMF* (Single Mode Fiber) волоконно-оптического кабеля.

В табл. 14.8 представлены обобщенные характеристики технологии 10GBase-LX4, которая обеспечивает передачу данных со скоростью до 10 000 Мбит/сек по магистральным волоконно-оптическим соединениям ЛВС.

Таблица 14.8. *Обобщенные характеристики технологии 10GBase-LX4*

Параметр	62,5 мкм MMF	50 мкм MMF		10 мкм SMF
Модальная скорость на 1300 нм (МГц × км)	500	400	500	—
Диапазон длин волн излучателя	см. табл. 14.7			
Минимальное значение мощности оптического излучения (dBm)	–6,75	–6,75	–6,75	–6,25
Минимальное значение мощности принимаемого сигнала (dBm)	–14,25	–14,25	–14,25	–14,45
Бюджет оптической мощности линии (дБ)	7,5	7,5	7,5	8,2
Максимальная длина сегмента (м)	300	240	300	10 000

Параллельная магистраль 10GBase-CX4

Легко подсчитать, что при использовании схемы кодирования 8B/10B общая скорость изменения сигнала в линии должна в 10/8 =1,25 раза превышать требуемое значение информационной скорости. Таким образом, для достижения скорости передачи данных 10 Гбит/сек скорость изменения сигнала в линии должна составлять 12 500 Мбит/сек, и, следовательно, символьная скорость в каждом из четырех компонентов магистрального канала 10GBase-X должна достигать 3 125 миллионов символов в секунду. Следовательно, скорость изменения сигнала в каждой из линий, составляющих интегральный канал 10GBase-X, более чем в три раза превышает аналогичную характеристику канала 1000Base X. Именно по этой причине к характеристикам каналов 10GBase-X предъявляются существенно более жесткие требования, которые оказывают заметное влияние на линейные размеры магистральных сегментов.

Спецификация 10GBase-CX4 определяет основные принципы построения предельно коротких магистральных соединений между оборудованием, размещенным на узлах ЛВС, на основе специального подготовленного экранированного многожильного медного кабеля в качестве среды передачи данных. Для информационного обмена при этом одновременно используются 8 независимо экранированных и сбалансированных пар. Основными характеристиками информационного обмена 10GBase-CX4 являются:

- передача данных в каждом из каналов со скоростью 3 125 Мбит/сек;
- амплитуда сигнального импульса напряжения 0,8—1,2 В;
- период следования импульсов 0,32 нсек.

Высокочастотный сигнал с приведенными выше характеристиками сильно искажается и быстро затухает при его передаче по медному кабелю. Кроме того, как уже было отмечено, на такой высокой частоте особенно трудно преодолеть неизбежные взаимные помехи, вызванные передачей сигнала по другой паре кабеля в режиме полного дуплекса. Поэтому максимальный размер сегмента ЛВС, построенного с использованием технологии 10GBase-CX4, ограничен значением 15 м.

Последовательные магистрали 10Gigabit Ethernet

Технологии, предназначенные для построения последовательных магистралей 10Gigabit Ethernet, могут быть условно разделены на две группы:

- технологии последовательной группы LAN (10GBase-R);
- технологии последовательной группы WAN (10GBase-W).

Технологии последовательной группы LAN предназначены для построения высокоскоростных соединений между магистральными узлами ЛВС. Технологии последовательной группы WAN предназначены для создания комбинированных магистралей, при помощи которых сегменты ЛВС могут быть соединены через сети, построенные на основе синхронной цифровой технологии разделения времени использования оптического канала — *SDH* (Synchronous Digital Hierarchy).

В технологиях 10GBase-R и 10GBase-W на уровне PCS вместо 8B/10B применяется принцип кодирования 64B/66B, что позволяет за счет более эффективного использования пропускной способности среды передачи данных обеспечить существенное увеличение дальности распространения сигнала и скорости информационного обмена в последовательной классической конфигурации среды передачи данных.

Организация информационного обмена 10GBase-R

Специфика организации информационного обмена в технологиях группы 10GBase-R определяется применением отработанной схемы кодирования 64B/66B на уровне PCS. Как и во всех описанных ранее технологиях построения магистральных каналов, кодирование позволяет повысить устойчивость взаимной синхронизации тактовых генераторов и обнаружить искажения передаваемых кодов. Нетрудно заметить при этом, что использование кодирующей схемы 64B/66B обеспечивает существенное (более чем в 1,2 раза) повышение эффективности использования пропускной способности канала передачи данных за счет сокращения доли управляющего (неинформативного) кода в интегральном информационном потоке.

Достаточная для обеспечения устойчивой синхронизации тактовых генераторов скорость изменения параметров формируемого сигнала обеспечивается при помощи предварительного перемешивания передаваемого кода (64 двоичных разряда). Управляющие символы 64B/66B не используют специальных выделенных байтовых кодов, таким образом, все возможные байтовые комбинации являются разрешенными. Признаком, который используется для разделения информационного и управляющего кодов, является значение двух младших битов 66 разрядного кода:

- 01XX...X — информационный код;
- 10УУ...У — управляющий код;
- 11XX...X и 00XX...X — запрещенные коды.

Примечание

Следует отметить, что запрещенными также считаются управляющие кодировки, не определенные в соответствующих таблицах спецификации 64B/66B.

Управляющие коды 64B/66B, как правило, включают в себя несколько восьмибитовых символов и используются для выполнения следующих функций:

- обеспечения устойчивой синхронизации в паузах между передаваемыми кадрами — символьная группа /I/;
- обозначения начала и конца передаваемого блока данных — символьные группы /S/ и /T/ соответственно;
- передачи сигнала об ошибке передаваемого кода — символьная группа /E/.

Следует отметить, что вследствие типового характера проектирования отмеченные выше символы, а также подавляющее большинство технических решений, которые используются для организации последовательных информационных магистралей 10Gigabit Ethernet, во многом аналогичны тем, что были описаны в предыдущих разделах данной главы. Универсальные принципы, которые широко используются при разработке спецификаций IEEE 802.3/Ethernet, позволяют применять типовые блоки при создании программных и реализации аппаратных решений в процессе проектирования и построения современного коммуникационного оборудования.

Специфика построения магистральных соединений 10GBase-W

Достоинства применения блочно-модульного принципа при разработке аппаратных и программных решений для построения магистральных соединений особенно наглядно проявляются на примере технологии 10Gigabit Ethernet. Именно применение такого принципа проектирования позволило специалистам комитета IEEE 802.3 при помощи внедрения всего одного дополнительного уровня обработки данных к тем, которые представлены в спецификации 10GBase-R, сформировать новую группу спецификаций (10GBase-W), предназначенных для построения комбинированных магистралей, при помощи которых сегменты ЛВС могут быть соединены через сети, основанные на технологи SDH.

Необходимость ввода дополнительного уровня обработки информации — *уровня WIS* (WAN Interface Sub) в данном случае была вызвана различием форматов представления и скоростей передачи данных, которые используются в технологиях LAN (Ethernet) и WAN (SDH).

Применяемый в технологии 10GBase-W промежуточный уровень WIS предназначен для прямого и обратного преобразования данных, которые передаются между уровнем PCS — 10GBase-R и стандартным уровнем PMA, и выполняет следующие функции:

- обеспечение полнодуплексного информационного обмена на уровне MAC Ethernet;

- поддержка стандартных программных и аппаратных решений, используемых на уровнях PCS, PMA и PMDL;
- обеспечение передачи данных со скоростью 9,95328 Гбит/сек в формате синхронного транспортного модуля уровня 64 — *уровня STM-64* (Synchronous Transport Module). При этом также выполняются стандартные для сетей SDH функции: формирование синхронных контейнеров — *SPE* (Synchronous Payload Envelope), перемешивание содержимого контейнеров и обнаружение ошибок при их передаче.

Основная особенность реализации информационного взаимодействия на уровне WIS в технологическом комплексе 10GBase-W определяется необходимостью согласования скоростей и обеспечения взаимной синхронизации между стандартными модулями физического уровня Ethernet и компонентами сети SDH. Так, например, информационный обмен через интерфейс между уровнями PCS и WIS выполняется путем передачи двухбайтовых слов со скоростью 599,04 миллионов пересылок в секунду. Общая информационная скорость передаваемого через интерфейс информационного потока, которая составляет в этом случае 9,58464 Гбит/сек, должна быть согласована с темпом передачи SPE — 149 760 байтов за каждые 125 мксек. Очевидно, что достичь требуемого согласования информационных скоростей в данном случае возможно за счет применения буферных накопителей с независимой синхронизацией или аналогичных им по выполняемым функциям устройств.

Характеристики последовательных магистралей 10Gigabit Ethernet

В спецификации IEEE 802.3/Ethernet определяются требования к характеристикам следующих разновидностей последовательных магистральных соединений 10Gigabit Ethernet:

- коротковолновая магистраль LAN 10GBase-SR (длина волны излучателя 850 нм);
- длинноволновая магистраль LAN 10GBase-LR (длина волны излучателя 1310 нм);
- длинноволновая магистраль LAN повышенной дальности 10GBase-ER (длина волны излучателя 1550 нм);
- коротковолновая магистраль WAN 10GBase-SW (длина волны излучателя 850 нм);
- длинноволновая магистраль WAN 10GBase-LW (длина волны излучателя 1310 нм);
- длинноволновая магистраль LAN повышенной дальности 10GBase-EW (длина волны излучателя 1550 нм).

В табл. 14.9 представлены обобщенные характеристики последовательных магистралей 10Gigabit Ethernet. Как уже было отмечено ранее, технологии последовательной группы LAN предназначены для построения соединений между магистральными узлами ЛВС, выполняющих передачу данных со скоростью 10 Гбит/сек по двум волокнам стандартного одномодового или многомодового волоконно-оптического кабеля. Технологии последовательной группы WAN предназначены для построения магистральных соединений через сети, построенные на основе технологии SDH.

Таблица 14.9. *Обобщенные характеристики магистралей 10Gigabit Ethernet*

Технология	Среда передачи данных	Модальная скорость (МГц × км) / 850 нм	Бюджет оптической мощности линии (дБ)	Максимальная длина сегмента (м)
10GBase-SR, 10GBase-SW	MMF 62.5 мм	160	7,3	26
10GBase-SR, 10GBase-SW	MMF 62.5 мм	200	7,3	33
10GBase-SR, 10GBase-SW	MMF 50 мм	400	7,3	66
10GBase-SR, 10GBase-SW	MMF 50 мм	500	7,3	82
10GBase-SR, 10GBase-SW	MMF 50 мм	2000	7,3	300
10GBase-LR, 10GBase-LW	B1.1 (3), SMF	—	9,4	10 000
10GBase-ER, 10GBase-EW	B1.1 (3), SMF	—	15	30 000

Применение модульных трансиверов в магистралях ЛВС

Магистральные компоненты телекоммуникационного оборудования — передатчики, приемники и соединительные элементы, как правило, имеют достаточно высокую стоимость. Это объясняется высокими требованиями к параметрам магистральных компонентов и характером их эксплуатации. При этом обычно магистральный компонент ЛВС обеспечивает передачу и прием данных с использованием крайне ограниченного набора технологий и средств передачи данных. Магистральные компоненты могут быть выполнены в виде отдельных устройств — приемопередатчиков или *трансиверов* — *Transceiver* (Transmitter/Receiver). Однако в подавляющем большинстве случаев магистральные компоненты встраиваются непосредственно в магистральный коммутатор, что позволяет использовать стандартные приложения для управле-

ния и контроля состояния магистрального соединения и избежать промежуточных интерфейсных соединений.

Основной недостаток применения встроенного магистрального компонента состоит в том, что изменение технологии построения магистрали, например переход от 1000Base SX к 1000Base LX, может потребовать полной замены магистрального коммутатора. В то же время большинство производителей активного оборудования ЛВС предлагают универсальное решение — модульные приемопередающие устройства — трансиверы.

Примечание

Следует учитывать, что в данном случае универсальность трансивера, как правило, означает возможность его применения в коммуникационных устройствах *конкретного* производителя. Поэтому перед приобретением или установкой в коммутатор встраиваемого трансивера следует внимательно ознакомиться с эксплуатационной документацией на оба этих устройства.

В момент подготовки материалов настоящего издания наиболее популярными среди производителей коммуникационного оборудования были встраиваемые трансиверы (конвертеры) следующих форматов:

- конвертер стандартного формата — *GBIC* (Gigabit Interface Converter);
- конвертер уменьшенного формата — *SFP* (Small Form-Factor Pluggable).

Размер лицевой панели конвертера формата SFP примерно в два раза меньше аналогичного размера конвертера GBIC, что обеспечивает более высокую плотность размещения портов на магистральном коммутаторе.

После установки в коммутатор модульный конвертер представляет собой обычный интерфейс коммутатора. Обычно в этом случае для него могут быть выполнены все команды изменения конфигурации и контроля состояния, которые используются для стандартных интерфейсов данного коммутатора. В дополнение к этому для контроля состояния оптических трансиверов могут быть использованы специфические команды, которые позволяют отображать текущие значения параметров оптического приемника и передатчика.

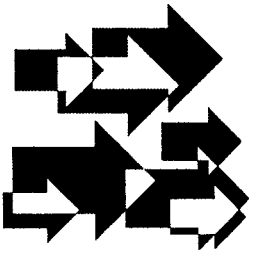
В листинге 14.2 приведены результаты выполнения команд, которые применяются для контроля состояния оптических компонентов модульного трансивера на коммутаторе Catalyst Cisco Systems.

Листинг 14.2. Контроль состояния оптических компонентов модульного трансивера на коммутаторе Catalyst Cisco Systems

```
Switch# show interfaces gigabitethernet0/3 transceiver detail
                        High Alarm  High Warn  Low Warn   Low Alarm
        Temperature     Threshold   Threshold  Threshold  Threshold
```

Port	(Celsius)	(Celsius)	(Celsius)	(Celsius)	(Celsius)
Gi0/3	41.5	110.0	103.0	-8.0	-12.0
		High Alarm	High Warn	Low Warn	Low Alarm
	Voltage	Threshold	Threshold	Threshold	Threshold
Port	(Volts)	(Volts)	(Volts)	(Volts)	(Volts)
Gi0/3	3.20	4.00	3.70	3.00	2.95
		High Alarm	High Warn	Low Warn	Low Alarm
	Current	Threshold	Threshold	Threshold	Threshold
Port	(milliamperes)	(mA)	(mA)	(mA)	(mA)
Gi0/3	31.0	84.0	70.0	4.0	2.0
	Optical	High Alarm	High Warn	Low Warn	Low Alarm
	Transmit Power	Threshold	Threshold	Threshold	Threshold
Port	(dBm)	(dBm)	(dBm)	(dBm)	(dBm)
Gi0/3	-0.0 (-0.0)	-0.0	-0.0	-0.0	-0.0

ГЛАВА 15



Организация подключения абонентов к оборудованию мультисервисных ЛВС

Подключение абонентов к оборудованию современных ЛВС обычно производится через *структурированную кабельную систему (СКС)* предприятия или организации. Как правило, эта кабельная система представляет собой сложную и разветвленную структуру, которая включает в себя сегменты кабелей UTP и разнообразные соединители — вилки, розетки, коммутационные панели, которые обеспечивают передачу данных между абонентами и активным оборудованием ЛВС. Таким образом, эффективность и качество информационного взаимодействия абонентов ЛВС во многом определяется качеством построения и исправностью компонентов системы СКС. Реализация на активном оборудовании ЛВС процедур автоматического контроля состояния абонентского подключения и оперативного согласования параметров информационного обмена позволяет существенно снизить трудоемкость обслуживания ЛВС и сократить время, необходимое для поиска возникающих в этой ЛВС неисправностей.

Специфика мультисервисных ЛВС состоит в том, что абоненты (функциональные компоненты) этих сетей, как правило, представляют собой логически обособленные автономные объекты, расположение которых в офисных помещениях определяется соображениями удобства эксплуатации или функциональными особенностями этих компонентов и не связано с размещением узлов активного оборудования ЛВС. Именно поэтому организация электропитания таких компонентов представляется достаточно сложной задачей, облегчить решение которой помогает использование технологии передачи электропитания по сигнальному кабелю Ethernet.

Первый раздел настоящей главы посвящен рассмотрению принципов построения и особенностей применения технологий автоматического контроля и согласования параметров линии.

Во втором разделе рассмотрены особенности организации электропитания абонентов мультисервисных локальных сетей с применением технических решений для передачи электропитания по сигнальному кабелю Ethernet.

Контроль и согласование параметров линии

При подключении абонентов к оборудованию ЛВС в первую очередь должен быть обеспечен постоянный и оперативный контроль соединительной линии, которая связывает абонентов с активным оборудованием. Использование технологий автоматического согласования параметров информационного обмена между активным оборудованием и абонентами мультисервисных ЛВС позволяет более полно реализовать возможности функциональных устройств и существенно упрощает процедуру администрирования активного оборудования ЛВС.

Далее будут описаны стандартные процедуры автоматической проверки целостности линии, которые входят в состав комплекса технологий Ethernet/IEEE 802.3.

Процедура проверки целостности линии

Процедура *проверки целостности линии — процедура Link Integrity Test* обеспечивает постоянное и автоматическое тестирование компонентов физического сегмента, который соединяет двух взаимодействующих абонентов мультисервисных ЛВС. Выполнение этой процедуры предусматривает периодический обмен технологическими импульсами между абонентами, подключение которых к ЛВС осуществляется с использованием кабеля UTP. Поскольку при выполнении этой проверки используются все компоненты физического сегмента — соединители и розетки RJ-45, патч-панели и патч-корды, она позволяет достаточно полно и оперативно локализовать такие неисправности ЛВС, как обрыв сегмента UTP или нарушение контакта в соединителе или розетке RJ-45.

При выполнении процедуры проверки целостности линии Link Integrity Test у каждого устройства, выполняющего информационный обмен в ЛВС в соответствии с требованиями, установленными спецификацией IEEE 802.3 10BaseT, на входных контактах интерфейса RD_INPUT постоянно должны присутствовать принимаемые данные. Эти данные представляют собой либо обычные кадры Ethernet, либо технологические импульсы — *NLP* (Normal Link Pulses) процедуры Link Integrity Test, передаваемые удаленным абонентом. В случае отсутствия принимаемых данных в течение интервала времени, определяемого значением параметра LINK_LOSS, принимающее устройство фиксирует нарушение целостности линии с удаленным абонентом ЛВС и переходит в состояние "LINK TEST FAIL". Выход из этого состояния и переход

к состоянию "LINK TEST PASS" осуществляется после получения на входной интерфейс нормального кадра Ethernet или нескольких последовательных технологических импульсов процедуры Link Integrity Test, количество которых определяется значением параметра LC_MAX. Последовательными считаются импульсы NLP, которые непрерывно поступают на входной интерфейс абонента ЛВС в течение интервала времени, определяемого значением параметра LINK_TEST_MAX. Минимальный период различимости технологических импульсов, обеспечивающих выполнение процедуры Link Integrity Test, определяется значением параметра LINK_TEST_MIN. Все технологические импульсы, которые будут приняты в этот период процедурой Link Integrity Test, рассматриваются как единый импульс. Это ограничение позволяет выполнить правильное диагностирование линий, которые обеспечивают постоянный физический контакт.

В табл. 15.1 приведены рекомендуемые значения параметров процедуры проверки целостности линии.

Таблица 15.1. *Рекомендуемые значения параметров процедуры Link Integrity Test*

Параметр процедуры Link Integrity Test	Минимальное значение	Максимальное значение
LINK_LOSS	50 мсек	150 мсек
LC_MAX	2 повторения	10 повторений
LINK_TEST_MAX	25 мсек	150 мсек
LINK_TEST_MIN	2 мсек	7 мсек

Примечание

Следует учитывать, что диагностика "LINK TEST PASS" процедуры проверки целостности линии — Link Integrity Test означает исправность только той части физического сегмента, которая обеспечивает прием данных от удаленного абонента ЛВС. Эта процедура не дает возможность локальной станции установить факт наличия или отсутствия приема на удаленной стороне тех данных, которые формирует ближняя станция.

Аналогичным образом процедура Link Integrity Test реализуется на устройствах, выполняющих информационный обмен в ЛВС в соответствии с требованиями, установленными спецификацией IEEE 802.3 100BaseT и 1000BaseT.

Автоматическое согласование параметров обмена

Процедура автоматического согласования параметров информационного обмена — процедура *Auto-Negotiation* (AN) обеспечивает возможность опера-

тивного автоматического конфигурирования по принципу "Plug and Play" компонентов локальных вычислительных сетей. Неэкранированная витая пара является универсальной средой передачи и может быть с успехом использована для построения сегментов ЛВС разнообразных вариантов спецификаций IEEE 802.3:

- 10BaseT;
- 100BaseTX;
- 100BaseT2;
- 100BaseT4;
- 1000BaseT.

Несмотря на единство используемой среды передачи, в каждой из отмеченных ранее спецификаций применяются специфические способы кодирования сигналов, передаваемых в линию, что исключает возможность непосредственного информационного обмена между двумя устройствами, которые используют несовпадающие технологии. Для того, чтобы упростить процесс системной интеграции и избежать процедуры ручного конфигурирования, набор спецификаций IEEE 802.3 был дополнен процедурой, которая позволяет автоматизировать процесс согласования оптимального типа технологии из числа поддерживаемых взаимодействующими устройствами.

Основные принципы автоматического согласования параметров

Процедура Auto-Negotiation выполняется на физическом уровне при помощи обмена специальными сообщениями, который выполняется между двумя взаимодействующими устройствами после их подключения к сегменту UTP. Используя информацию, полученную в сообщениях AN, эти устройства могут определить и согласовать друг с другом наиболее подходящий режим информационного обмена между ними.

Процедуры Link Integrity Test и Auto-Negotiation являются взаимно исключающими, поскольку для выполнения каждой из этих процедур взаимодействующие устройства должны обмениваться различными по форме последовательностями периодических импульсов. В случае процедуры Link Integrity Test это импульсы NLP, которые формируются с периодом 8—16 мсек. Для выполнения процедуры Auto-Negotiation используются группы быстрых канальных импульсов — *FLP* (Fast Link Pulse). Группы импульсов FLP также передаются с периодом 8—16 мсек и состоят обычно из 33 импульсов, которые следуют друг за другом с периодом 62,5 мксек.

Примечание

Значение периода повторения импульсов FLP специально выбрано таким образом, чтобы в том случае, когда партнер не способен участвовать в процедуре

Auto-Negotiation, он мог бы интерпретировать импульсы FLP в качестве обычных импульсов NLP.

Нечетные импульсы последовательности FLP (1, 3, 5, ... 33) используются для синхронизации передаваемой группы. Шестнадцать четных импульсов FLP предназначены для передачи информационного слова [D0—D15]. Наличие импульса в четной позиции FLP интерпретируется как "1", его отсутствие как "0" соответствующего разряда информационного слова.

Операции, которые выполняются в пределах процедуры Auto-Negotiation (AN), могут быть условно разделены на два класса:

- основная операция;
- вспомогательные операции.

Процедура Auto-Negotiation (AN) предусматривает выполнение дополнительных функций, которые не применяются в ходе согласования параметров информационного обмена, а используются для того, чтобы обеспечить возможность быстрой локализации неисправности в канале передачи данных или предотвратить возникновение такой неисправности. К числу таких дополнительных функций относятся:

- *интерфейс управления* — Management Interface;
- *сигнализация об ошибке на удаленной стороне* — Remote Fault Indication.

Интерфейс управления обеспечивает накопление и представление информации о проблемах, которые возникают при выполнении процедуры AN. В частности, с помощью данной функции могут быть выполнены следующие действия:

- определение причины, из-за которой автоматическое согласование параметров соединения оказалось невозможным;
- оперативное изменение параметров установленного соединения;
- сигнализация об ошибке на удаленной стороне. Используется для того, чтобы представить информацию о характере возникших проблем (неправильный тип кабеля, неправильная раскладка используемых пар). Обычно результаты выполнения этой операции передаются с использованием описываемых далее дополнительных страниц AN.

Основная операция процедуры AN — автоматическое определение типа технологии, используемой для передачи данных — в зависимости от типа взаимодействующих компонентов может выполняться в двух режимах:

- *в обычном режиме* (Normal Operation) — когда оба взаимодействующих устройства поддерживают процедуру AN;
- *в режиме параллельного определения* (Parallel Detection) — когда только одно из взаимодействующих устройств поддерживает процедуру AN.

Во втором случае более продвинутое устройство должно определить единственный тип технологии, которую поддерживает удаленный абонент, исследуя характер формируемых им сигналов. Этот режим реализуется путем проверки параллельного приема импульсов NLP во всех форматах, которые поддерживает активный абонент AN. Поскольку в данном случае проверка может дать положительный результат только для одной технологии — той, которую поддерживает удаленный абонент AN, необходимость в процедуре выбора отпадает.

Примечание

Следует отметить, что применение асимметричного режима (Parallel Detection) реализации процедуры Auto-Negotiation теоретически не позволяет определить тип дуплексного обмена, который использует удаленная сторона для передачи и приема данных.

Наиболее верным признаком того, что при автоматическом выполнении асимметричного варианта процедуры Auto-Negotiation были выбраны несовпадающие режимы дуплексного обмена, является резкое увеличение количества ошибок и коллизий на интерфейсах взаимодействующих устройств. Единственным способом разрешения подобных ситуаций может быть только ручное изменение конфигурации на одном из взаимодействующих абонентов Ethernet.

На рис. 15.1 представлен результат выполнения диагностических команд на рабочей станции, подключенной к активному оборудованию ЛВС с использованием режима Auto-Negotiation.

В листинге 15.1 представлен результат контроля состояния порта на коммутаторе Cisco Catalyst 2950. В данном случае порт коммутатора сконфигурирован для информационного обмена со скоростью передачи данных 10 Мбит/сек в полудуплексном режиме. Вследствие искусственно вызванного несовпадения настроек портов на коммутаторе будут фиксироваться коллизии и ошибки приема кадров. Соответствующие строки на приводимом далее листинге отмечены маркером.

Листинг 15.1. Результат контроля состояния порта на коммутаторе Cisco Catalyst 2950

```
2950_ST#sh int f0/2
FastEthernet0/2 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0015.c6bc.f782 (bia
0015.c6bc.f782)
  MTU 1500 bytes, BW 10000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 10Mb/s, media type is 100BaseTX

5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 14000 bits/sec, 5 packets/sec
   1224 packets input, 139479 bytes, 0 no buffer
   Received 12 broadcasts (0 multicast)
   0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 6 multicast, 0 pause input
   0 input packets with dribble condition detected
   3415 packets output, 1151576 bytes, 0 underruns
   25 output errors, 9 collisions, 0 interface resets
   0 babbles, 25 late collision, 21 deferred
   0 lost carrier, 0 no carrier, 0 PAUSE output
   0 output buffer failures, 0 output buffers swapped out
```

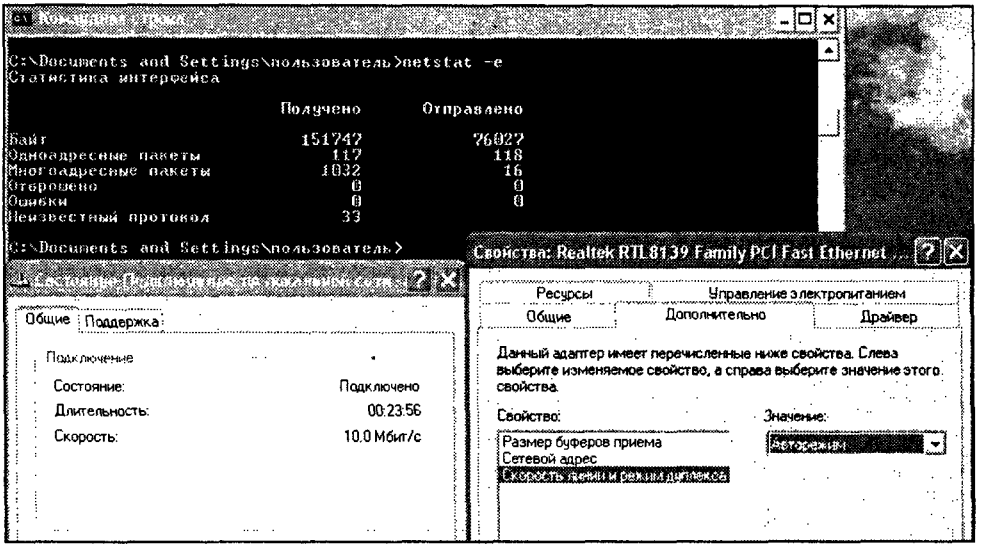


Рис. 15.1. Результат выполнения диагностических команд на рабочей станции, подключенной к ЛВС в режиме Auto-Negotiation

Сообщения Auto-Negotiation

Компоненты локальной вычислительной сети, которые участвуют в выполнении процедуры Auto-Negotiation, в дальнейшем описании будут называться партнерами. Как уже было отмечено, выполнение процедуры Auto-Negotia-

tion заключается в том, что один из партнеров предоставляет другому информацию о своих возможностях. На первой стадии этого взаимного обмена информацией каждый из партнеров независимо принимает решение о том, какой именно протокол физического уровня должен быть использован для установления соединения. На последующих стадиях взаимного обмена каждый из партнеров согласует тип выбранной технологии с удаленным партнером. В том случае, если оба партнера согласны использовать выбранную технологию передачи данных, процедура Auto-Negotiation считается успешно завершенной.

Примечание

Следует ***особо отметить***, что процедура Auto-Negotiation данных ***не предусматривает*** выполнение проверки соответствия характеристик используемой среды требованиям выбранной технологии передачи данных. Поэтому успешное выполнение этой процедуры ***не гарантирует*** возможность эффективной передачи данных с использованием взаимно согласованной технологии в сегменте ЛВС.

Информация, которой партнеры обмениваются при выполнении процедуры Auto-Negotiation, представлена в виде кадров физического уровня. В табл. 15.2 приведена структура кодового слова канала — *Link Codeword* (LCW), которое передается партнерами при выполнении процедуры Auto-Negotiation.

Таблица 15.2. *Структура кодового слова Link Codeword*

Номер бита	Наименование и содержание поля	Длина поля (бит)
D0—D4	S0-S4 — selector field — тип технологии канального уровня	5
D5—D12	A0-A7 — technology ability field — тип протокола физического уровня	8
D13	RF — извещение об ошибке	1
D14	ACK — подтверждение приема последовательных наборов FLP	1
D15	NP — признак использования дополнительной страницы	1

Значение поля S0-S4 — selector field определяет, какая из технологий, использующих кабель UTP в качестве среды передачи данных, поддерживается данным устройством. Значения 0 и свыше 5 данного поля зарезервированы для дальнейшего использования. На момент подготовки материалов настоящего издания были определены следующие значения кодировок данного поля:

- 1 — технология CSMA/CD — Ethernet (IEEE 802.3);
- 2 — технология IEEE 802.9 ISLAN-16T;

- 3 — технология Token Ring (IEEE 802.5);
- 4 — технология Fire Wire (IEEE 1394).

Значение поля A0-A7 — technology ability field используется для задания типов технологий, которые могут применяться для передачи данных на физическом уровне. При формировании значения этого поля применяется позиционный способ кодирования, при котором каждому из вариантов технологии соответствует выбранный разряд:

- A0 — 10BaseT Full-duplex;
- A1 — 10BaseT;
- A2 — 100BaseTX;
- A3 — 100BaseTX Full-duplex;
- A4 — 100BaseT4;
- A5 — Asymmetric PAUSE toward link partner;
- A6 — Symmetric PAUSE.

Старшие разряды поля TECHNOLOGY ABILITY используются для указания возможности применения партнерами технологий управления потоком кадров на сегменте Ethernet, которые будут описаны более подробно в последующих разделах настоящей главы.

Поле RF (Remote Fault) используется для формирования извещения об ошибке, которая возникла в процессе выполнения одной из процедур, обеспечивающих прием или передачу данных на данном объекте.

Признак, размещаемый в поле ACK (Acknowledge), используется при выполнении процедуры Auto-Negotiation для указания того, что ближняя станция приняла достаточное количество последовательных наборов импульсов NLP для того, чтобы перейти к следующему этапу согласования технологий передачи данных.

Поле NP (Next Page) используется для указания того, что ближняя станция предполагает участвовать в расширенном варианте информационного обмена, при котором могут быть использованы дополнительные, по отношению к основной, информационные страницы.

Особенности организации процесса согласования

Как уже было отмечено ранее, информация, которая необходима для успешного выполнения процедуры Auto-Negotiation (AN), передается между партнерами в кадрах специальной формы, которые называются *кодовыми страницами канала*.

В процессе выполнения процедуры Auto-Negotiation можно выделить несколько последовательных стадий:

- на первоначальном этапе оба партнера обмениваются словами LCW, в которых установлены значения бита ACK = 0;
- ближняя станция определяет отношение партнера к процедуре Auto-Negotiation по наличию FLP-импульсов в принимаемой группе NLP;
- ближняя станция переходит в режим "ожидание", в котором она ожидает приема 3 полных последовательных групп FLP. После того как станция принимает ожидаемые группы, она начинает передавать слова LCW с признаком ACK = 1;
- после того как ближняя станция получит от партнера более трех последовательных слов LCW с установленным признаком ACK = 1, она переходит в режим "подтверждение". В этом режиме могут быть выполнены дальнейшие действия по согласованию параметров информационного обмена;
- после передачи более 6—8 последовательных слов LCW станции могут принять участие в информационном обмене с использованием дополнительных страниц процедуры Auto-Negotiation (AN).

Информационный обмен с использованием дополнительных страниц может производиться после того, как между станциями, которые участвуют в процедуре AN, установлено состояние типа "Полное подтверждение". Если обе станции заявляют готовность участия в обмене с использованием дополнительных страниц, то они должны передать, как минимум, по одной дополнительной странице.

Применение дополнительных страниц позволяет передавать диагностическую информацию о проблемах, которые возникли в процессе выполнения основной процедуры Auto-Negotiation (AN), а также обеспечивает возможность дальнейшего развития этой процедуры. Примером подобного развития, в частности, является дополнение базовой процедуры согласования в части использования таких технологий, как 100BaseT2 и 1000BaseT.

Для выполнения дополнительного информационного обмена в процедуре Auto-Negotiation используются два типа дополнительных страниц:

- *страница сообщения — AN-MP* (Auto-Negotiation Message Page);
- *неформатированная страница — AN-UP* (Auto-Negotiation Unformatted Page).

Обмен с использованием дополнительных страниц включает в себя передачу одной страницы сообщения Auto-Negotiation Message Page, за которой следует одна или несколько неформатированных страниц (кодовых слов) Auto-Negotiation Unformatted Page. Эти страницы так же, как и слово состояния

канала LCW, передаются с использованием импульсов FLP и имеют примерно одинаковую структуру.

Структура дополнительных кодовых слов, которые используются для выполнения расширенной процедуры AN, представлена в табл. 15.3.

Таблица 15.3. *Структура дополнительных кодовых слов процедуры Auto-Negotiation (AN)*

Номер бита	Назначение	Наименование и содержание поля	Длина поля (бит)
D0—D10	M0—M10/ U0—U10	MESSAGE CODE — код сообщения — Message Page / UNFORMATTED CODE — неформатированный код	11
D11	T	T — признак последовательности приема кодовых слов	1
D12	ACK2	ACK2 — признак подтверждения выбранного режима	1
D13	MP	MP — тип дополнительного кодового слова	1
D14	ACK	ACK — подтверждение приема последовательных наборов	1
D15	NP	NP — признак использования дополнительной страницы	1

В поле MESSAGE CODE страницы сообщения размещается код сообщения. Обычно в данном поле размещается тип данных, которые будут передаваться в последующих неформатированных страницах. Признаком завершения информационного обмена с использованием дополнительных кодовых слов является прием страницы с кодом сообщения "Null Message" (код = 00000000001 = 1). На момент подготовки материалов настоящего издания были определены следующие значения кодировок данного поля:

- 0 — зарезервировано для дальнейшего использования;
- 1 — пустое сообщение ("Null Message");
- 2 — универсальное сообщение, за которым следует одно неформатированное сообщение с указанием вариантов поддерживаемых протоколов информационного обмена;
- 3 — универсальное сообщение, за которым следуют два неформатированных сообщения с указанием вариантов поддерживаемых протоколов информационного обмена;
- 4 — сообщение об ошибке, которая была зафиксирована при выполнении протокола информационного обмена;
- 5 — передача старших разрядов MAC-адреса (Organizationally Unique Identifier Code);

- 6 — передача младших разрядов MAC-адреса (PHY Identifier Tag Code);
- 7 — сообщение согласования технологии 100BaseT2, которым следует неформатированное сообщение с указанием вариантов поддерживаемых протоколов информационного обмена;
- 8 — сообщение согласования технологии 1000BaseT, которым следует два неформатированных сообщения с указанием вариантов поддерживаемых протоколов информационного обмена.

В поле UNFORMATTED CODE размещаются фиксированные коды, которые определяют тип сформированного дополнительного сообщения, например, диагностическое сообщение о причине возникновения аварийной ситуации или сообщения о типе поддерживаемых вариантов протокола физического уровня. Например, поле UNFORMATTED CODE первого неформатированного сообщения, которое следует за сообщением согласования технологии 1000BaseT, имеет следующую структуру:

- U10—U5 — зарезервированы для дальнейшего использования;
- U4 — признак поддержки технологии 1000BaseT half duplex;
- U3 — признак поддержки технологии 1000BaseT full duplex;
- U2 — признак типа порта 1000BaseT ("1" = multiport device или "0" = single-port device);
- U1 — ручная настройка режима ведущий-ведомый (Master-Slave) для порта 1000BaseT ("1" = Master или "0" = Slave);
- U0 — признак разрешения ручной настройки режима ведущий-ведомый для порта 1000BaseT ("1" = ручная конфигурация режима разрешена).

Примечание

Согласование вариантов протокола физического уровня при помощи дополнительных сообщений AN выполняется только для протоколов 100BaseT2 и 1000BaseT, использование которых не может быть согласовано партнерами AN при помощи слов Link Codeworld (LCW) стандартного формата.

Поле T (Toggle) используется для выполнения контроля последовательности приема дополнительных слов. Значение этого слова поочередно меняется из "1" в "0" для каждого последующего формируемого слова, и, таким образом, приемник может узнать о том, что он получает передаваемые слова без потерь.

В поле MP размещается признак типа дополнительного кодового слова:

- значение MP = 0 соответствует неформатированной странице;
- значение MP = 1 соответствует странице сообщения.

Поля ACK и ACK2 используются для размещения признаков подтверждения, причем значение признака ACK полностью соответствует значению аналогичного признака, размещенного в базовом слове LCW, а признак ACK2 может быть использован для согласования режимов, объявляемых дополнительными кодовыми словами.

Содержимое поля NP используется для того, чтобы указать на наличие или отсутствие следующей страницы, которая должна быть получена после данной. У последней дополнительной страницы в потоке признак NP устанавливается равным "1".

Критерии выбора технологии

Выбор оптимального типа протокола физического уровня из числа протоколов, поддерживаемых обоими участниками процесса Auto-Negotiation, осуществляется с использованием установленной системы приоритетов этого протокола. В соответствии с этой системой технологии, которые могут быть использованы для передачи данных по UTP, упорядочены в порядке убывания предпочтения следующим образом:

1. 1000BaseT full duplex.
2. 1000BaseT.
3. 100BaseT2 full duplex.
4. 100BaseTX full duplex.
5. 100BaseT2.
6. 100BaseT4.
7. 100BaseTX.
8. 10BaseT full duplex.
9. 10BaseT.

Естественно, что при выборе в первую очередь предпочтение отдается технологиям обмена, которые способны обеспечить большее значение скорости информационного обмена. При прочих равных условиях преимущества получают технологии полнодуплексной передачи данных. Кроме того, дополнительное преимущество при выборе технологии получают те технологии, которые предъявляют меньшие требования к характеристикам используемой среды передачи данных. Именно по этой причине, например, технология 100BaseT4 имеет преимущество по отношению к технологии 100BaseTX.

Управление потоком данных в сегменте Ethernet

Резкий рост скорости передачи данных в локальных вычислительных сетях 802.3 заставил разработчиков IEEE сформировать дополнительные механиз-

мы, которые могли бы защитить сетевые приложения компонентов локальных сетей от перегрузок, обеспечивая управление потоком передачи данных. В частности, спецификация IEEE 802.3x определяет механизм выполнения процедуры Flow Control на канальном уровне IEEE 802.3.

Когда один из компонентов локальной вычислительной сети начинает принимать больше кадров, чем он может обработать, возникает опасность переполнения буферов предварительного хранения и, как следствие этого, потери данных на канальном уровне. Данные, которые были потеряны на канальном уровне, будут восстановлены компонентами следующих уровней — сетевого и транспортного, однако пропускная способность сети в данном случае будет резко уменьшена. Если компонент локальной сети, который находится в состоянии временной перегрузки, сможет ограничить поток поступающих кадров, то потери кадров можно будет избежать.

Формат кадра управления потоком

Для обеспечения управления потоком компоненты локальной сети обмениваются кадрами специального формата, которые называются кадры паузы (PAUSE Frames).

В табл. 15.4 представлена структура кадра типа PAUSE (Пауза).

Таблица 15.4. *Структура кадра PAUSE*

Номер поля	Наименование и содержание поля	Значение	Длина поля (байт)
1	DA — групповой или индивидуальный адрес назначения кадра PAUSE		6
2	SA — адрес источника кадра PAUSE		6
3	LENGTH/TYPE — признак кадра PAUSE	88-08	2
4	OPCODE — тип операции	00-01	2
5	PAUSE _TIME — величина паузы		2
6	RESERVED — зарезервировано		42
7	FCS — контрольная сумма кадра		4

В поле DA (Destination Address) кадра данного типа должен быть размещен код 01-80-C2-00-00-01, который представляет собой Multicast-адрес станций, поддерживающих выполнение данной процедуры, или Unicast-адрес конкретного абонента в сети, формирующего избыточный трафик для данной станции.

В поле SA (Source Address) кадра типа PAUSE помещается MAC-адрес станции, которая инициирует выполнение процедуры управления потоком.

В поле LENGTH/TYPE этого кадра размещается код 8808, зарезервированный IEEE для кадров, применяемых в процедурах управления на уровне MAC.

Поле OPCODE содержит признак кадра управления потоком 0001.

В поле PAUSE_TIME размещается код, который соответствует размеру предлагаемой паузы, выраженному в битовых интервалах. Единица младшего разряда этого кода соответствует 512 битовым интервалам используемой технологии. Таким образом, размер предлагаемой паузы для технологий Fast Ethernet может иметь значение от 0 до 0,3 сек.

Остальные поля кадра PAUSE зарезервированы для дальнейшего использования или выполняют служебные функции.

Режимы использования процедуры управления потоком

Процедура управления потоком может выполняться в двух режимах:

- симметричном режиме;
- асимметричном режиме.

Симметричный режим управления потоком возможен в том случае, если оба взаимодействующих устройства могут формировать и правильно интерпретировать кадры типа PAUSE. В том случае, если только одно из взаимодействующих устройств поддерживает процедуру управления потоком, должен быть использован асимметричный режим. Возможности партнеров по информационному взаимодействию относительно использования управления потоком могут быть определены в процессе выполнения процедуры Auto-Negotiation.

Биты D10 и D11 в слове LCW определяют способность формировать и интерпретировать кадр типа PAUSE и возможность участия в процедуре асимметричного управления потоком ASM_DIR, соответственно.

В табл. 15.5 приведены возможные варианты режима управления потоком в зависимости от заявленных возможностей партнеров по информационному взаимодействию.

Таблица 15.5. *Варианты реализации режима управления потоком*

Ближняя станция		Дальний партнер		Ближняя станция		Дальний партнер	
D10	D11	D10	D11	PAUSE в передаче	PAUSE на приеме	PAUSE в передаче	PAUSE на приеме
0	0	X	X	Нет	Нет	Нет	Нет
0	1	0	X	Нет	Нет	Нет	Нет

Таблица 15.5 (окончание)

Ближняя станция		Дальний партнер		Ближняя станция		Дальний партнер	
D10	D11	D10	D11	PAUSE в передаче	PAUSE на приеме	PAUSE в передаче	PAUSE на приеме
0	1	1	0	Нет	Нет	Нет	Нет
0	1	1	1	Да	Нет	Нет	Да
1	0	0	X	Нет	Нет	Нет	Нет
1	X	1	X	Да	Да	Да	Да
1	1	0	0	Нет	Нет	Нет	Нет
1	1	0	1	Нет	Да	Да	Нет

Электропитание абонентов мультисервисных ЛВС

Специфика электропитания функциональных компонентов мультисервисных сетей определяется тем, что эти компоненты обычно представляют собой логически обособленные автономные объекты. К объектам такого рода в первую очередь следует отнести:

- камеры видеонаблюдения;
- аппаратные шлюзы VoIP;
- IP-телефоны.

Расположение функциональных компонентов в офисных помещениях определяется соображениями удобства эксплуатации или функциональными особенностями этих компонентов и, зачастую, никак не связано с размещением узлов активного оборудования ЛВС. Так, например, камеры наружного и внутреннего видеонаблюдения должны быть размещены в таких точках, с которых обеспечивается достаточный угол обзора отслеживаемых объектов. Поэтому такие камеры обычно закрепляются высоко на стене или под потолком. Телефонные аппараты, наоборот, устанавливаются таким образом, чтобы было удобно их использовать — на рабочем столе или на стене, в непосредственной близости от рабочего места оператора.

Как в первом, так и во втором из описанных случаев обеспечение электропитания функционального оборудования мультисервисной ЛВС является достаточно сложной задачей. Одним из наиболее эффективных способов решения этой проблемы является электропитание функционального оборудования

мультисервисной ЛВС низковольтным напряжением, которое подается непосредственно по сетевому кабелю Ethernet. Для обозначения комплекса технических решений, которые обеспечивают такой режим электропитания оборудования ЛВС, иногда используют неофициальное наименование *PoE* (Power over Ethernet).

Протокол PoE

Основные принципы организации и требования к значениям технических характеристик систем электропитания функционального оборудования ЛВС по сетевому кабелю Ethernet приведены в главе 33 "Power via Media Dependent Interface (MDI)" общей спецификации IEEE 802.3. Эти системы обеспечивают электропитание абонентов ЛВС напряжением 36—56 В постоянного тока с мощностью до 12 Вт и отвечают большинству требований, которые предъявляются к системам электропитания абонентов мультисервисных ЛВС.

Особенности электропитания абонентов мультисервисных ЛВС

При решении этой задачи должны быть учтены следующие условия и требования:

- *необходимость преобразования промышленного напряжения*. Функциональные компоненты мультисервисных ЛВС, как правило, представляют собой малогабаритные низковольтные устройства. Подключение таких устройств к сети переменного тока 200 В/50 Гц обычно выполняется через индивидуальные адаптеры промышленного электропитания. Следовательно, для подключения такого функционального устройства должна быть использована дополнительная розетка в том месте, в котором она могла и не быть запланирована исходным проектом ЛВС;
- *резервирование электропитания*. Функциональные компоненты мультисервисных ЛВС, как правило, используются для выполнения ответственных функций, и поэтому обеспечение их бесперебойного функционирования является, безусловно, достаточно актуальной задачей. Однако очевидно, что практически невозможно предусмотреть в проекте установку розеток гарантированного электропитания во всех точках, где потенциально могут быть размещены функциональные компоненты мультисервисной ЛВС;
- *защита от несанкционированных манипуляций электропитанием*. В некоторых случаях, например, при использовании камер видеонаблюдения, проектные решения должны исключать или ограничивать возможность несанкционированного физического отключения электропитания функ-

циональных компонентов мультисервисной ЛВС. Очевидно, что такое требование трудно или невозможно обеспечить при использовании стандартной схемы электропитания;

- *доставка питающего напряжения на функциональное устройство.* Само по себе подключение функционального компонента к системе электропитания мультисервисной ЛВС может также вызвать существенные затруднения. Эти затруднения обусловлены необходимостью одновременного выполнения эстетических и эргономических требований заказчика и нормативов проектирования сетей промышленного электропитания, которые определяют тип используемого кабеля, способ его прокладки и закрепления.

Совершенно очевидно, что необходимость решения отмеченных ранее или подобных задач существенно усложняет проектирование, снижает качество проектных решений и увеличивает стоимость реализации проекта.

Основные принципы PoE

В соответствии с терминологией, используемой в системах PoE, активные компоненты ЛВС — в первую очередь, коммутаторы Ethernet, выполняют функции *источников питающего напряжения — PSE* (Power Sourcing Equipment). Функциональное оборудование ЛВС в данном случае рассматривается в качестве *потребителя электрической энергии — PD* (Powered Device). Спецификация "Power via MDI" (PoE) определяет следующие режимы и характеристики формирования электропитания:

- характеристики источника напряжения электропитания, обеспечивающие передачу этого напряжения от PSE к PD по кабелю UTP;
- протокол, обеспечивающий автоматическое определение потребности абонента ЛВС в электропитании;
- способ классификации PD в зависимости от их требований к характеристикам питающего напряжения;
- метод автоматического отключения электропитания в том случае, если PD более не нуждается во внешнем источнике электропитания.

Назначение PSE, таким образом, состоит не только в том, чтобы осуществлять электропитание подключенного абонента. Устройство, выполняющее функцию PSE, должно также обеспечивать постоянный контроль параметров этого напряжения с тем, чтобы снять электропитание в том случае, если потребитель в нем более не нуждается. Для электропитания PD могут быть использованы различные схемы передачи напряжения. В табл. 15.6 приведены варианты использования проводящих пар UTP и соответствующих контактов соединителя RJ-45 для передачи питающего напряжения от PSE к PD.

Таблица 15.6. Использование пар UTP для передачи питания от PSE к PD

Контакт соединителя RJ-45	Вариант А (MDI-X)	Вариант А (MDI)	Вариант В
1	Negative VPort (–U)	Positive VPort (+U)	—
2	Negative VPort (–U)	Positive VPort (+U)	—
3	Positive VPort (+U	Negative VPort (–U)	—
4	—	—	Positive VPort (+U)
5	—	—	Positive VPort (+U)
6	Positive VPort (+U)	Negative VPort (-U)	—
7	—	—	Negative VPort (–U)
8	—	—	Negative VPort (–U)

Как видно из представленной таблицы, в обеих разновидностях реализации электропитания PD по варианту "А" для передачи питающего напряжения используются те же пары UTP, по которым производится передача данных. Это, с одной стороны, обеспечивает возможность применения выбранного решения в более широком спектре технологий Ethernet и, с другой стороны, позволяет использовать решения PoE в тех ЛВС, где применяются экономичные двухпарные сегменты UTP.

Реализация протокола PoE

В процессе реализации протокола устройство PoE выполняет несколько последовательных этапов тестирования подключенного оборудования, что призвано исключить возможность подключения электропитания не по назначению. Можно выделить три этапа:

1. Контроль подключения PD (Detection).
2. Классификация PD (Classification).
3. Передача полного питающего напряжения на PD.

Контроль подключения потребителя электропитания производится при помощи измерения электрических характеристик линии, которая связывает PSE и PD. Это измерение производится путем передачи контрольных напряжений по цепям предполагаемого электропитания PD. Спецификация PoE предусматривает выполнение, как минимум, двух таких проверок и ограничивает величину допустимых расхождений между полученными в них результатами. В табл. 15.7 приведены регламентированные значения основных параметров, которые используются при выполнении контроля подключения абонентов PoE.

Таблица 15.7. *Значения параметров контроля подключения абонентов PoE*

Наименование параметра	Ед. изм.	Значение	
		Мин.	Макс.
R.GOOD — допустимое значение сопротивления линии	кОм	19	26,5
R.BAD — недопустимое значение сопротивления линии	кОм	15	33
R.OPEN — значение сопротивления открытой линии	кОм	500	—
C.GOOD — допустимое значение емкости линии	нФ	—	150
C.BAD — недопустимое значение емкости линии	мкФ	10	—
VOS — допустимый разброс измеряемых значений	В	—	2,0

Процедура проверки подключения PD считается успешно выполненной в том случае, если измеренные значения параметров линии соответствуют допустимым значениям параметров R.GOOD и C.GOOD. В том случае, если хотя бы одно из контролируемых значений выходит за рамки разрешенного диапазона, проверка подключения считается невыполненной. В последнем случае ход выполнения дальнейших проверок зависит от того, какой из возможных вариантов (см. табл. 15.6) был выбран для подключения данного абонентского устройства к активному оборудованию ЛВС. Так, в частности, слишком большая величина измеренного значения сопротивления линии может быть признаком того, что провода проверяемой пары просто не подключены к абоненту. Такая ситуация возникнет, например, в процессе проверки пары 4—5 при подключении потребителя электропитания по варианту "А".

Процедура PoE, для сокращения общего цикла выполнения проверки подключения, предусматривает диагностирование пар UTP, которые не используются на абонентском устройстве ЛВС. В соответствии с требованиями этой процедуры, пара считается неподключенной в том случае, если измеренное значение сопротивления линии превышает пороговое значение открытой линии — R.OPEN. Очевидно, что повторные проверки подключения и все последующие операции по организации электропитания абонента следует выполнять только для тех пар UTP, которые отвечают критериям нормального подключения.

Задачей второго этапа процедуры PoE является классификация подключенного устройства PD, которая выполняется для определения требуемых параметров напряжения электропитания. Определение оптимального и согласованного режима электропитания позволяет, с одной стороны, наиболее рационально и эффективно использовать совокупный ресурс источника электропитания —

PSE и, с другой стороны, обеспечивает возможность защиты источника и потребителя электроэнергии от повышенных напряжений и замыканий питающих цепей.

Классификация подключенного устройства PD производится путем передачи эталонного напряжения классификации V.CLASS (от 15,5 до 20,5 В), по тем парам UTP, которые были определены на этапе контроля подключения. Классификация PD выполняется в зависимости от величины тока, потребляемого этим абонентом от источника эталонного напряжения. Для исключения возможности перегрузки источника эталонного напряжения максимальная величина тока, потребляемого абонентом на этапе классификации, ограничивается значением 100 мА.

В табл. 15.8 приведены общие характеристики питающего напряжения, формируемого PSE для различных классов потребителей, и пороговые значения тока, которые используются для классификации соответствующей группы абонентов.

Таблица 15.8. *Характеристики PSE для различных классов потребителей*

Характеристика	Класс 0	Класс 1	Класс2	Класс 3	Класс 4
Минимальное значение питающего напряжения (В)	36	36	36	36	36
Максимальное значение питающего напряжения (В)	56	56	56	56	56
Минимальное значение потребляемой мощности PD* (Вт)	0,44	0,44	3,84	6,49	—
Максимальное значение потребляемой мощности PD* (Вт)	12,95	3,84	6,49	12,95	—
Минимальное значение передаваемой мощности PSE (Вт)	0,5	0,5	4,0	7,0	0,5
Максимальное значение передаваемой мощности PSE (Вт)	15,40	4,0	7,0	15,40	15,40
Минимальное значение тока классификации (мА)	0	9	17	26	36
Максимальное значение тока классификации (мА)	4	12	20	30	44

*Здесь приведены значения уровня мощности, которые измеряются на входе потребляющего устройства PD. От 5 до 20% мощности, передаваемой от PSE, обычно теряются из-за рассеивания на UTP.

В исходной конфигурации источник PSE осуществляет питание абонентов напряжением постоянного тока, характеристики которого соответствуют тре-

бованиям класса 0. Электропитание с использованием повышенных токов потребления (классы 1, 2 и 3) применяется только в случае успешного завершения процедуры классификации для соответствующего класса. Электропитание абонентов по классу 4 текущей версией протокола PoE не предусмотрено, т. к. этот класс зарезервирован для обеспечения возможности дальнейшего расширения протокола.

Протокол PoEP

Опыт промышленной эксплуатации активного оборудования ЛВС, обеспечивающего поддержку спецификации PoE, показал работоспособность выбранных технических решений. Основным недостатком PoE является то, что вследствие малого сечения проводника и большой длины соединительной линии, эта технология принципиально не может обеспечить такую степень эффективности передачи питающего напряжения, которая свойственна стандартным источникам электропитания. К недостаткам PoE следует отнести и относительно небольшой уровень мощности, который может быть использован для электропитания потребителя. Но, тем не менее, несомненные преимущества ее использования, которые были отмечены в начале данного раздела, обеспечивают постоянный рост производства компонентов PoE и расширение области их применения. Так, например, достаточно перспективным представляется применение этой технологии при создании распределенных беспроводных сетей IEEE 802.11 и IEEE 802.16, однако следует отметить, что уровни мощности, которые необходимы для питания базовых станций IEEE 802.16, в некоторых случаях могут существенно превысить возможности технологии Po.

Обеспечение совместимости с PoE

Стремительный рост мультисервисных сетей и появление новых возможностей применения технологии PoE привели к необходимости модернизации этой, теперь уже достаточно популярной, технологии. Разработка спецификации расширенного протокола электропитания абонентов ЛВС — *PoEP* (Power over Ethernet Plus) выполняется специалистами комитета IEEE 802.3at. К моменту подготовки материалов настоящего издания этим комитетом были разработаны основные принципы, в соответствии с которыми должна быть подготовлена новая версия протокола, и сформулированы основные требования к характеристикам питающих напряжений.

Так, в частности, одним из основных принципов технологии PoEP является обеспечение обратной совместимости с устройствами PoE. В табл. 15.9 приведены варианты соединения устройств, которые поддерживают базовую или расширенную версию протокола PoE.

Таблица 15.9. Соединение устройств базовой и расширенной версии протокола PoE

Характеристики потребителя электропитания	Источник PoE PSE	Источник PoEP PSE
Стандартный PoE PD	Нормальный режим	Нормальный режим
PoEP PD с потреблением <12,95 Вт	Нормальный режим	Режим расширенной классификации
PoEP PD с потреблением >12,95 Вт	Извещение на PD об ограничении мощности	Режим расширенной классификации

В соответствии с основным требованием PoEP стандартные потребители PoE PD могут получать электропитание от любого из источников PoE(P), без каких-либо ограничений. Потребители PoEP PD с уровнем потребления, который соответствует требованиям процедуры PoE, также получают питание от источников любого типа, но при этом источник PoEP PSE может обеспечить расширенный режим классификации, который позволяет более точно учесть потребности абонента. При подключении к источнику PSE PoE абонента с повышенным уровнем потребления требуемый режим электропитания не может быть обеспечен, и в этом случае потребитель PoEP PD должен сформировать диагностику о включении режима ограниченного питания.

Планируемые характеристики PoEP

Основное отличие систем электропитания PoEP от классических систем PoE, естественно, заключается в увеличении до 60 Вт мощности, передаваемой для электропитания абонента ЛВС (режим повышенной мощности PoEP — High Power). Планируется, что это увеличение может быть достигнуто благодаря использованию всех четырех пар UTP для передачи питающего напряжения от PSE к PD. Предусматривается также и возможность двукратного увеличения мощности питающего напряжения, которое передается только по двум сигнальным или свободным парам UTP — до 30 Вт (режим пониженной мощности PoEP — Medium Power).

Большое внимание разработчики PoEP уделяют модернизации процедуры классификации. В частности, эту модернизацию предлагается вести по следующим направлениям:

- увеличение количества градаций, используемых в процедуре классификации до 20—30;
- использование логарифмической шкалы для классификации потребностей абонентов PoEP. В диапазоне малых мощностей (<12 Вт) при этом предполагается использовать строго линейную шкалу, а в диапазоне повышенных мощностей (>30 Вт) — использовать строго логарифмическую шкалу;

- обеспечение возможности динамического управления на PSE потреблением выбранного PD с использованием, при необходимости, возможностей протокола канального уровня OSI ISO 7498. Реализация такого управления не только обеспечивает существенную экономию электроэнергии, но и позволяет строить на PSE гибкие и эффективные политики распределения этой энергии.

Не вызывает никакого сомнения, что модернизированная технология PoEP будет с успехом использоваться при построении перспективных мультисервисных вычислительных сетей.

Особенности организации электропитания абонентов мультисервисных ЛВС

Очень многие из функциональных компонентов современных ЛВС обеспечивают возможность их электропитания по сигнальному кабелю. О поддержке спецификации Power over Ethernet — PoE — могут говорить указания о совместимости с PoE-устройствами или о соответствии с требованиями IEEE 802.3af — предварительной версии основной спецификации PoE, приведенные в технической документации на оборудование. Отсутствие разъема или кабеля питания на функциональном компоненте ЛВС также может считаться признаком поддержки этой спецификации.

Основная часть необходимых настроек по определению параметров электропитания абонентов мультисервисной ЛВС выполняется на специальных коммутаторах, которые реализуют функции PoE PSE и обеспечивают передачу электропитания абоненту ЛВС через сигнальный кабель Ethernet.

Особенности конфигурации активного оборудования PoE

В процессе настройки функций PoE на коммутаторе Ethernet должны быть определены следующие характеристики и параметры этой технологии:

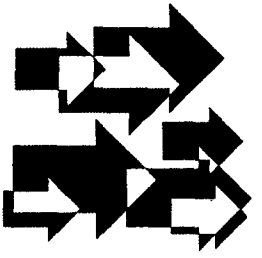
- значение максимальной мощности, которая может быть передана через порт для электропитания абонента, подключенного к этому порту (для PoE — не более 15,5 Вт);
- способ передачи электропитания по проводам UTP (см. табл. 15.6);
- относительный приоритет порта при распределении общего ресурса электропитания коммутатора. Как правило, общий ресурс источника электропитания ограничивается значением 200—300 Вт. В том случае, если этот ресурс окажется недостаточным для электропитания всех подключенных к нему абонентов, в первую очередь отключению подлежат абоненты, которые имеют более низкий приоритет.

В листинге 15.2 приведены результаты выполнения настройки функций и контроля параметров PoE на коммутаторе 3COM 4500. Маркером в листинге помечены значения параметров, которые были изменены в данной конфигурации.

Листинг 15.2. Результаты выполнения настройки функций и контроля параметров PoE на коммутаторе 3COM 4500

```
   1. Включение режима PoE на коммутаторе
[3C-45-Ethernet1/0/1]poe enable
Port power supply is enabled
   2. Установка режима автоматического управления питанием на
      коммутаторе
[3C-45]poe power-management auto
Auto Power Management is enabled
   3. Установка значения максимальной мощности, которая может быть
      передана через порт для электропитания абонента
[3C-45-Ethernet1/0/1]poe max-power 15000
Set Port max power successfully
   4. Выбор способа передачи питающего напряжения (в данном случае — по
      сигнальным парам)
[3C-45-Ethernet1/0/1]poe mode signal
Set PoE mode successfully
   5. Установка относительного приоритета порта для распределения общего
      ресурса электропитания коммутатора
[3C-45-Ethernet1/0/1]poe priority critical
Set Port POE priority successfully
   6. Контроль параметров источника электропитания
[3C-45]display poe interface ethernet1/0/1
Port power enabled :enable
Port power ON/OFF :on
Port power status :Standard PD
Port power mode :signal
Port PD class :0
port power priority :critical
Port max power :15000 mW
Port current power :460 mW
Port peak power :550 mW
Port average power :540 mW
Port current :10 mA
Port voltage :51 V
```

ГЛАВА 16



Программные компоненты мультисервисных ЛВС

Все программные компоненты, которые используются в мультисервисных ЛВС можно условно разделить на следующие группы:

- компоненты функционального программного обеспечения;
- компоненты технологического программного обеспечения.

Функциональные программные комплексы используются как для формирования мультисервисных потоков, так и для непосредственного приема этих потоков абонентами ЛВС. Технологическое программное обеспечение предназначается для выполнения разнообразных служебных функций, которые связаны с организацией вещания мультисервисных потоков в ЛВС.

Первый раздел данной главы посвящен рассмотрению технологических программ, обеспечивающих управление оборудованием мультисервисных ЛВС и мониторинг состояния этого оборудования. В этом разделе также рассматриваются технические решения и программные компоненты, которые обеспечивают анализ и документирование информации о трафике, передаваемом в мультисервисных ЛВС.

Во втором разделе рассматриваются компоненты функционального программного обеспечения, обеспечивающие прием и формирование видео- и аудиопотоков. В этом разделе, в частности, рассматриваются абонентские и серверные приложения, которые могут быть использованы для реализации систем пакетной телефонии (VoIP), а также трансляции аудио- и видеопотоков в ЛВС Ethernet.

Технологическое программное обеспечение

Технологическое программное обеспечение представляет собой комплекс инструментов, обеспечивающих выполнение вспомогательных задач, возни-

кающих в процессе управления мультисервисными ЛВС. К задачам подобного рода можно отнести:

- администрирование и обслуживание активного оборудования ЛВС;
- сбор и предоставление оперативной информации о состоянии компонентов сети, сигнализация о возникновении аварийных ситуаций;
- локализация и устранение неисправностей;
- управление качеством и учет предоставляемых услуг;
- обеспечение информационной безопасности.

Функции технологического программного обеспечения можно разделить на две большие группы:

- контроль состояния (мониторинг) и управление компонентами мультисервисной ЛВС;
- мониторинг и управление информационными потоками мультисервисной ЛВС.

Технологическое программное обеспечение первой группы обеспечивает анализ выбранных параметров сетевых устройств. Такой анализ может производиться постоянно или по требованию оператора. Управление сетевыми компонентами предполагает изменение параметров (конфигурации) этих компонентов в процессе функционирования.

Мониторинг и управление информационными потоками ЛВС осуществляется для учета предоставляемых услуг и обеспечения безопасности информационного обмена в мультисервисной ЛВС.

Контроль состояния и управление компонентами мультисервисных ЛВС

Технологические программы, обеспечивающие контроль состояния и управление компонентами современных мультисервисных ЛВС, обычно используют протокол SNMP, который не только досконально анализирует состояние любого устройства, подключенного к сети, но и позволяет этому устройству формировать и направлять сигналы об изменении своего состояния. Протокол сетевого обслуживания SNMP обладает практически неограниченными возможностями мониторинга состояний сложных иерархически организованных объектов.

Функция управления компонентами мультисервисных ЛВС является более сложной и многогранной, чем описанная ранее функция мониторинга. Специфика этой функции заключается в том, что управляющие действия должны быть выполнены в максимально короткие сроки. Вследствие этого выполне-

ние функций управления в большинстве случаев должно быть реализовано без участия оператора и максимально автоматизировано. Протоколы и технические решения, которые обеспечивают оперативное управление компонентами ЛВС, описаны в *главах 8 и 9* настоящего издания.

Протокол SNMP

Первоначально основные положения, которые регламентируют принципы построения и использования протокола управления сетевыми компонентами Интернета — *SNMP* (Simple Network Management Protocol), были представлены специалистами IETF в середине 1990 года. С тех пор эти положения неоднократно подвергались дополнениям и переработкам, поэтому в настоящее время существует группа документов IETF, в которых описаны различные аспекты построения и применения протокола SNMP. В табл. 16.1 приведен перечень основных документов, которые описывают общие принципы построения протокола SNMP.

Таблица 16.1. *Документы, описывающие общие принципы протокола SNMP*

RFC	STD	Месяц и год	Статус	Наименование документа
1155	0016	May 1990	STANDARD	Structure and identification of management information for TCP/IP-based internets
1156	—	May 1990	HISTORIC	Management Information Base for network management of TCP/IP-based internets
1157	—	May 1990	HISTORIC	Simple Network Management Protocol (SNMP)
1213	0017	March 1991	STANDARD	Management Information Base for Network Management of TCP/IP-based internets: MIB-II
3414	0062	December 2002	STANDARD	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

SNMP представляет собой расширяемый протокол прикладного уровня, предназначенный для обеспечения обмена управляющей информацией между сетевыми устройствами. Возможность расширения и дальнейшего развития систем управления, построенных на основе протокола SNMP, обеспечивается применением при создании этого протокола стандартных и универсальных технических решений. К таким решениям можно отнести использование в протоколе SNMP расширяемых баз данных управляющей информации — *MIB* (Management Information Base) и универсальной системы описания управляемых объектов — *ASN.1* (Abstract Syntax Notation one). Доработка спецификации протокола SNMP может быть продолжена по мере того, как

будут развиваться и разрабатываться современные прикладные программы управления, основанные на использовании этого протокола. Именно по этой причине, несмотря на относительную простоту протокола SNMP, он является достаточно мощным средством для решения большинства проблем, возникающих при управлении компонентами мультисервисных сетей.

Принципы построения системы управления сетью SNMP

Система управления сетью, основанная на использовании протокола SNMP, представляет собой комплекс, который включает в себя следующие компоненты:

- управляемые объекты с агентами управления SNMP;
- управляющие станции;
- систему управления.

Объектами управления протокола SNMP являются аппаратные и программные компоненты, которые используются для формирования и обслуживания информационных потоков мультисервисных ЛВС, например, коммутаторы, маршрутизаторы, программные модули сетевых операционных систем.

Агентами в SNMP (SNMP Agent) называются специализированные программные блоки управляемых объектов протокола SNMP, которые собирают информацию о состоянии этих объектов и размещают ее в своих локальных переменных. Локальные переменные агентов SNMP представляют собой компоненты единой и универсальной информационной базы данных управления сетью — MIB. Каждая из локальных переменных имеет двунаправленную информационную связь с одним из компонентов управляемого устройства. Изменение состояния некоторого компонента управляемого объекта влечет за собой изменение значения соответствующей локальной переменной, и, наоборот, изменение значения некоторой локальной переменной влечет за собой изменение состояния соответствующего компонента управляемого объекта.

На управляющих станциях выполняются приложения, которые управляют действиями агентов SNMP, расположенных на сетевых элементах мультисервисной ЛВС, путем анализа и модификации значений локальных переменных. Протокол SNMP в данном случае используется для обмена управляющей и контрольной информацией между управляющими станциями и объектами управления. Сформированная при помощи протокола SNMP база локальных переменных MIB однозначно отображает текущее состояние всех управляемых компонентов ЛВС.

Система управления сетевыми компонентами — *NMS* (Network Management Systems) представляет собой программно-аппаратный комплекс, включаю-

щий в себя одну или несколько управляющих станций, которые действуют под управлением единого программного обеспечения с использованием протокола SNMP.

Идентификация объектов MIB

Гибкость протокола SNMP и возможность дальнейшего развития решений на его основе во многом обеспечиваются использованием древообразной иерархической формы адресации записей в информационной базе MIB. В этом случае все управляемые объекты информационной базы представляют собой ветви единого дерева управляемых объектов MIB, листьями которого являются отдельные компоненты управляемого объекта. Использование этого способа адресации позволяет легко добавлять к существующей информационной базе новые ветви — объекты или листья — новые компоненты управляемых объектов.

Каждый управляемый объект MIB имеет уникальный идентификатор, а также имя, которое соответствует функции, выполняемой этим объектом. Идентификатор представляет собой последовательность номеров ветвей, по которым проходит путь к объекту от корня дерева MIB.

Корень дерева управляемых объектов MIB не имеет идентификатора. Первый уровень ветвей, исходящих от безымянного корня, составляют объекты, находящиеся в ведении международных стандартизирующих организаций:

- CCITT (ITU) — идентификатор ветви = 0;
- ISO — идентификатор ветви = 1;
- JOINT-ISO-ITU — идентификатор ветви = 2.

Во втором уровне общего дерева и первом уровне дерева ISO (1) располагаются объекты, которые находятся под администрированием международной стандартизирующей организации — ISO. Так, в частности, на ветви ISO (1).ORG (3) общего дерева MIB располагаются управляемые объекты различных организаций, подведомственных ISO в части формирования баз протокола SNMP. Одной из таких организаций третьего уровня является Министерство обороны США: ISO (1).ORG (3) DOD (6), в ведении которого, согласно иерархии управления протокола SNMP, находится пакетная сеть TCP/IP: ISO (1).ORG (3) DOD (6) Internet (1). Таким образом, согласно этой иерархии, идентификаторы всех управляемых объектов MIB в сети Интернет должны начинаться с кода 1.3.6.1.

В свою очередь, ветвь сети Интернет дает начало нескольким ветвям пятого уровня иерархии управляемых объектов MIB:

- ветви справочника (Directory) — идентификатор ветви = 1;
- ветви управления (Mgmt) — идентификатор ветви = 2;

- экспериментальной ветви (Experimental) — идентификатор ветви = 3;
- частной ветви (Private) — идентификатор ветви = 4.

Частная ветвь (Private) является вырожденной и имеет в настоящее время только одно дерево шестого уровня иерархии MIB — Enterprises (предприятия). В отличие от своей предшественницы, ветвь Enterprises дает начало более чем 27 000 ветвей седьмого уровня, которые занимают различные поставщики оборудования, разработчики программного обеспечения и разнообразные государственные учреждения и организации. Идентификаторы частной ветви используются этими организациями для того, чтобы определить номенклатуру и состав управляемых объектов MIB для своего оборудования и обеспечить возможность использования универсальных технологических программ для управления этим оборудованием. Например, идентификаторы ветви 171 (1.3.6.1.4.1.171) используются для описания управляемых объектов телекоммуникационного оборудования D-Link Systems, Inc., ветвь 43 (1.3.6.1.4.1.43) используется для описания объектов компании 3COM. На рис. 16.1 представлен пример формирования идентификатора MIB — в данном случае в качестве объекта мониторинга используется усредненная скорость передачи данных через интерфейс № 1 маршрутизатора компании Cisco Systems.

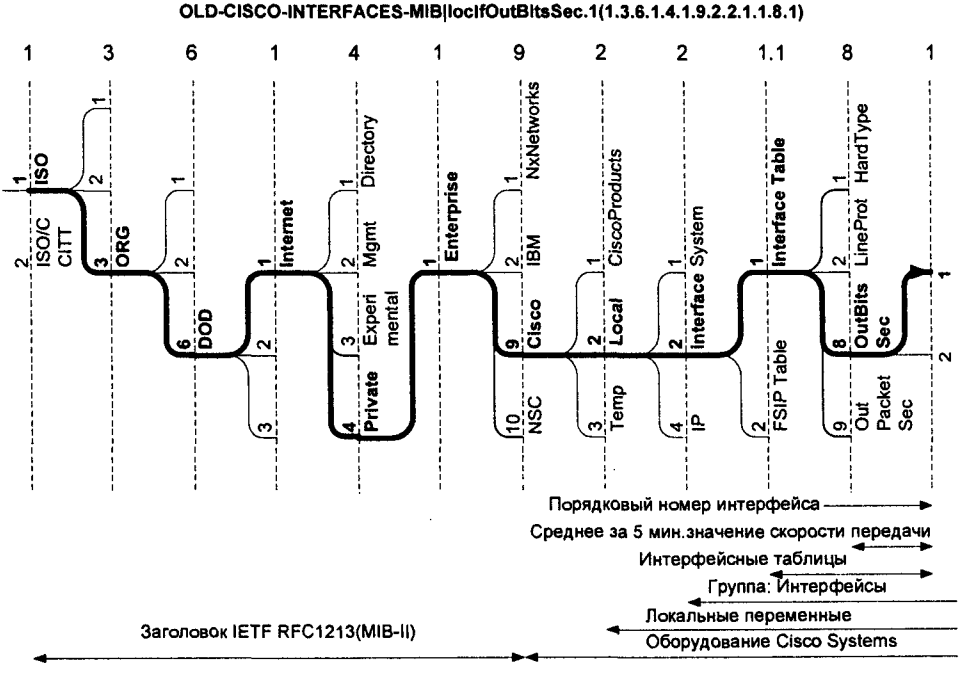


Рис. 16.1. Пример формирования идентификатора управляемого объекта MIB

Дерево MIB содержит также и универсальные ветви, на которых размещаются описания локальных объектов управления, обязательных для конкретного типа сетевых устройств. Так, например, ветвь Mgmt (четвертый уровень MIB) содержит описания локальных переменных, которые используются для сетевого управления. Переменные системной группы, идентификатор которой 1.3.6.1.2.1.4, могут быть использованы для мониторинга и управления процессами обработки данных сетевого уровня OSI ISO 7498 (маршрутизация) на управляемых по протоколу SNMP узлах сети Интернет.

Описание управляемых объектов MIB

Описание объектов управления MIB производится в соответствии со стандартными правилами, определенными для структур управляющей информации — *SMI* (Structure of Management Information) протокола SNMP. Правила описания структур SMI представляют собой подмножество универсальных правил ASN.1, которые специально адаптированы для использования с протоколом SNMP. Основные принципы и способы описания управляемых объектов MIB приведены в IETF RFC 2578 Structure of Management Information Version 2 (SMIv2). April 1999. (Status: STANDARD.

В соответствии со спецификацией SMI для описания управляемого объекта MIB могут быть использованы компоненты следующих типов:

- *целочисленное значение* (SMIv2-Integer32 или SMIv2-INTEGER) — десятичное число в диапазоне –2147483648—2147483647);
- *строка символов* (SMIv2-OCTET STRING) — упорядоченная последовательность длиной 65 535 байтов, которая может быть использована для формирования текстовых компонентов управляемых объектов, таких, например, как описания и справочные данные;
- *идентификатор объекта* (SMIv2-OBJECT IDENTIFIER) — значение, сформированное в соответствии с правилами ASN.1. В дополнение к этому значению для каждого из компонентов управляемого объекта может быть определено не более 128 вторичных идентификаторов;
- *последовательность бит* (SMIv2-BITS construct), которая может содержать поименованные битовые поля различной длины;
- *сетевой адрес протокола IP* (SMIv2-IP Address) — используется для указания адреса в стандартном десятично-точечном формате;
- *счетчики* (SMIv2-Counter32 и SMIv2-Counter64) — представляют собой неотрицательные целые числа, которые циклически изменяются в пределах от минимального значения, т. е. 0 до максимального значения. Максимальное значение, допустимое для объекта MIBv1 данного типа — $2^{32} - 1$. Для описания объектов MIBv2 могут быть также использованы счетчики с максимальным значением $2^{64} - 1$;

- *измерители* (SMIv2-Gauge32) — неотрицательные целые числа, которые могут увеличиваться или уменьшаться в пределах, которые устанавливаются максимальным и минимальным допустимыми значениями измерителя, соответственно. Примером измерителя является длина очереди, состоящей из выходных пакетов;
- *метки времени* (SMIv2-Time Ticks) — представляют собой продолжительность временного интервала, прошедшего от момента наступления некоторого события, измеренную в сотых долях секунды;
- *произвольное значение* (SMIv2-Opaque) — этот тип используется для описания переменных, которые определены нестандартным образом. Основное назначение данного типа состоит в обеспечении совместимости со спецификациями предыдущих версий;
- *натуральное значение* (SMIv2-Unsigned32) — представляет собой неотрицательное десятичное число в диапазоне (0—2 147 483 647);
- *табличные значения* (SMIv2-Conceptual Tables) — используются для представления переменных векторного и матричного типов. Для указания конкретного элемента табличного компонента должны быть использованы дополнительные индексы. Так, например локальная переменная `locIfOutBitsSec.1` (1.3.6.1.4.1.9.2.2.1.1.8.1) представляет собой первый элемент таблицы `locIfOutBitsSec` (1.3.6.1.4.1.9.2.2.1.1.8). Определение значений элементов таблицы выполняется с использованием ключевого словосочетания SEQUENCE OF с указанием типа определяемого массива.

Определение любого управляемого объекта SNMP содержит формализованное описание этого объекта, которое разделено на пять отдельных полей при помощи ключевых слов:

- OBJECT — заголовок определения имени объекта;
- Syntax — заголовок определения типа объекта;
- Definition — заголовок текстового описания объекта;
- Access — заголовок определения разрешенного типа доступа к объекту;
- Status — заголовок состояния объекта.

В листинге 16.1 приведен пример заголовка формального описания управляемого объекта SNMP.

Листинг 16.1. Заголовок формального описания управляемого объекта SNMP

```
OBJECT-TYPE MACRO ::=
BEGIN
  TYPE NOTATION ::= "SYNTAX" type (TYPE ObjectSyntax)
                                  "ACCESS" Access
                                  "STATUS" Status
```

```
  VALUE NOTATION ::= value (VALUE ObjectName)
  Access ::= "read-only"| "read-write"
                        | "write-only"
                        | "not-accessible"
  Status ::= "mandatory"| "optional"
                        | "obsolete"
END
```

При построении описаний управляемых объектов частной ветви в дополнение к описанным ранее типам переменных могут быть использованы некоторые специфические типы, определенные конкретным производителем оборудования. В листинге 16.2 приведен пример фрагмента формального описания MIB для интерфейса маршрутизатора Cisco Systems. Файл OLD-CISCO-INTERFACES-MIB.my (**ftp://ftp-sj.cisco.com/pub/mibs/supportlists/c2611/c2611-supportlist.html**). В этом листинге маркером выделены определения представленной ранее переменной `locIfOutBitsSec` (1.3.6.1.4.1.9.2.2.1.1.8).

Листинг 16.2. Фрагмент формального описания MIB для интерфейса маршрутизатора Cisco Systems

```
    1. Определение табличной переменной
lifTable OBJECT-TYPE
                    SYNTAX  SEQUENCE OF LifEntry
                    ACCESS  not-accessible
                    STATUS  mandatory
                    DESCRIPTION
"A list of interface entries."
                    ::= { linterfaces 1 }
    2. Определение дополнительных объектов для интерфейса Cisco
lifEntry OBJECT-TYPE
                    SYNTAX LifEntry
                    ACCESS  not-accessible
                    STATUS  mandatory
                    DESCRIPTION
"A collection of additional objects in the cisco interface."
                    INDEX { ifIndex }
                    ::= { lifTable 1 }
                LifEntry ::=
                    SEQUENCE {
                        locIfHardType
                            DisplayString,
                              ...
                        locIfInPktsSec
                            INTEGER,
```

```
                    locIfOutBitsSec
                        INTEGER,
                          ...
                    locIfDribbleInputs
                        Counter
                         }
                          ...
```

3. Определение среднего значения скорости передачи бит через интерфейс

```
locIfOutBitsSec OBJECT-TYPE
                    SYNTAX  INTEGER
                    ACCESS  read-only
                    STATUS  mandatory
                    DESCRIPTION
"Five minute exponentially-decayed moving average of output bits per
second."
                    ::= { lifEntry 8 }
```

Взаимодействие компонентов SNMP

Информационный обмен управляющей станции с управляемыми объектами SNMP осуществляется с использованием принципов клиент-серверного взаимодействия. Функции сервера в данном случае выполняет управляемый объект со встроенным агентом управления SNMP, функции клиентов SNMP выполняют управляющие станции.

Большинство операций SNMP выполняется в форме запросов, поступающих от клиента для чтения или записи значений внутренних переменных управляемого объекта. При этом допускается, что часть переданных запросов не будет обработана, например, из-за отсутствия у клиента прав доступа к запрошенным переменным. В подобных случаях SNMP-сервер должен возвратить запрашивающей системе уведомление о невозможности получения запрошенных данных.

В табл. 16.2 приведен перечень основных сообщений, которые используются при обмене между клиентом и сервером в протоколе SNMP.

Таблица 16.2. *Сообщения протокола SNMP*

Наименование	Назначение	Источник
GET-REQUEST	Чтение значения внутренней переменной сервера	Клиент
GET-NEXT-REQUEST	Чтение очередного значения из таблицы переменных	Клиент

Таблица 16.2 (окончание)

Наименование	Назначение	Источник
RESPONSE	Ответ сервера на любой из запросов GET, принятых от клиента	Сервер
GET-BULK-REQUEST	Чтение всех значений из таблицы серверв	Клиент
SET-REQUEST	Устновка значения внутренней переменной сервера	Клиент
SNMPV2-TRAP	Уведомление клиентв о самопроизвольном изменении состояния внутренней переменной нв сервере	Сервер
INFORM-REQUEST	Уведомление клиента о наступлении ожидаемого события нв сервере	Сервер

Для передачи сообщений протокола SNMP используется протокол транспортного уровня UDP (User Datagram Protocol). Каждое сообщение SNMP передается независимо от других сообщений, в виде самостоятельной UDP-дейтаграммы.

Дейтаграммы UDP, содержащие запросы SNMP, адресуются в порт 161. Информационные сообщения SNMP, такие, например, как уведомления, принимаются на порт 162.

Административное ограничение границ действия протокола SNMP выполняется путем явного указания имени сообщества управляемых объектов (SNMP-community) во всех передаваемых сообщениях этого протокола. Сервер SNMP принимает к исполнению только запросы, которые поступают от клиентов, находящихся в одном сообществе с ним. Таким образом, имя сообщества (по умолчанию — public) определяет границы сетевой области, в пределах которой SNMP-агенты находятся под единым административным управлением.

Примечание

Использование переменных SNMP-community обеспечивает лишь базовый уровень информационной безопасности при взаимодействии с управляемыми объектами. Для дальнейшего повышения информационной безопасности следует использовать решения, предлагаемые в IETF RFC 3414 (User-based Security Model USM).

В ответных сообщениях, которые формируются при выполнении поступающих от клиента запросов, SNMP-сервер указывает состояние выполнения запроса (SNMP-Error-Status). В табл. 16.3 приведен перечень основных сообщений об ошибках, которые могут возникнуть при выполнении запросов на SNMP-сервере.

Таблица 16.3. Сообщения об ошибках при выполнении SNMP-запросов

Наименование	Назначение	Код
NO.ERROR	Запрос выполнен без ошибок	0
TOO.BIG	Принятое сообщение имеет недопустимый размер	1
NO.SUCHNAME	Объект отсутствует на сервере	2
BAD.VALUE	Недопустимое значение для переменной	3
READ.ONLY	Переменная доступна только для чтения	4
GEN.ERR	Ошибка неопределенного типа	5
NO.ACCESS	Нет доступа к переменной	6
WRONG.TYPE	Недопустимый тип переменной	7
WRONG.LENGTH	Недопустимая длина переменной	8
WRONG.ENCODING	Недопустимая кодировка переменной	9
WRONG.VALUE	Недопустимое значение связываемой переменной	10
NO.CREATION	Переменная не может быть создана	11
INCONSISTENT.VALUE	Несовместимое значение для переменной	12
RESOURCE.UNAVAILABLE	Запрошенный ресурс отсутствует	13
COMMIT.FAILED	Присвоение не выполнено	14
UNDO.FAILED	Отмена операции не выполненв	15
AUTHORIZATION.ERROR	Несанкционированное обращение к переменной	16
NOT.WRITABLE	Переменная не доступна для записи	17
INCONSISTENT.NAME	Несовместимое имя переменной	18

Мониторинг состояния сети

Для обеспечения возможности управления компонентами мультисервисной ЛВС по протоколу SNMP на этих компонентах необходимо выполнить дополнительные настройки в соответствии с рекомендациями фирмы-производителя оборудования.

В листинге 16.3 приведен пример — фрагмент конфигурационного файла настройки протокола SNMP на коммутаторе Catalyst Cisco Systems. Маркером на листинге отмечены индивидуальные настройки, которые должны быть изменены при практической реализации.

Листинг 16.3. Фрагмент конфигурационного файла настройки протокола SNMP на коммутаторе Catalyst Cisco Systems

```
    1. Настройка SNMP-агента на коммутаторе:
snmp-server community no-secure RO
    2. Обеспечение передачи уведомлений (SNMP — traps) о наступлении
       различных событий на сервере:
snmp-server enable traps snmp authentication linkdown linkup coldstart
     // Передача оповещений о подключениях по SNMP, изменениях
     // состояния канала и рестартах коммутатора
snmp-server enable traps config
      // Передача оповещения об изменении конфигурации коммутатора
    3. Обеспечение передачи оповещений на выбранную управляющую станцию
snmp-server host 27.16.17.44 trap no-secure
```

Собственно управление и мониторинг состояния компонентов мультисервисных ЛВС осуществляется специальными программными комплексами-платформами сетевого управления. Такие программные комплексы помимо мониторинга и оперативного управления сетевыми компонентами позволяют реализовать множество вспомогательных функций, среди которых в первую очередь следует выделить:

- измерение и регистрацию основных характеристик ЛВС;
- графическое отображение состояния сетевых устройств;
- реализацию систем оперативного оповещения.

Примером платформы сетевого управления является программный комплекс *SNMPc* компании Castle Rock Computing, Inc. Все последующие иллюстрации данного раздела были получены в ЛВС, управляемой NMS на основе одной из ранних версий программного обеспечения SNMPc. В листинге 16.4 приведены оповещения SNMP, сформированные специально настроенным (см. листинг 16.3) коммутатором Catalyst Cisco Systems. Приведенные далее оповещения зафиксированы рабочей станцией, на которой установлено программное обеспечение Castle Rock SNMPc.

Листинг 16.4. Оповещения SNMP, сформированные коммутатором Catalyst Cisco Systems

```
Minor    12/22/2006 22:07:09 Catalyst Authentication Failure
// Попытка несанкционированного доступа — уровень тревоги — низкий
Normal   11/29/2006 09:59:01 Catalyst Interface 19 Link Up Trap
// Подключение абонента к интерфейсу № 19
Minor    12/25/2006 08:22:07 Catalyst Interface 19 Link Down Trap
// Отключение абонента от интерфейса № 19 - уровень тревоги — низкий
```

На управляющей станции NMS все оповещения, принятые от различных компонентов ЛВС, упорядочиваются по идентификатору компонента и времени поступления оповещающего сообщения. Изначально с каждым из таких сообщений в NMS связан один из возможных уровней тревожности. Администратор NMS при желании может изменить этот уровень, а также определить перечень дополнительных действий, которые будут выполняться системой при получении оповещений данного уровня:

- передача сообщений во всплывающем окне на управляющей станции;
- формирование звукового сигнала;
- отправка SMS-сообщения на мобильный телефон администратора.

Одним из основных компонентов платформы сетевого управления является обозреватель локальных переменных SNMP — *MIB Browser*. При помощи MIB Browser можно получить доступ к любому компоненту сетевого устройства, управляемого по протоколу SMNP. На рис. 16.2 приведен пример использования встроенного обозревателя MIB для чтения значения локальной переменной `locIfOutBitsSec.1` (1.3.6.1.4.1.9.2.2.1.1.8.1) из маршрутизатора Cisco Systems.

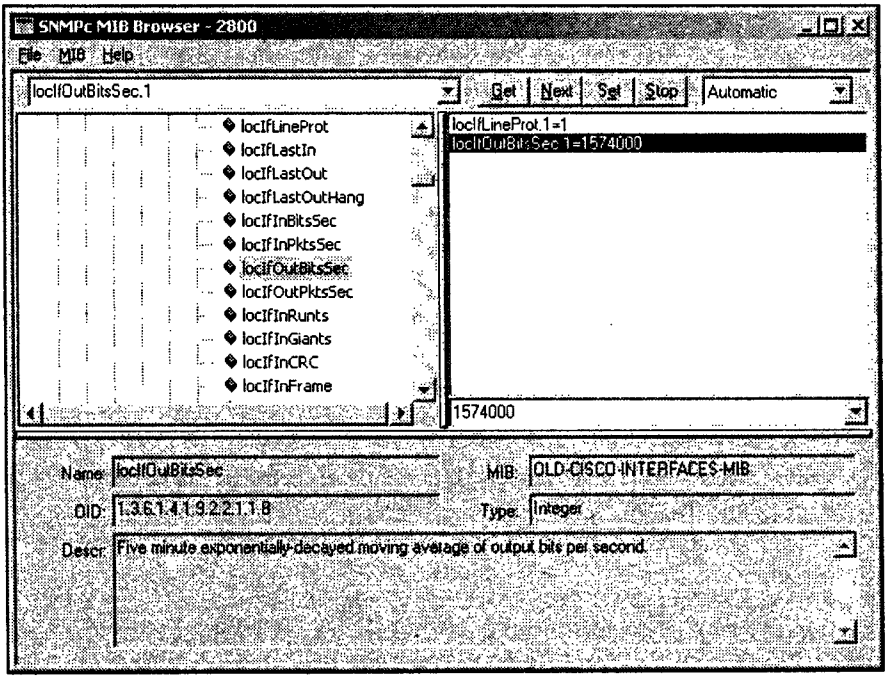


Рис. 16.2. Чтение значения локальной переменной `locIfOutBitsSec.1` (1.3.6.1.4.1.9.2.2.1.1.8.1)

Интерфейс взаимодействия с обозревателем MIB позволяет выполнять навигацию в базе управляемых объектов, считывать и устанавливать значения локальных переменных. Так в представленном на рис. 16.2 случае скорость отправки данных через первый интерфейс (Fast Ethernet 0/0) маршрутизатора Cisco Systems 2811 составляет 1,574 Кбит/сек.

Бесспорно, однако, что графическое представление локальных переменных более наглядно отображает изменяющиеся во времени характеристики управляемого объекта. К характеристикам такого типа можно отнести:

- информационную скорость передачи и приема данных через интерфейсы управляемого объекта;
- объем оперативного запоминающего устройства (ОЗУ), который используется для обработки передаваемых данных на управляемом объекте;
- процент загрузки центрального процессора на управляемом объекте;
- количество ошибок, зафиксированных при получении данных на заданный интерфейс управляемого объекта.

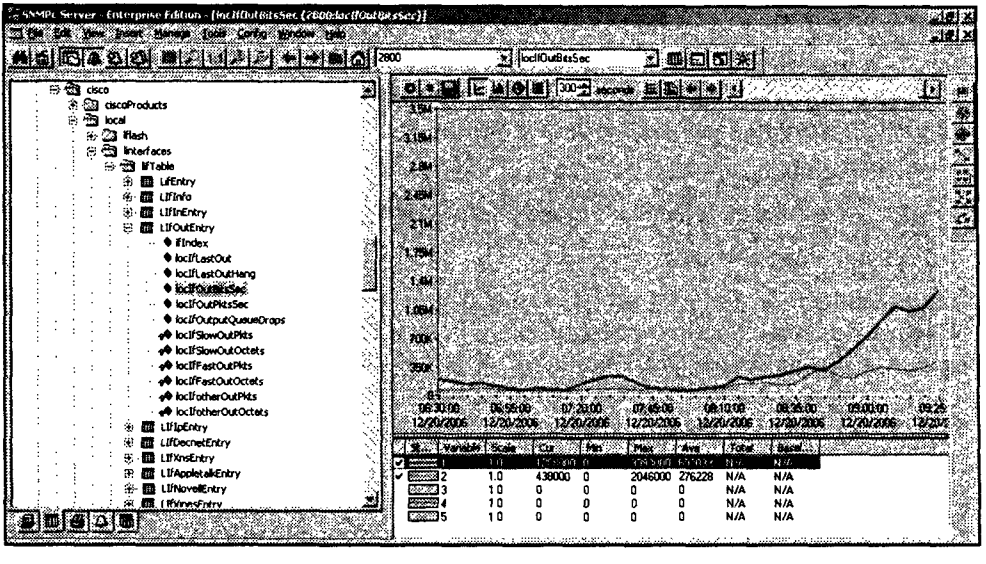


Рис. 16.3. График изменения скорости отправки данных через интерфейс маршрутизатора Cisco Systems

Именно по этой причине программное обеспечение NMS, как правило, содержит богатый набор инструментов, которые позволяют строить разнообразные графики изменяющихся во времени характеристик управляемого объекта. На рис. 16.3 представлен пример построения графика изменения во времени скорости отправки данных через интерфейс маршрутизатора Cisco

Systems с использованием программного обеспечения SNMPc компании Castle Rock Computing, Inc.

Для того, чтобы построить подобный график в данной или какой-либо другой NMS, вполне достаточно указать идентификатор MIB отображаемого объекта — в данном случае — locIfOutBitsSec.1(1.3.6.1.4.1.9.2.2.1.1.8.1). Поскольку локальная переменная `locIfOutBitsSec` представляет собой таблицу, индексом которой является номер интерфейса (см. листинг 16.2), на одном графике могут быть показаны характеристики всех интерфейсов. Так утолщенной линией на рис. 16.3 представлен график изменения скорости отправки данных через интерфейс Fast Ethernet 0/0, а тонкой линией — через интерфейс Fast Ethernet 0/1. Поскольку другие интерфейсы не используются для передачи информации, данный график одновременно отображает и скорость приема, и скорость передачи данных в ЛВС для этого маршрутизатора.

Анализ и документирование трафика мультисервисной ЛВС

Анализ трафика, передаваемого в мультисервисной ЛВС, который может производиться как периодически, так и на постоянной основе, представляет собой оперативный контроль и документирование основных параметров проходящего через сеть информационного потока. Учет и анализ проходящего через ЛВС трафика выполняется для решения следующих задач:

- обеспечения безопасности информационного обмена в ЛВС;
- определения узких мест и локализации неисправностей;
- тарификации абонентов.

Для выполнения документирования и анализа сетевого трафика могут быть использованы разнообразные методы и решения. Например, как это было показано в предыдущем разделе настоящей главы, для мониторинга интенсивности передаваемого или принимаемого информационного потока могут быть использованы решения, основанные на протоколе SNMP.

Практика, однако, показывает, что возможности анализа и документирования трафика, предоставляемые стандартными решениями, далеко не всегда способны удовлетворить потребности администраторов ЛВС. Так, например, решения на основе протокола SNMP не позволяют выполнить детальный — с точностью до адресов сетевого уровня или номеров портов транспортного уровня — анализ трафика. Именно поэтому для выполнения анализа и документирования трафика зачастую применяются нестандартные средства и технические решения.

Применение технологии Netflow, разработанной компанией Cisco Systems, дает возможность производить детальный анализ потоков в сетях, построенных на базе оборудования Cisco.

Технология NetFlow

Разработанная компанией Cisco Systems технология NetFlow включает в себя специальные программные модули сбора и предварительной обработки информации на маршрутизаторах и многоуровневых коммутаторах, функционирующих под управлением операционной системы Cisco IOS, а также комплекс технических решений, которые позволяют собирать и накапливать эту информацию на внешних серверах-накопителях (NetFlow-Collector).

Примечание

Сбор и агрегирование информации о проходящем трафике не является единственной функцией технологии NetFlow. Эта технология также может быть использована для реализации распределенной маршрутизации в сети, содержащей процессор многоуровневой коммутации (MLS-RP) и несколько коммутирующих узлов (MLS-SE).

В основе технологии NetFlow лежит понятие потока — однонаправленной последовательности блоков данных, которые передаются между двумя сетевыми приложениями. Ключевая идея технологии NetFlow состоит в том, что все блоки данных, принадлежащие одному потоку, обрабатываются в сети по единому алгоритму.

Принадлежность блока данных к тому или иному потоку однозначно определяется по значениям семи ключевых признаков:

- IP-адресу отправителя трафика (IP source address);
- IP-адресу получателя трафика (IP destination address);
- порту протокола транспортного уровня отправителя трафика (Source port);
- порту протокола транспортного уровня получателя трафика (Destination port);
- типу протокола сетевого уровня (Layer 3 protocol type);
- классу обслуживания передаваемого трафика (Class of Service);
- входному интерфейсу (Input interface).

При получении каждого нового пакета эти признаки (поля) сравниваются с записями потоков, находящимися в буферной области ОЗУ (NetFlow Cache) сетевого устройства, которое выполняет функцию экспорта информации о проходящих через него потоках. По итогам этого сравнения либо увеличивается количество переданных данных у одного из существующих потоков, либо в буферном ОЗУ создается новый поток. Поток завершается, и соответствующая ему запись удаляется из NetFlow Cache в двух случаях, когда:

- превышен интервал ожидания очередного блока данного потока (15 сек);
- время существования потока в NetFlow Cache превысило предельное значение (30 мин).

Записи завершенных потоков группируются и отправляются в виде UDP-дейтаграммы на выбранный порт коллектора, где происходит дальнейшая обработка, фильтрация, агрегация и хранение полученных данных.

Собираемые таким образом данные могут быть использованы как для тарификации абонентского трафика, так и для детального исследования текущего состояния сети.

Особенности применения NetFlow

Основные отличия технологии NetFlow от большинства технологий, которые используются для сбора информации о трафике ЛВС, заключаются в том, что экспортер выполняет предварительное агрегирование данных и передает их на коллектор по своей инициативе. Такая идеология обмена между экспортером и коллектором трафика существенно снижает объем передаваемых данных и обеспечивает возможность дальнейшей модернизации построенных систем анализа трафика.

В листинге 16.5 приведен фрагмент конфигурационного файла для анализа проходящего трафика по технологии NetFlow на маршрутизаторе Cisco Systems.

Листинг 16.5. Настройка анализа проходящего трафика по технологии NetFlow на маршрутизаторе Cisco Systems

```
    1. Установить номер версии ПО NetFlow, которая будет использована
       для сбора информации о проходящем трафике
ip flow-export version 5
    2. Определить сетевой адрес NetFlow-коллектора и номер порта,
       на который будут отправляться агрегированные данные
ip flow-export destination 27.16.17.38 9996
    3. Определить критерии и формы оперативного отображения наиболее
       активных потребителей трафика
ip flow-top-talkers
 top 10
 sort-by bytes
 match destination address aa.bb.cc.0 255.255.255.0
    4. Включить на интерфейсе функции сбора информации о проходящем
       трафике по технологии NetFlow
interface FastEthernet0/1
ip route-cache flow
```

При настройке NetFlow нужно учитывать, что эта технология обеспечивает сбор информации о входящих в интерфейсы маршрутизатора потоках. Поэтому для сбора статистики об уходящем из маршрутизатора трафике коман-

ду `ip route-cache flow` следует поставить на тот интерфейс, через который трафик приходит на маршрутизатор.

В листинге 16.6 приведены результаты выполнения диагностических команд экспорта агрегированной информации NetFlow на маршрутизаторе Cisco Systems.

Листинг 16.6. Результаты выполнения диагностических команд экспорта агрегированной информации NetFlow на маршрутизаторе Cisco Systems

```
#sh ip flow export
Flow export v5 is enabled for main cache
  Exporting flows to 27.16.17.38 (9996)
  Version 5 flow records
  561714196 flows exported in 18869136 udp datagrams
  0 flows failed due to lack of export packet
  10 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures

#sh ip cache flow
// Общая информация об агрегированных потоках
IP Flow Switching Cache, 278544 bytes
  257 active, 3839 inactive, 564909077 added
...
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
// Суммарные данные NetFlow по типам активных приложений
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec)
Idle(Sec)
--------   Flows   /Sec     /Flow  /Pkt     /Sec     /Flow      /Flow
TCP-Telnet 86647   0.0       268   101       5.4     472.7       9.8
TCP-FTP    558045  0.1         9    71        1.2       4.2       8.2
TCP-FTPD 341434    0.0        92  1024        7.3       5.9       2.9
TCP-WWW 230192435  53.5       10   916     564.9        1.8       4.0
TCP-SMTP 22242537   5.1       16   266      85.9        5.7       4.5
UDP-DNS 1473358     0.3        2    64       0.7        3.7      15.4
UDP-NTP  4242874    0.9        1    76       0.9        0.0      15.4
UDP-TFTP  46801     0.0        6    54       0.0       29.8      15.4
// Информация  NetFlow по активным потокам
'SrcIf SrcIPaddress    DstIf     DstIPaddress  Pr SrcP DstP  Pkts
 Fa0/1  62.118.203.158  Fa0/0  aa.bb.cc.65     06 0F0E 01BD     2
```

```
Fa0/1   194.67.57.206    Fa0/0   aa.bb.cc.51      06 07F9 0A20    1
Fa0/1   24.205.1.12      Fa0/0   aa.bb.cc.68      11 0035 FD35    1
Fa0/1   195.70.36.75     Fa0/0   aa.bb.cc.107     06 0019 0DA6    55
Fa0/1   74.107.63.250    Fa0/0   aa.bb.cc.97      11 77F8 F36D    1
Fa0/1   62.118.252.32    Fa0/0   dd.ee.ff.5       06 07E4 06F4    23
Fa0/1   194.67.57.206    Fa0/0   aa.bb.cc.70      06 01BB 5C16    1
Fa0/1   87.229.19.226    Null    dd.ee.ff.207     06 10A5 0599    1
Fa0/1 205.188.248.199    Fa0/0   aa.bb.cc.173     06 0050 072F    1
Fa0/1 85.235.40.37        Null   aa.bb.cc.54      01 0000 0303    1
```

В последнем фрагменте листинга 16.6 приведены обобщенные данные об активных потоках, которые находятся в NetFlow Cache. Каждый из этих потоков характеризуется следующими параметрами:

- SRCIF — интерфейс, через который принимается трафик;
- SRCIPADDRESS — адрес источника трафика;
- DSTIF — интерфейс, через который отправляется трафик;
- DSTIPADDRESS — адрес получателя трафика;
- PR — относительный приоритет пакета IP для данного потока;
- SRCP — порт протокола транспортного уровня отправителя трафика;
- DSTP — порт протокола транспортного уровня получателя трафика;
- PKTS — количество пакетов, переданных в данном потоке.

Номера портов протокола транспортного уровня в данном листинге приведены в шестнадцатеричной системе счисления, 0050 в данном случае соответствует приложению протокола HTTP, а 0035 — DNS. Потоки, направленные в виртуальный интерфейс Null, представляют трафик блокированных абонентов.

В листинге 16.7 приведен результат выполнения диагностической команды оперативного контроля передаваемого трафика на маршрутизаторе Cisco Systems `show ip flow top-talkers`. Эта команда показывает 10 наиболее активных на текущий момент времени потребителей трафика и может быть использована для диагностических целей. Дополнительные настройки маршрутизатора, необходимые для корректного выполнения этой команды, приведены в п. 3 листинга 16.5.

Листинг 16.7. Результат выполнения диагностической команды оперативного контроля передаваемого трафика на маршрутизаторе Cisco Systems

```
#sh ip flow top-talkers
SrcIf   SrcIPaddress    DstIf  DstIPaddress     Pr SrcP DstP  Bytes
Fa0/1   81.19.80.164    Fa0/0  aa.bb.cc.99      06 0050 F776  7741K
```

```
Fa0/1    217.16.18.76     Fa0/0   aa.bb.cc.144    06 0050 FFAE   4035K
Fa0/1    81.91.32.122     Fa0/0   aa.bb.cc.96     2F 0000 0000   2090K
Fa0/1    80.75.85.26      Fa0/0   aa.bb.cc.96     2F 0000 0000    325K
Fa0/1    85.235.40.36     Fa0/0   aa.bb.cc.53     11 43FA 5CB0    191K
Fa0/1    85.12.58.3       Fa0/0   aa.bb.cc.131    06 D65B FB2A    188K
Fa0/1    62.168.250.90    Fa0/0   aa.bb.cc.144    32 215E 03B7    152K
Fa0/1    27.16.17.38      Fa0/0   aa.bb.cc.36     06 0017 0418    134K
Fa0/1    217.212.227.28   Fa0/0   aa.bb.cc.121    06 0050 0DBB     89K
Fa0/1    84.42.2.2        Fa0/0   aa.bb.cc.131    06 0050 C108     86K
10 of 10 top talkers shown. 228 of 298 flows matched
```

Благодаря данным, собираемым при помощи NetFlow, становится возможным в реальном масштабе времени отслеживать состояние сети, своевременно выявляя сетевые атаки и паразитную деятельность. Помимо этого, накопленные данные, полученные посредством NetFlow, могут существенно облегчить процесс поиска неисправностей в мультисервисной ЛВС.

Принципы и программное обеспечение тарификации абонентов

К основным требованиям, которые предъявляются к программному обеспечению тарификации абонентов, в первую очередь относятся:

- высокий уровень информационной безопасности;
- экономичное использование ресурсов и надежность функционирования;
- обеспечение возможности доступа к хранимой информации через сети общего пользования.

Наиболее важным в данном случае следует считать первое из перечисленных требований, поскольку процесс анализа и документирования трафика имеет не только технические, но также экономические, юридические и нравственные аспекты.

Именно поэтому программное обеспечение, которое используется для тарификации абонентского трафика, должно быть сертифицировано на предмет соответствия специфическим требованиям, предъявляемым к программным системам подобного рода. Промышленные программные системы тарификации абонентского трафика, как правило, представляют собой закрытые программные комплексы, основной частью которых является база данных абонентского трафика. Способы формирования и обслуживания этой базы данных, которые в каждой системе тарификации могут быть различными, не являются предметом обсуждения в данном издании. Вместе с тем в подобных системах обычно широко применяются универсальные программные модули для сбора и предварительной обработки полученных от накопителей данных

о передаваемом трафике. Применение промежуточных программных модулей позволяет сделать систему анализа и документирования трафика более универсальной благодаря возможности совместного использования различных форм и способов предварительного накопления данных.

Так, например, в качестве модуля промежуточной обработки может быть использовано программное обеспечение *NeTraMet*, общие принципы построения которого приведены в IETF RFC 2123: Traffic Flow Measurement: Experiences with NeTraMet Category: Informational: March 1997.

Настройка правил предварительной обработки трафика, принимаемого на коллектор, в комплексе NeTraMet может быть выполнена при помощи скрипта, текст которого приведен в листинге 16.8.

Листинг 16.8. Настройка правил предварительной обработки трафика, принимаемого на коллектор, в комплексе NeTraMet — (файл IP.SRL)

```
net = ( aa.bb.cc.0/24, dd.ee.ff.0/24);
// Определение адресов сетей, для которых будет осуществляться
// сбор трафика
 IF SourcePeerType == IP
  SAVE;
ELSE
  IGNORE; # Not Ip
// Определение правил предварительной обработки
IF DestPeerAddress == net || SourcePeerAddress == net
{
 SAVE DestPeerAddress/32;
  SAVE SourcePeerAddress/32;
 SAVE SourceTransAddress;
 SAVE DestTransAddress;
 SAVE SourceASN;
 SAVE DestASN;
}
ELSE
  IGNORE; # Not account net
COUNT;
FORMAT
// Определение формата результирующего потока
  FlowRuleSet FlowIndex FirstTime SourcePeerAddress DestPeerAddress
SourceASN DestASN
  ToOctets FromOctets ToPDUs FromPDUs SourceInterface DestInterface
SourceTRansAddress DestTransAddress SourceKind;
STATISTICS;
SET 5;
```

После трансляции файла IP.SRL в системе создается файл IP.RULES, который и выполняет предварительную обработку всех завершенных потоков NetFlow, принимаемых на порт 9996 коллектора NeTraMet. В результате этой обработки на сервере сформируется файл IP.FLW, в котором будет храниться информация о завершенных потоках NetFlow, прошедших процедуру предварительной обработки. В листинге 16.9 приведен пример итогового файла NetFlow/NeTraMet.

Листинг 16.9. Пример итогового файла NetFlow/NeTraMet (IP.FLW)

```
##NeTraMet v4.3:  -c600 -r /usr/local/netflow/ip.rules  127.0.0.1
udp-9996  300000 flows  starting at 15/12/2006 23:55:01
#Format: flowruleset flowindex firsttime sourcepeeraddress
destpeeraddress sourceasn destasn tooctets fromoctets topdus frompdus
sourceinterface destinterface sourcetransaddress desttransaddress
sourcekind
#Time: 16/12/2006 00:00:00 127.0.0.1 Flows from 2778529781 to 2778589772
#Ruleset: 15  5 /usr/local/netflow/ip.rules  ip.rules
#Stats: aps=18 apb=0 mps=1141 mpb=0 lsp=0 avi=100.0 mni=97.5 fiu=4329
frc=3954 gci=10 rpp=1.5 tpp=0.5 cpt=1.0 tts=262139 tsu=4250
...
15 156767
219495360 212.23.90.34 aa.bb.cc.144 0 0 398 0 5 0 0 0 80 63759 0
15 156768
3638692033 212.23.90.34 aa.bb.cc.144 0 0 2640 0 6 0 0 0 80 63760 0
15 156769
3630330079 89.108.82.91 aa.bb.cc.119 0 0 3387 0 7 0 0 0 80 60680 0
15 156771
3630330083 89.108.82.91 aa.bb.cc.119 0 0 2813 0 6 0 0 0 80 60681 0
15 156772
3638744799 89.108.82.91 aa.bb.cc.119 0 0 3388 0 6 0 0 0 80 60682 0
```

Состав и порядок записи основных компонентов файла IP.FLW практически полностью повторяет структуру исходного потока NetFlow. В дальнейшем этот файл может быть использован для импортирования текущей информации в базу данных абонентского трафика.

Функциональное программное обеспечение

Функциональные компоненты программного обеспечения предназначены для непосредственного выполнения разнообразных форм мультисервисного об-

мена между абонентами ЛВС. Таким образом, компоненты этой категории программного обеспечения непосредственно выполняют формирование и прием потокового трафика мультисервисных ЛВС.

К числу наиболее распространенных компонентов этой группы следует отнести:

- программные IP-телефоны и коммуникаторы, которые предназначены для обеспечения различных форм оперативного обмена между абонентами мультисервисных ЛВС;
- программные комплексы обработки телефонных вызовов, представляющие собой набор программных средств, позволяющий автоматизировать процесс телефонного обмена при помощи решений пакетной телефонии;
- программные формирователи и приемники мультимедийных потоков, задача которых состоит в организации различных форматов сетевого телевизионного или радиовещания.

Клиентские приложения VoIP

Голосовые приложения были первыми потоковыми приложениями, которые появились и стали использоваться в локальных сетях. Программные голосовые компоненты могут использовать стандартные внешние акустические устройства (микрофон и звуковые колонки) и центральный процессор персонального компьютера для формирования и приема голосового потокового трафика. Некоторые программные системы, впрочем, для организации и приема телефонного вызова обеспечивают возможность использования также и специализированных компьютерных приставок, таких, например, как USB-телефоны.

Назначение и состав программного call-центра

Основные принципы построения центра обработки телефонных вызовов (call-центра) были приведены в *главе 2* настоящего издания. Построение такого центра позволяет не только понизить стоимость приема и ускорить обработку телефонных вызовов, но и существенно повысить эффективность производственной деятельности сотрудников компании и перейти на качественно новый уровень обслуживания клиентов. Следует отметить, что программная реализация существенно сокращает затраты на построение и обслуживание такого телефонного центра.

В качестве примера подобной системы можно рассмотреть свободно распространяемую версию программного комплекса обработки телефонных вызовов компании NCH Swift Sound.

Основными компонентами программного центра обработки телефонных вызовов компании NCH Swift Sound являются:

- виртуальная офисная телефонная станция — *Axon*;
- программный телефон — *Express Talk*;
- телефонный ассистент — *IVM Telephone Answering Attendant*;
- многоканальная звукозаписывающая система — *VRS* (Voice Recording System).

Виртуальная телефонная станция

Программное обеспечение *Axon* компании NCH Swift Sound обеспечивает реализацию основных функций телефонной станции на персональном компьютере, работающем под управлением операционной системы MS Windows. Это программное обеспечение позволяет выполнять прием телефонных вызовов, поступающих по сети Интернет, с использованием SIP в качестве протокола управления вызовом. Программный комплекс Axon позволяет также выполнять обработку и маршрутизацию поступающих телефонных вызовов на программные и аппаратные IP-телефоны, а также, при наличии соответствующих адаптеров — на обычные аналоговые телефонные аппараты. Следует учитывать, что многие основные и дополнительные функции телефонной станции Axon реализуются совместно с такими программами компании NCH Swift Sound, как: IMS On-Hold Messages System, VRS (Voice Recording System), IVM Call Attendant, IVR с Voice Mail Software.

Программное обеспечение Axon является связующим элементом центра обработки вызовов компании NCH Swift Sound и предоставляет следующие возможности:

- прием входящих телефонных вызовов по сети Интернет или сети беспроводной телефонной связи;
- неограниченное число внутренних или внешних линий;
- поддержку всех функций стандартных офисных АТС, например, таких как маршрутизация, удержание и регистрация вызова;
- полный набор инструментов для построения интерактивного голосового меню, который содержит различные администраторы фоновых мелодий и редакторы речевых приглашений;
- управление телефонными вызовами по универсальному открытому протоколу SIP (RFC 3261);
- возможность совместного использования с программными (Soft phones) и аппаратными (USB phones) реализациями IP-телефонов различных производителей;

- возможность совместного применения со стандартными аппаратными VoIP-шлюзами;
- управление всеми функциями виртуальной АТС через встроенный WWW-интерфейс.

Подключение виртуальной АТС к телефонной сети может быть выполнено через внешний аппаратный или программный шлюз PSTN-VoIP (SIP).

В листинге 16.10 приведен пример настройки сервера доступа AS5300 для подключения виртуальной АТС на телефонный номер PSTN.

Листинг 16.10. Настройка сервера доступа AS5300 для подключения виртуальной АТС на телефонный номер PSTN

```
    1. Определение параметров исходящего вызова сервера доступа AS5300
dial-peer voice 9503 voip
    2. Расширение номера для исходящего вызова
 destination-pattern 9997
    3. Тип протокола управления вызовом (SIPv2)
 session protocol sipv2
    4. IP-адрес виртуальной АТС
 session target ipv4:aa.bb.cc.2
    5. Тип используемого кодека
 codec g711alaw
    6.Параметры приема факсимильных сообщений
 fax-relay ecm disable
 fax rate 14400
 fax protocol t38 ls-redundancy 0 hs-redundancy 0
 ip precedence 5
 no vad
```

Для обеспечения приема телефонных вызовов на виртуальной АТС должны быть зарегистрированы абоненты. На рис. 16.4 приведен пример совместной настройки программного телефона Express Talk и виртуальной АТС Axon для приема входящих с расширением 9997 телефонных вызовов.

Особенность приведенной конфигурации виртуальной АТС заключается в том, что программное обеспечение Soft phones, в данном случае — Express Talk, выполняется на той же рабочей станции, что и программное обеспечение самой виртуальной АТС. Именно поэтому при регистрации программного телефона на SIP-сервере использован виртуальный IP-адрес этой рабочей станции — 127.0.0.1. Естественно, что у всех внешних телефонов, подключаемых к этой АТС, в поле **Server (SIP Proxy or Virtual P&X)** меню **Lines** должен быть указан реальный IP-адрес рабочей станции, на которой выполняется программное обеспечение виртуальной АТС.

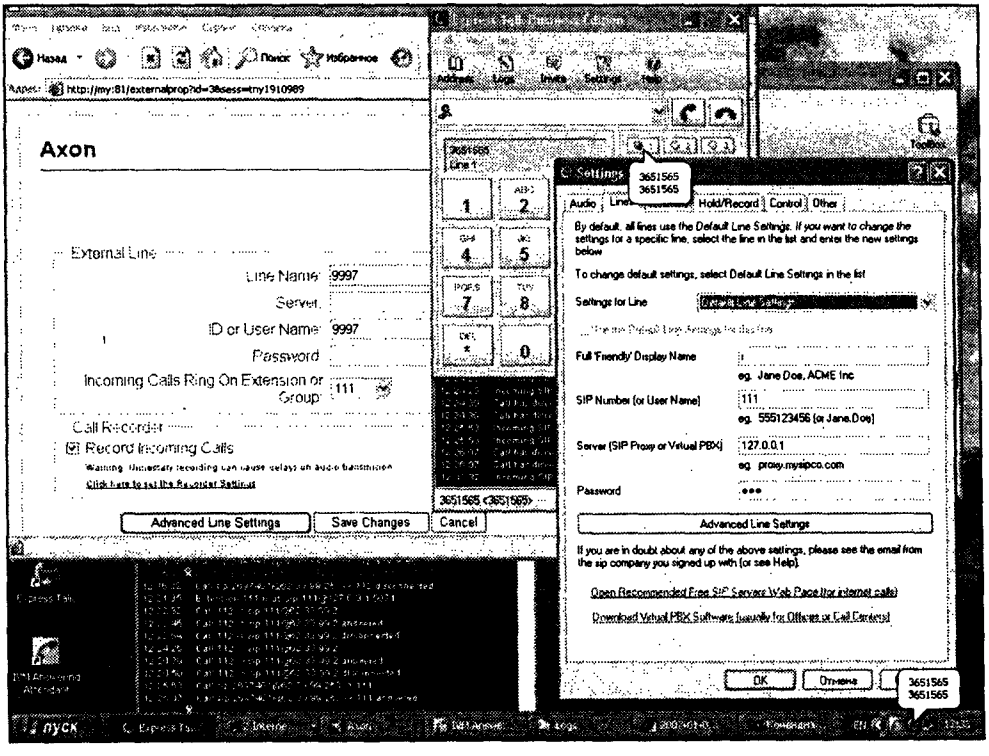


Рис. 16.4. Настройка программного телефона и виртуальной АТС для приема входящих телефонных вызовов

Программный IP-телефон

В листинге 16.11 приведен фрагмент протокола регистрации программного IP-телефона Express Talk на телефонной станции SIP Axon.

Листинг 16.11. Протокол регистрации программного IP-телефона Express Talk на телефонной станции SIP Axon

```
-------------------------------------------------------------
19:11:44UDP Packet Sent to 127.0.0.1:5060 >>>>>>>>>>>>>>>>>>>>>
REGISTER sip:127.0.0.1 SIP/2.0
Via: SIP/2.0/UDP 127.0.0.1:5072;rport;branch=z9hG4bK22132
Max-Forwards: 20
To: <sip:111@127.0.0.1>
From: <sip:111@127.0.0.1>;tag=9845
Call-ID: 1167829908-2132-COMPANY-NNT5XT8@127.0.0.1
CSeq: 4 REGISTER
```

```
Contact: <sip:111@127.0.0.1:5072>;expires=3600;q=0.90
Authorization: Digest username="9999",realm="axon@company-nnt5xt8",
nonce="v43400qaq29911w",uri="sip:127.0.0.1",response="b12e3be52e9998dd4b0
a39ff42b16002",opaque=""
User-Agent: Express Talk 2.02
Content-Length: 0
-----------------------------------------------------------------
19:11:45 UDP Packet Received from 127.0.0.1:5060 <<<<<<<<<<<<<<<<
SIP/2.0 200 OK
Via: SIP/2.0/UDP 127.0.0.1:5072;rport;branch=z9hG4bK22132
To: <sip:111@127.0.0.1>
From: <sip:111@127.0.0.1>;tag=9845
Call-ID: 1167829908-2132-COMPANY-NNT5XT8@127.0.0.1
CSeq: 4 REGISTER
User-Agent: Axon 1.09
Contact: <sip:111@127.0.0.1:5072>;expires=3600;q=0.90
Content-Length: 0
```

Маркером в приведенном листинге отмечены стандартные сообщения протокола SIP, которые были сформированы в процессе регистрации программного IP-телефона Express Talk на телефонной станции SIP Axon.

Программные телефоны, в дополнение к стандартному набору функций, реализуемых на стандартных аналоговых и цифровых телефонных аппаратах — прием, удержание, переадресация входящего вызова, обеспечивают возможность реализации и дополнительных функций:

- запись телефонного разговора в файл;
- автоматическое подключение к системе голосовой почты;
- прямой вызов удаленного абонента по адресу IP или SIP.

На рис. 16.5 приведен результат выполнения телефонного вызова с программного телефона на номер 9999@local host, т. е. на этот же самый программный телефон. Программное обеспечение Soft phone зафиксировало входящий вызов на линии 1, и, поскольку он остался без ответа, программный телефон по истечении установленного интервала времени автоматически активизировал систему голосовой почты. В данном случае эта система реализована с использованием программы "Телефонный ассистент" — IVM Answering Attendant v.4.01.

Вспомогательные программы систем пакетной телефонии

Проигрыватель IMS On-Hold Messages Player обеспечивает редактирование, хранение и администрирование приветственных и информационных голосо-

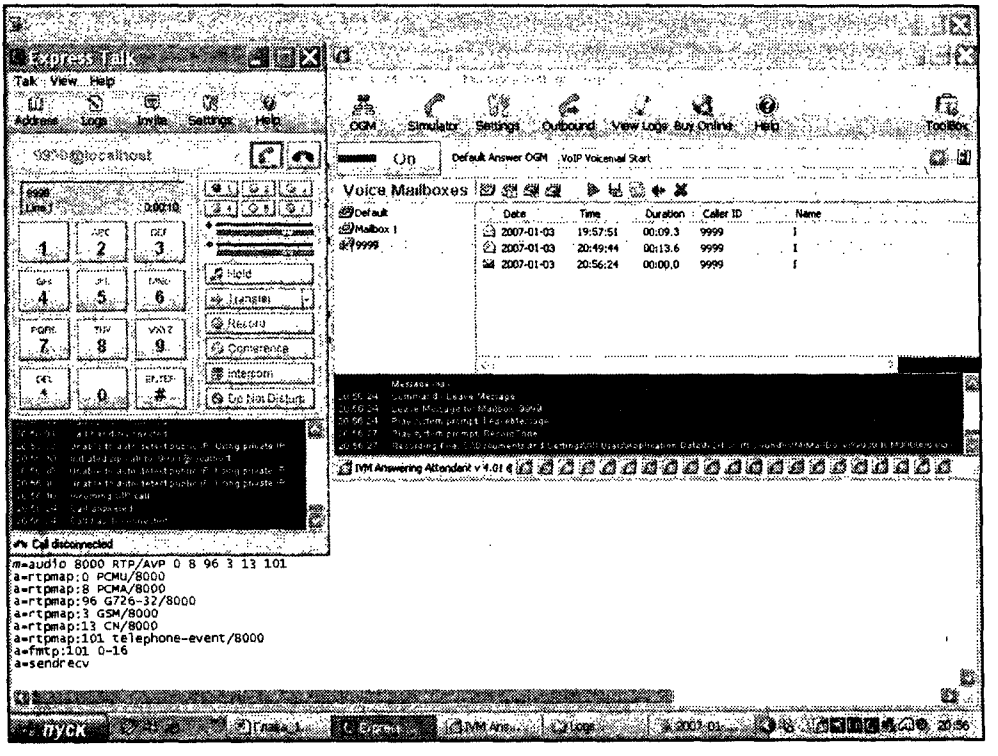


Рис. 16.5. Выполнение и прием телефонного вызова на Soft Phone Express Talk

вых сообщений, а также фонового музыкального сопровождения, воспроизводимого в период переадресации или удержания входящего телефонного вызова.

Программное обеспечение "Телефонный ассистент" — IVM Answering Attendant предназначено для реализации двух вспомогательных функций:

- приема, регистрации, редактирования и администрирования сообщений голосовой почты;
- создания, редактирования и выполнения программ речевого меню — *IVR* (Interactive Voice Response).

В качестве администратора голосовой почты программа "Телефонный ассистент" — IVM Answering Attendant обеспечивает построение архива принятых сообщений. Эта программа также позволяет выполнять такие операции над записями архива сообщений, как упорядочивание, редактирование и отправка по электронной почте.

Системы речевого меню, реализованные с помощью специальных IVR-программ, являются удобным и эффективным способом реализации динамиче-

ских процедур обработки телефонных вызовов. Эти системы могут быть использованы для автоматического информирования и обеспечения навигации звонящего абонента, что позволит существенно повысить эффективность деятельности телефонных операторов.

Многоканальная звукозаписывающая система — *VRS Recording System* компании NCH Swift Sound предназначена для создания и обслуживания архива голосовых сообщений и телефонных разговоров. Программное обеспечение VRS позволяет выполнять одновременную запись голосовых потоков, которые поступают по 32 независимым каналам. В случае совместного применения с виртуальной телефонной станцией Axon, десять каналов VRS могут быть использованы для автоматической регистрации телефонных разговоров, выполняемых на этой станции. Остальные регистрирующие каналы могут применяться для разнообразных технологических целей, например, для регистрации служебного обмена в системах с речевым вызовом.

Звукозаписывающая система VRS также обеспечивает возможность автоматического экспорта хранящейся информации в форматах, которые используются в стандартных системах MS Access и Dbase.

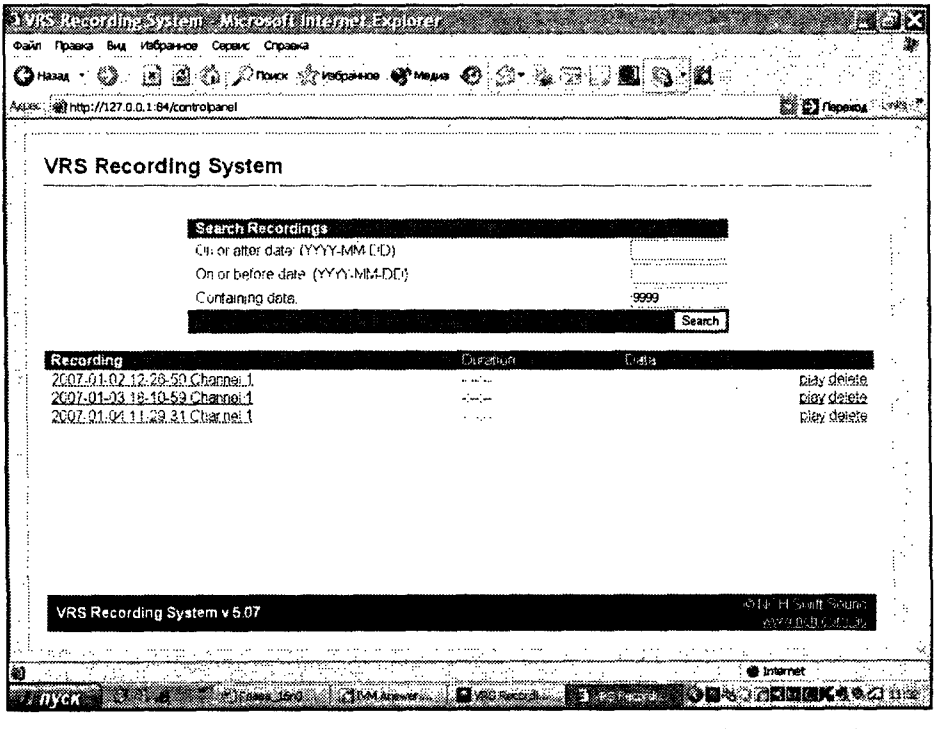


Рис. 16.6. Интерфейс удаленного управления звукозаписывающей системой VRS по протоколу HTTP

Удаленное взаимодействие абонентов ЛВС с многоканальной звукозаписывающей системой выполняется по протоколу IP:

- подключение источников звукового потока осуществляется через порт 4080 TCP;
- администрирование архива голосовых сообщений реализуется через порт 84 по протоколу HTTP.

Для обеспечения безопасности информационного обмена в процессе организации удаленного доступа к архивам голосовых сообщений в многоканальной звукозаписывающей системе VRS Recording System предусмотрены использование многоуровневых паролей и защита передаваемых сообщений по протоколу MD5. На рис. 16.6 приведен внешний вид интерфейса удаленного управления многоканальной звукозаписывающей системой по протоколу HTTP.

В примере, приведенном на рис. 16.6, удаленный доступ по протоколу HTTP к архиву многоканальной звукозаписывающей системой был выполнен с той же рабочей станции, на которой размещается этот архив (IP-адрес 127.0.0.1).

Серверные и клиентские видеоприложения

Основными задачами серверных и клиентских видеоприложений ЛВС являются прием и формирование видеопотоков. В качестве входного потока видеосервер ЛВС может, в зависимости от особенностей реализации, использовать потоки от разнообразных источников:

- локально доступный файл;
- внешний носитель данных, например, аудио- или видеодиск;
- поток данных от внешнего видеосервера;
- поток данных от непосредственно подключенного аудио- или видеоустройства.

Принятый от основного источника видеосигнал сервер преобразует в форму, которая необходима для трансляции этого сигнала через ЛВС. Для обеспечения правильного приема видеопотока, сформированного сервером, на программном обеспечении приемников потока, которое установлено на рабочих станциях ЛВС, должны быть выполнены соответствующие изменения настроек основных параметров. Задача определения настроек еще более усложняется в том случае, если в сервере используется для одновременного вещания несколько программ, или когда в сети одновременно действуют несколько видеосерверов. Для обеспечения навигации в среде потоков и автоматической настройки приемников видеопотока может быть использован протокол анонсирования потоков — *протокол SAP* (Session Announcement

Protocol), который позволяет всем серверам передавать служебную информацию о транслируемых ими потоках.

Протокол анонсирования потоков — протокол SAP

Основные положения протокола анонсирования потоков приведены в документе IETF RFC 2974: Session Announcement Protocol: October 2000 Category: Experimental.

Протокол SAP предназначен для применения в тех мультисервисных сетях Интернет, в которых применяется групповой режим информационного обмена с использованием адресов из диапазона (224.0.0.0—239.255.255.255). Информация о потоках транслируется по сети в виде специальных сообщений, которые групповой сервер (SAP-Announcer) передает для клиентов (SAP-Listener). Сообщения протокола SAP также передаются с использованием группового режима адресации абонентов, причем адрес назначения этого сообщения определяется диапазоном групповых адресов, который сервер использует для трансляции потоков:

- для анонсирования вещания в диапазоне глобально уникальных групповых адресов Интернета (Global Scope) используется адрес 224.2.127.254;
- для анонсирования вещания в диапазоне локально уникальных групповых адресов Интернета (Administrative Scope) используется последний адрес диапазона — в данном случае — 239.255.255.255.

Нормативный документ RFC 2974 предписывает также, что анонсирующие поток сообщения протокола SAP должны быть адресованы в порт 9875, а значение времени жизни (TTL) у дейтаграмм протокола IP, которые используются для их доставки по сети Интернет, должно быть установлено равным 255.

Каждый приемник группового трафика обязательно должен принимать и анализировать анонсирующие сообщения для диапазона Global Scope. В дополнение к этому, приемник группового трафика, размещенный в административно ограниченной зоне, должен принимать анонсирующие сообщения SAP, передаваемые для этой локальной зоны.

Анонсирующие сообщения протокола SAP передаются периодически. Период повторения сообщений выбирается таким образом, чтобы совокупная пропускная способность, которая используется для передачи этих сообщений, не превысила значение 4000 бит/сек. В то же время, в соответствии с требованиями, приведенными в документе RFC 2974, максимальный период повторения анонса для каждого из потоков не должен превышать 300 сек.

В протоколе SAP используются сообщения двух типов:

- сообщения анонсирования сессии (Session announcement);
- сообщения завершения сессии (Session deletion).

В анонсирующем SAP-сообщении содержится адрес источника, а также разнообразные идентификаторы потока, такие, например, как наименование канала, название передачи (фильма). На рис. 16.7 приведен пример последовательности сообщений протокола SAP, анонсирующих группу мультисервисных потоков, транслируемых в ЛВС Ethernet с использованием групповых адресов Administrative Scope IP.

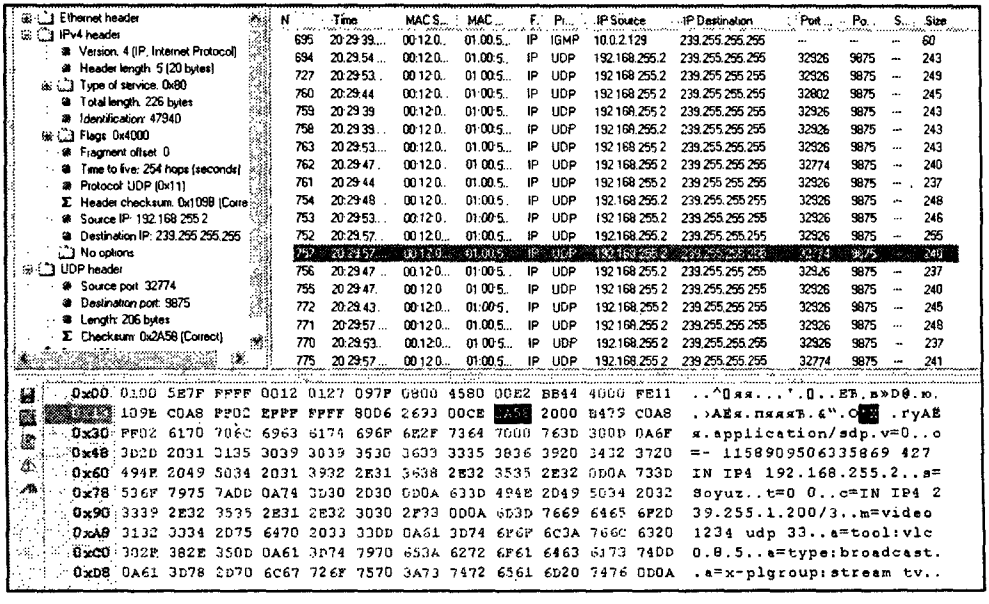


Рис. 16.7. SAP-сообщения, анонсирующие потоки, транслируемые с использованием групповых IP-адресов

При получении анонсирующего сообщения приемник мультимедийного потока формирует соответствующую запись в буферном запоминающем устройстве (SAP-Cache). Данные этой записи в дальнейшем могут быть использованы приемниками мультимедийных потоков для обеспечения выбора принимаемого потока. На представленном рисунке источником потоков и формирователем SAP-сообщений является сервер 192.168.255.2. Поскольку вещание абонентам в данной ЛВС Ethernet выполняется с использованием режима групповой (Multicast) адресации в диапазоне административно ограниченных адресов (239.0.0.0—239.255.255.255), то анонсирующие SAP-сообщения направляются по последнему адресу этого диапазона (239.255.255.255). Выделенное на рис. 16.7 SAP-сообщение анонсирует видеопоток станции "Soyuz", который транслируется по адресу 239.255.1.200 (порт 1234) с использованием программного обеспечения VLC v.0.8.5.

Сообщения завершения сессии формируются в том случае, если сервер прекратил вещание одного из ранее анонсированных потоков. При получении

этого сообщения приемник потокового трафика удаляет соответствующую запись из SAP-Cache, что делает невозможным автоматическое подключение к завершенному потоку.

Формирователь мультимедийных потоков VLC

Основной задачей программного обеспечения видеосервера является формирование мультимедийных потоков. Типичным примером такого формирователя потоков является программное обеспечение *VLC* (VideoLAN Client) от VideoLAN Team (**www.VideoLAN.org**). Программное обеспечение VLC может быть использовано и распространяется на условиях, которые отмечены в Основной Лицензии GNU, и представляет собой универсальную программу, которая сочетает в себе функции формирователя и приемника мультимедийных потоков.

Серверный компонент VLC обеспечивает прием мультимедийных потоков в реальном масштабе времени от разнообразных источников, например, от внешнего видеосервера по сети Интернет или от непосредственно подключенного аудио- или видеоустройства. Принимаемый поток сервер VLC может

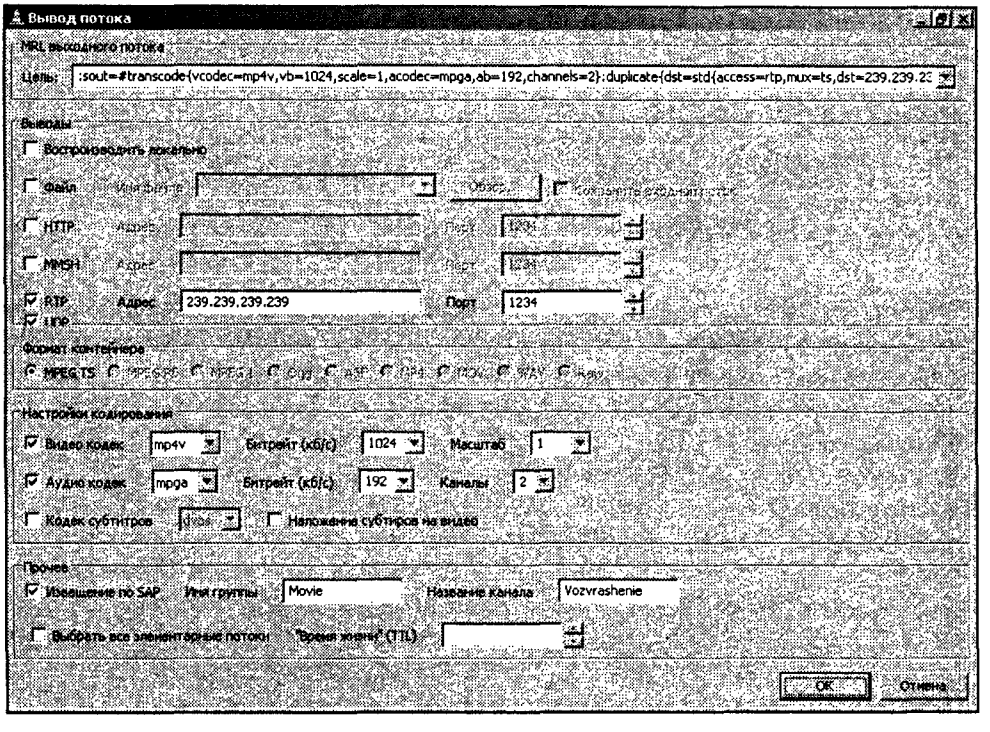


Рис. 16.8. Настройки сервера VLC для трансляции видеопотока в режиме групповой адресации Интернета

сохранять в виде файла или транслировать в ЛВС. На рис. 16.8 приведен пример настройки сервера VLC для трансляции видеопотока с использованием режима групповой адресации Интернета.

В данном случае анонсирование формируемого сервером видеопотока (видеофильм "Возвращение") выполняется с использованием протокола SAP.

Применение данного режима вещания оказывает наименьшую нагрузку на центральный процессор сервера и оборудование *ЛВС*, поскольку вне зависимости от количества приемников видеотрафика сервер формирует только один поток UDP со следующими характеристиками:

- адрес назначения — 239.239.239.239;
- порт назначения протокола транспортного уровня UDP — 1234;
- размер дейтаграммы — 1370 байт (полезная нагрузка — 1328 байт);
- период следования дейтаграмм — 80 мсек.

Программный мультимедийный плеер VLC

Программный приемник VLC, который также входит в комплект программного обеспечения VideoLAN Team (**www.VideoLAN.org**), позволяет выполнять прием и воспроизведение на персональном компьютере мультисервисных потоков, представленных в различных форматах. В частности, VLC позволяет принимать потоки и воспроизводить файлы, представленные в фор-

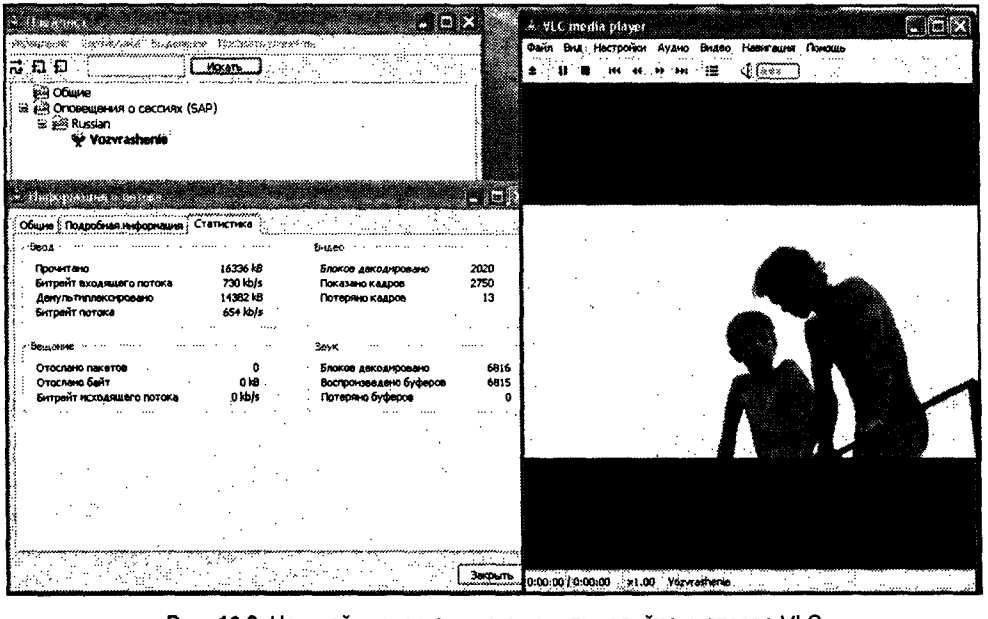


Рис. 16.9. Настройки программного мультимедийного плеера VLC

матах MPEG-1, MPEG-2, MPEG-4, DivX, XviD и многих других. Исключение могут составлять некоторые закрытые форматы, которые используются для кодирования потоков, передаваемых в коммерческих сетях.

Для приема внешнего видеопотока удобно использовать список воспроизведения, куда автоматически заносятся все анонсируемые мультисервисные потоки. На рис. 16.9 представлен пример настройки программного мультимедийного плеера VLC для приема видеопотока, сформированного видеосервером VLC (см. предыдущий раздел).

Как видно на представленном рисунке, в данном случае на приемнике достаточно только выбрать один из источников видеопотока, остальные настройки выполняются автоматически.

Рекомендации по использованию программных компонентов

Далее приведены наиболее общие рекомендации по выбору и использованию программных компонентов мультисервисных ЛВС.

При выборе программных компонентов для реализации приложений мультисервисных ЛВС в первую очередь следует обратить внимание на следующие характеристики и параметры программного обеспечения:

- использование открытых стандартов для передачи данных;
- применение открытых и распространенных стандартов для представления данных.

Применение открытых стандартов для передачи данных во внедряемом программном обеспечении не только защищает инвестиции, но и обеспечивает возможность дальнейшего развития и модернизации компонентов проектируемой системы. Кроме того, использование открытых стандартов позволит более точно и грамотно оценить на этапе проектирования стоимость предлагаемых или получаемых услуг. Отсутствие должного внимания к этому аспекту проектирования может привести к непредвиденному увеличению расходов на эксплуатацию системы.

Так, например, высокое качество передачи голосового сигнала в программной системе пакетной телефонии легко может быть обеспечено за счет негласного применения кодека с предельно малым коэффициентом сжатия данных или отказа от подавления пауз. При этом, однако, высокое качество будет обеспечиваться только на широких каналах, которые будут очень неэффективно использоваться. Именно поэтому программные компоненты с нестандартными протоколами передачи и представления данных следует внедрять только после всестороннего и внимательного тестирования.

Перечень сокращений

A

AAL (ATM Adaptation Layer)

Уровень адаптации сетевых протоколов ATM. Назначение уровня адаптации состоит в определении процедур, в соответствии с которыми выполняется прямое и обратное преобразование блоков данных сетевого и последующих уровней OSI ISO 7498 в поток ячеек ATM.

Access Layer

Уровень доступа является самым нижним уровнем в иерархических ЛВС. Активное оборудование, размещенное на этом уровне, обеспечивает непосредственное подключение абонентов к ресурсам сети.

ACL (Access Control Lists)

Списки управления доступом предназначены для разделения трафика по атрибутам канального, сетевого и транспортного уровней эталонной модели OSI-7 (ISO 7498).

ACK (Acknowledge)

Стандартное сообщение, используемое в процедурах квитирования для обозначения позитивного подтверждения.

ADPCM (Adaptive Differential Pulse Code Modulation)

Технология адаптивной дифференциальной импульсно-кодовой модуляции (АДИКМ), которая применяется для повышения эффективности цифрового кодирования аналогового сигнала.

ANSI (American National Standards Institute)

Национальная стандартизирующая организация США.

ATM (Asynchronous Transfer Mode)

Технология, которая при интеграции разнородного трафика в едином канале обеспечивает строгое соблюдение соглашений о качестве обслуживания.

ATSC (Advanced Television Systems Committee)

Американская спецификация цифрового телевидения.

AP (Access Point)

Точка доступа — устройство, которое используется для организации информационного обмена между абонентами беспроводной сети.

APON (ATM PON)

Технология построения пассивной оптической сети, ориентированной на использование принципов ATM для интеграции разнородного трафика.

ARP (Address Resolution Protocol)

Протокол, используемый для установления взаимного соответствия адресов канального и сетевого уровней в сетевых технологиях множественного доступа к среде передачи данных.

Auto-Negotiation

Процедура, используемая для автоматического согласования параметров информационного обмена в сегментах ЛВС Ethernet, построенных на основе UTP.

B

BIFS (Binary Format for Scenes)

Двоичный формат, который позволяет описывать и синтезировать видеоизображения в спецификации MPEG-4.

BPDU (Bridge Protocol Data Units)

Блоки данных канального уровня, в которых размещаются служебные сообщения, формируемые коммутаторами Ethernet.

BPON (Broadband PON)

Общее наименование технологий построения пассивных оптических сетей, ориентированных на использование принципов ATM для интеграции разнородного трафика (ITU-T G.983).

BRI (Basic Rate Interface)

Пакет услуг, который обеспечивает абоненту сети ISDN возможность использования двух цифровых каналов 64 Кбит/сек для передачи данных или трафика цифровой телефонии.

BS (Base Station)

Базовая станция, которая используется для подключения беспроводных абонентов по технологии IEEE 802.16.

C

CAM (Content Addressable Memory)

Тип запоминающего устройства, в котором для формирования адреса используется значение хранимых данных.

CARP (Common Address Redundancy Protocol)

Протокол предназначен для обеспечения динамического резервирования серверов и шлюзов, которые работают под управлением операционных систем, развиваемых в рамках проекта OpenBSD.

CDP (Cisco Discovery Protocol)

Протокол, который используется сетевыми устройствами Cisco Systems для обмена служебной информацией.

CGMP (Cisco Group Management Protocol)

Протокол, в соответствии с которым осуществляется информационное взаимодействие между маршрутизатором и коммутатором компании Cisco Systems для обеспечения эффективного распространения группового трафика.

CELP (Code Excited Linear Prediction)

Алгоритм линейной экстраполяции, который применяется для повышения эффективности цифрового кодирования аналогового сигнала.

CHAP (Challenge Handshake Authentication Protocol)

Вспомогательный протокол, который применяется для установления подлинности партнеров PPP-соединения и использует 3-этапный алгоритм квитирования.

CIF (Common Intermediate Format)

Типовой (промежуточный) формат видеоизображения.

CIR (Committed Information Rate)

Значение соответствует информационной скорости, которая была согласована с пользователем для выполнения обмена по отдельному виртуальному каналу.

CM (Cable Modem)

Кабельный модем — устройство, которое используется абонентом или группой абонентов для передачи данных в мультисервисных коаксиальных сетях и сетях HFC.

CMTS (Cable Modem Termination System)

Транслирующая станция кабельных модемов, которая обеспечивает передачу данных абонентам мультисервисных коаксиальных сетей и сетей HFC в частотном формате сетей кабельного телевидения.

Codec (*Кодек* — кодер/декодер)

Устройство или программа, выполняющая функцию взаимного преобразования потокового трафика в последовательность кодов.

Core Layer

Верхний уровень иерархической структуры ЛВС. Активное оборудование, размещенное на этом уровне, обеспечивает управление обменом между всеми абонентами мультисервисной вычислительной сети, а также взаимодействие абонентов ЛВС с внешними сетями и системами.

CoS (Class of Service)

Класс обслуживания. Используется в системах DiffServ для указания принадлежности трафика к одной из групп с гарантированными значениями сетевых ресурсов, выделяемых на его обработку.

CSMA/CD (Carrier Sense Multiple Access/Collision Detection)

Метод множественного доступа к среде передачи данных с прослушиванием несущей и обнаружением коллизий, положенный в основу сети Ethernet.

CWND (Congestion Window)

Обозначение переменной, которая в протоколе STCP используется для указания размера окна перегрузки.

D

Datagram (Дейтаграмма)

Термин, используемый для обозначения блока данных сетевого уровня Интернета.

DCE (Data Circuit terminal Equipment)

Тип последовательного интерфейса линейного оборудования передачи данных.

DDL (Description Definition Language)

Язык формирования описаний, который используется для определения правил построения описаний мультимедийных объектов MPEG-7.

Default Gateway

Термин, используемый для обозначения соседнего узла, которому следует направлять дейтаграммы, адресованные в сети, не указанные в таблице маршрутизации.

Dense mode

Режим трансляции группового трафика по сети, при использовании которого трафик не получают только те узлы, которые явным образом отказались от его приема.

DCT (Discrete Cosine Transform)

Стандартный алгоритм дискретного гармонического преобразования растрового видеоизображения.

DHCP (Dynamic Host Configuration Protocol)

Протокол, обеспечивающий динамическое определение основных сетевых параметров оконечного узла Интернета.

Digital Item

Понятие, применяемое для обозначения разнообразных форм цифровых продуктов — мультимедийных объектов, например, фильмов или музыкальных композиций, представленных в электронном виде. Это понятие непосредственно связано с понятием пользователя цифрового продукта (Digital Item User), поскольку мультимедийный объект является цифровым продуктом только по отношению к потенциальному пользователю.

DiffServ (Differentiated Service Model)

Модель раздельного обслуживания. Схема обеспечения качества обслуживания в сети Интернет, которая предполагает разделение обрабатываемого трафика на классы с установленным уровнем QoS.

Distribution Layer

Уровень распределения является промежуточным уровнем в иерархической структуре вычислительной сети. Активное оборудование, размещенное на этом уровне, предназначено для решения задач управления информационным обменом между функциональными группами абонентов мультисервисной ЛВС.

DLCI (Data-Link Connection Identifier)

Идентификатор логического канала, который используется в качестве номера виртуального канала в сетях, основанных на технологии Frame Relay.

DOCSIS (Data-Over-Cable Service Interface Specifications)

Наименование комплекса спецификаций, определяющих основные принципы передачи данных в системах кабельного телевидения (КТВ).

DSG (DOCSIS Set-top Gateway)

Наименование типовой приставки, обеспечивающей получение дополнительных услуг абонентом сетей кабельного телевидения (КТВ), построенных с использованием технологий DOCSIS.

DSSS (Direct Sequence Spread Spectrum)

Модуляционная схема прямого расширения спектра — способ формирования сигнала, использовавшийся в ранних версиях спецификаций Wi-Fi.

DVB (Digital Video Broadcasting)

Европейская спецификация цифрового вещания.

DVMRP (Distance Vector Multicast Routing Protocol)

Протокол маршрутизации группового трафика, построенный аналогично классическим протоколам типа Distance — Vector.

E

EAPOL (Extensible Authentication Protocol Over LAN)

Расширяемый протокол аутентификации, применяемый для управления доступом абонентов к ресурсам ЛВС.

EAS (Emergency Alert System)

Система приема и передачи сообщений о чрезвычайных ситуациях.

EFM (Ethernet In The First Mile)

Проект, в рамках которого разрабатывались технические решения по применению технологий Ethernet в сетях абонентского доступа.

EIA (Electronic Industries Alliance)

Национальная организация США, объединяющая производителей телекоммуникационного оборудования. Задачей EIA является развитие американского рынка высоких технологий.

Ethernet

Технология, предложенная корпорацией Xerox для построения локальных вычислительных сетей с использованием метода CSMA/CD для обеспечения множественного доступа к среде передачи данных.

EPG (Electronic Program Guide)

Система, которая обеспечивает прием информации о программах кабельного телевидения.

F

FCS

Обозначение поля контрольной суммы в заголовке блока данных протокола канального уровня.

FDD (Frequency Division Duplex)

Способ организации дуплексного режима в беспроводных сетях, при использовании которого принимаемый и передаваемый сигналы разделяются по частоте.

FDDI (Fiber Distributed Data Interface)

Технология построения резервированных магистральных межсетевых соединений на основе волоконно-оптических линий связи.

FRAD (Frame Relay Access Device)

Устройства, используемые для подключения абонентов в сетях, построенных на основе технологии Frame Relay.

Frame (Кадр)

Стандартный термин, используемый для обозначения блоков данных протоколов канального уровня (SLIP, PPP).

Frame Relay

Обеспечивает информационное взаимодействие на физическом и канальном уровне OSI ISO 7498 и позволяет реализовать динамическое разделение ресурсов канала между абонентскими приложениями. Применяется как альтернатива выделенным линиям при построении сетей доступа в Интернет.

FTP (File Transfer Protocol)

Протокол прикладного уровня, применяемый для организации файлового обмена в сети Интернет.

FTTB (Fiber-To-The-Building)

Схема построения сети доступа, в которой волоконно-оптический кабель используется только на магистральном участке, а подключение абонентов выполняется по выделенным медным линиям.

FTTC (Fiber-To-The-Curb)

Схема, используемая для подключения разрозненных абонентов, находящихся на значительном расстоянии до центрального офиса или точки предоставления услуги.

FTTH (Fiber-To-The-Home)

Схема построения сети доступа, которая предполагает применение только волоконно-оптических каналов и может быть реализована с использованием принципов PON.

FTTN (Fiber-To-The-Node)

Схема, в которой для подключения разрозненных абонентов, находящихся на значительном удалении от центрального офиса или точки предоставления услуги, могут быть использованы удаленные терминалы, установленные на промежуточных узлах.

FXS (Foreign Exchange Station)

Абонентский аналоговый интерфейс телефонной станции.

FXO (Foreign Exchange Office)

Станционный аналоговый интерфейс телефонной станции.

G

Gatekeeper (Привратник)

Устройство, предназначенное для управления шлюзами и терминалами H.323 в части организации и обслуживания вызовов, регистрации, аутентификации и авторизации пользователей и т. д.

Gateway (Шлюз)

Общий термин, применяемый для обозначения сетевых узлов, обеспечивающих информационное взаимодействие между несколькими сетями.

GARP (Generic Attribute Registration Protocol)

Протокол, определяющий совокупность процедур, которые могут быть использованы для формирования и распространения по сетям прозрачных мостов дополнительных параметров (атрибутов).

GBIC (Gigabit Interface Converter)

Встраиваемый конвертер стандартного формата, который может быть использован для организации на коммутаторе магистрального соединения Gigabit Ethernet.

GLBP (Gateway Load Balancing Protocol)

Протокол разработан компанией Cisco Systems и предназначен для динамического выравнивания нагрузки в резервированных группах оконечных узлов ЛВС.

GOB (Groups Of Blocks)

Фрагмент, который включает в себя несколько стандартных блоков видеоизображения.

GOP (Group Of Pictures)

Обозначение способа чередования кадров видеоизображения, формируемого при выполнении стандартных процедур сжатия MPEG.

GPON (Gigabit-capable PON)

Общее наименование технологий построения высокоскоростных пассивных оптических сетей, ориентированных на использование принципов ATM и Ethernet/IEEE 802.3 для интеграции разнородного трафика (ITU-T G.984).

GRE (Generic Routing Encapsulation)

Универсальный туннельный протокол сетевого уровня, который используется для повышения безопасности информационного взаимодействия через сети общего пользования.

GVRP (Generic VLAN Registration Protocol)

Протокол, который является частным приложением протокола GARP и предназначен для автоматического создания и обслуживания таблицы виртуальных сетей.

H

HDLC (High-level Data Link Control)

Универсальный протокол канального уровня, обеспечивающий управление звеном передачи данных.

HDTV (High-Definition Television)

Цифровое телевидение повышенной четкости.

HFC (Hybrid-Fiber/Coax)

Гибридные волоконно-оптические/коаксиальные кабельные структуры, которые используются для трансляции сигнала в сетях кабельного телевидения (КТВ). Прямое и обратное преобразование сигнала, передаваемого из волоконно-оптического сегмента в коаксиальный сегмент, выполняется стандартными конвертерами.

HSRP (Hot Standby Router Protocol)

Протокол Cisco Systems Inc., обеспечивающий горячее резервирование маршрутизаторов ответственных сетевых узлов.

HTTP (Hypertext Transfer Protocol)

Протокол прикладного уровня, используемый для доступа к информации, размещенной на www-серверах.

I

IANA (Internet Authority National Association)

Организация, которая курирует распределение общих ресурсов сети Интернет.

ICMP (Internet Control Message Protocol)

Протокол, используемый для обмена управляющими сообщениями в сети Интернет.

IETF (Internet Engineering Task Force)

Международная организация, выполняющая весь комплекс работ по подготовке основополагающих документов и рабочих спецификаций сети Интернет.

IGMP (Internet Group Management Protocol)

Протокол, используемый оконечными узлами сети Интернет для указания своей потребности в приеме группового трафика.

IntServ (Integrated Service Model)

Модель объединенного обслуживания, в которой заданный уровень качества обслуживания достигается путем применения специальных механизмов динамического резервирования ресурсов для выделенной части передаваемого трафика.

IP (Internet Protocol)

Протокол сетевого уровня Интернета.

IP (Intellectual Property)

Право интеллектуальной собственности, например, по отношению к цифровому продукту.

IPCP (IP Control Protocol)

Вспомогательный протокол, который обеспечивает согласование параметров протокола IP (например, назначение IP-адресов) на обоих концах PPP-соединения.

IPMP (Intellectual Property Management and Protection)

Комплекс средств и процедур для обслуживания и защиты прав интеллектуальной собственности по отношению к цифровому продукту.

IPv4 (Internet Protocol version 4)

Современная (четвертая) версия протокола сетевого уровня Интернета.

IPv6 (Internet Protocol version 6)

Перспективная (шестая) версия протокола сетевого уровня Интернета.

IPTV (Internet Protocol Television)

Системы, в которых для трансляции телевизионных программ используются протоколы стека TCP/IP.

ISDN (Integrated Services Digital Network)

Технология построения сетей с объединенными услугами — оцифрованные голос, видео и передача данных. Объединение и разделение разнородного трафика в канале ISDN выполняется по принципу временного разделения (TDM).

ISDB (Integrated Services Digital Broadcasting)

Японская спецификация цифрового вещания.

ISL (Inter Switch Link)

Технология, используемая на некоторых коммутаторах компании Cisco для построения магистральных каналов, в которой применяется принцип внешнего маркирования кадров меткой виртуальной сети.

ISO (International Standardization Organization)

Официальная международная стандартизирующая организация.

ITU (International Telecommunication Union)

Международная организация, выполняющая комплекс работ по развитию телекоммуникационных технологий.

IVR (Interactive Voice Response)

Интерактивное голосовое меню — система управления, которая используется в автоматизированных центрах обработки телефонных вызовов.

L

L2TP (Layer Two Tunneling Protocol)

Туннельный протокол канального уровня, используемый для управления доступом пользователя к защищенным ресурсам частной сети.

LACP (Link Aggregation Control Protocol)

Протокол управления агрегированным каналом, предназначенный для автоматического построения и обслуживания агрегированных каналов на сетевых устройствах с интерфейсами Ethernet.

LAN (Local Area Network)

Сеть, информационное взаимодействие между узлами которой осуществляется протоколами канального уровня.

LCP (Link Control Protocol)

Вспомогательный протокол, который обеспечивает непосредственное управление функционированием канала передачи данных при использовании протокола PPP.

LED (Light Emission Diode)

Светодиод, который может быть использован в качестве источника излучения для передачи данных через волоконно-оптическую линию связи.

Link Integrity Test

Процедура, используемая для автоматической проверки подключения удаленного абонента в сетях Ethernet.

LLC (Logical Link Control)

Обозначение верхнего промежуточного уровня доступа к среде передачи в технологиях CSMA/CD (Ethernet).

LMI (Local Management Interface)

Интерфейс локального управления — совокупность процедур, которые обеспечивают контроль параметров виртуального канала в сети, построенной с использованием технологий Frame Relay.

Load Balancing

Процедура увеличения скорости информационного обмена при объединении нескольких параллельных каналов.

M

MAC (Media Access Control)

Обозначение нижнего промежуточного уровня доступа к среде передачи в технологиях CSMA/CD.

MCU

Устройства управления многоточечными конференциями, организующие мультимедийный информационный обмен с участием трех и более абонентов H.323.

MEGACO (Media Gateway Control)

Протокол, предназначенный для управления компонентами иерархических систем в процессе организации и обслуживания мультисервисного вызова с передачей данных по пакетной сети общего пользования.

MGCP (Media Gateway Control Protocol)

Протокол, предназначенный для управления компонентами иерархических систем в процессе организации и обслуживания мультисервисного вызова с передачей данных по пакетной сети общего пользования.

MIB (Management Information Base)

Информационная база, в которой размещается информация, необходимая для управления сетевыми объектами по протоколу SNMP.

MII (Media Independent Interface)

Универсальный промежуточный интерфейс Ethernet, предназначенный для реализации взаимодействия компонента LLC со специализированными и универсальными блоками канального уровня.

MMF (Multi Mode Fiber)

Многомодовое оптическое волокно.

MMPE (Microsoft Point-To-Point Encryption Protocol)

Протокол, предложенный компанией Microsoft для кодирования сообщений, передаваемых через соединение "точка-точка".

MOD (Music on Demand)

Услуга трансляции музыкальных программ по запросу абонента.

MPEG (Moving Picture Expert Group)

Неофициальное наименование рабочей группы экспертов кодирования подвижных изображений ISO/IEC JTC1 SC29 WG11.

MPCP (Multipoint Control Protocol)

Протокол управления многоточечным соединением Ethernet.

MS (Mobile Station)

Мобильная станция — термин, который используется для обозначения абонентских устройств в сетях беспроводного доступа.

MSTP (Multiple Spanning Tree Protocol)

Многоплановый протокол Spanning Tree, применяемый для создания на коммутаторе независимых процессов STP для выбранных групп (планов), сконфигурированных на нем виртуальных сетей.

MTU (Maximum Transfer Unit)

Максимальный размер блока данных, установленный для передачи между узлами сети на канальном уровне.

Multicast (групповая передача)

Режим адресации, который используется для передачи блоков данных сетевого уровня только для установленной группы узлов сети.

N

NAT (Network Address Translation)

Трансляция сетевых адресов — алгоритм преобразования IP-адресов источника и/или назначения у пакетов, проходящих через маршрутизатор.

NCP (Network Control Protocol)

Вспомогательный протокол, который обеспечивает выбор и согласование конфигурации протокола PPP для взаимодействия с протоколом сетевого уровня.

NetFlow

Технология, разработанная компанией Cisco Systems для сбора и предварительной обработки на маршрутизаторах информации о проходящем через них трафике.

NMS (Network Management Systems)

Программные комплексы, выполняющие функции управления сетевыми компонентами.

NNI (Network-to-Network Interface)

Обозначение интерфейса между двумя сетевыми устройствами в сети, построенной с использованием технологии ATM.

NTP (Network Time Protocol)

Протокол, который обеспечивает взаимную синхронизацию счетчиков времени различных объектов сети Интернет.

NTSC (National Television System Committee)

Американский национальный телевизионный комитет, отвечающий за развитие одноименных промышленных стандартов цветного телевизионного вещания.

O

OFDM (Orthogonal Frequency-Division Multiplexing)

Технология ортогонального частотного мультиплексирования, которая применяется для создания высокочастотных каналов передачи данных в сетях беспроводного доступа.

OLT (Optical Line Terminal)

Оптический терминал центрального офиса — устройство, используемое для формирования сигнала в узлах доступа сетей PON.

ONU (Optical Network Unit)

Оптический терминал абонента — устройство, используемое для организации абонентских подключений в сетях PON.

OSI (Open System Interconnect)

Концепция организации информационного взаимодействия открытых систем, основные принципы которой изложены в стандарте ISO 7498.

OSPF (Open Shortest Path First)

Протокол, используемый для автоматического построения маршрутов в сети Интернет.

P

P2MP (Point-To-Multipoint)

Многоточечное соединение (Ethernet).

PAL (Phase Alternating Line)

Европейский стандарт цветного телевизионного вещания.

PAM5 (Five-level Pulse Amplitude Modulation)

Технология многоуровневого амплитудно-импульсного кодирования, которая применяется для формирования линейного сигнала в технологии 1000BaseT.

PAP (Password Authentication Protocol)

Вспомогательный протокол, который применяется для установления подлинности партнеров PPP соединения и использует простую схему аутентификации.

PCM (Pulse Code Modulation)

Импульсно-кодовая модуляция — ИКМ. Способ преобразования непрерывного голосового сигнала в последовательность кодовых посылок.

PCS (Physical Coding Sub layer)

Уровень физического кодирования. Вспомогательный уровень информационного взаимодействия в технологиях Ethernet, на котором определяются операции по преобразованию передаваемого и принимаемого кодов в соответствии с характером используемой среды передачи данных.

PDH (Plesiochronous Digital Hierarchy)

Плезиохронная цифровая иерархия — технология построения цифровых каналов передачи данных. Основные принципы этой технологии изложены в рекомендациях ITU-T G.703 и G.704.

PDU (Protocol Data Units)

Термин, который может быть использован для обозначения блоков данных протокола любого уровня.

PKM (Key Management Protocol)

Протокол, используемый для управления ключами при шифровании блоков данных, передаваемых в беспроводных сетях.

PMA (Physical Medium Attachment)

Уровень подключения к физической среде. Вспомогательный уровень информационного взаимодействия в технологиях Ethernet, на котором определяются основные требования к значениям характеристик используемой среды передачи данных и параметрам приемопередающих компонентов.

PoE (Power over Ethernet)

Неофициальное наименование комплекса технических решений, которые обеспечивают передачу электропитания подключенному абоненту от активного оборудования ЛВС через сигнальный кабель Ethernet.

PON (Passive Optical Networks)

Технология построения оптических сетей на основе пассивных оптических разделителей передаваемого сигнала.

Port Security

Функция, которая обеспечивает управление подключением абонентов к порту коммутатора на основе анализа адресов канального уровня.

PPP (Point-to-Point Protocol)

Универсальный протокол канального уровня, предназначенный для использования на двухточечных каналах передачи данных.

PPPoE (Point-to-Point Protocol over Ethernet)

Стандартный способ передачи кадров PPP через сеть Ethernet, который используется для управления доступом к ресурсам ЛВС.

PPTP (Point-to-Point Tunneling Protocol)

Туннельный протокол канального уровня, используемый для управления доступом пользователя к защищенным ресурсам частной сети.

PRI (Primary Rate Interface)

Интерфейс первичной скорости, который предназначен для организации корпоративных подключений в сетях PSTN и ISDN.

PSK (Phase-Shift Keying)

Фазовая манипуляция — способ формирования линейного сигнала, при котором передаваемые данные кодируются скачками фазы несущего гармонического колебания.

PSNR (Peak Signal-to-Noise Ratio)

Максимальное значение соотношения уровней сигнала и шума. Используется в качестве критерия для оценки качества преобразования и восстановления видеоизображений.

PSTN (Public Switching Telephone Network)

Телефонная сеть общего пользования (ТфОП).

PTP (Point to Point)

Технология построения оптических сетей на основе сквозных каналов от точки до точки.

PVC (Permanent Virtual Circuit)

Постоянный виртуальный канал — логическая конструкция, которая организуется для обеспечения постоянного соединения между двумя объектами в сетях, построенных с использованием технологий X.25, Frame Relay и ATM.

PVR (Personal Video Recorder)

Услуга "Персональный видеомагнитофон", которая обеспечивает возможность абоненту VOD копировать и просматривать выбранные видеопрограммы.

PVST (Per-VLAN Spanning Tree Protocol)

Протокол, предложенный компанией Cisco Systems для создания на коммутаторе независимых процессов STP для каждой из сконфигурированных на нем виртуальных сетей.

Q

QAM

Квадратурная амплитудно-фазовая модуляция — способ формирования линейного сигнала, при котором передаваемые данные кодируются изменениями амплитуды и фазы несущего гармонического колебания.

QCIF (Quarter-size Common Intermediate Format)

Уменьшенный вчетверо типовой (промежуточный) формат видеоизображения.

QoS (Quality of Service)

Совокупность значений сетевых ресурсов, выделяемых для обработки трафика, принадлежащего к соответствующему классу.

R

RADIUS (Remote Authentication Dial In User Service)

Приложение, которое используется для выполнения комплекса процедур управления доступом абонента к сетевым ресурсам.

RAID (Redundant Array Of Independent Disks)

Разделяемые отказоустойчивые массивы накопителей данных.

RAS (Registration, Admission and Status)

Совокупность процедур управления доступом абонентов H.323, представленная в рекомендации H.225.

RFC (Requests For Comments)

Название серии документов IETF, в которых рассматриваются предварительные предложения, определяющие направления модернизации и дальнейшего развития комплекса технологий сети Интернет.

RDD (Rights Data Dictionary)

Словарь языка выражения прав собственности, используемого в спецификации MPEG-21.

REL (Rights Expression Language)

Язык выражения прав собственности по отношению к цифровым продуктам, используемый в спецификации MPEG-21.

Router (Маршрутизатор)

Специальное сетевое устройство или выделенный компьютер, реализующий комплекс процедур информационного взаимодействия на сетевом уровне.

RPC (Remote Procedure Call)

Протокол сеансового уровня, который определяет порядок выполнения процедуры на удаленном узле сети.

RPF (Reverse Path Forwarding)

Алгоритм, который используется в протоколах групповой маршрутизации для противодействия возникновению циклических маршрутов.

RPR (Resilient Packet Ring)

Обозначение комплекса протоколов, предназначенных для построения кольцевых магистралей в сетях с коммутацией пакетов.

RSTP (Rapid Spanning Tree Protocol)

Модифицированный протокол STP, который способен существенно сократить время построения ациклических структур (активных топологий) соединения коммутаторов ЛВС.

RSVP (Resource reSerVation Protocol)

Протокол прикладного уровня, предназначенный для резервирования ресурсов ЛВС для обработки трафика выделенной группы в системах IntServ.

RTCP (Real Time Control Protocol)

Вспомогательный протокол, который обеспечивает управление сетевыми компонентами при использовании протокола RTP.

RTP (Real Time Protocol)

Протокол прикладного уровня, обеспечивающий передачу потокового трафика по сети Интернет.

RWND (Receiver Window)

Обозначение переменной, которая в протоколе STCP используется для указания размера окна приемника.

S

SAP (Session Announcement Protocol)

Протокол, используемый для анонсирования сессий мультисервисных потоков групповой (Multicast) адресации.

SDH (Synchronous Digital Hierarchy)

Синхронная цифровая иерархия — технология построения магистральных цифровых сетей передачи данных.

SDTV (Standard-Definition Television)

Цифровое телевидение стандартной четкости.

SDP (Session Description Protocol)

Универсальный протокол, используемый для описания сеансов связи в мультисервисных сетях.

SEAL (Simple and Efficient Adaptation Layer)

Неофициальное наименование протокола уровня адаптации AAL5, который используется для передачи по сетям ATM трафика локальных вычислительных сетей.

SECAM (Sequential Couleur Avec Memoire)

Альтернативный, по отношению к PAL, европейский стандарт цветного телевизионного вещания.

SFP (Small Form-Factor Pluggable)

Встраиваемый конвертер уменьшенного формата, который может быть использован для организации на коммутаторе магистрального соединения Gigabit Ethernet.

SIP (Session Initiation Protocol)

Протокол организации вызова, назначение которого состоит в обеспечении управления мультисервисным информационным обменом абонентов сети Интернет.

SLIP (Serial Line Internet Protocol)

Протокол канального уровня, обеспечивающий подключение удаленного узла к сети Интернет по последовательному каналу.

SMDS (Switched Multi megabit Data Service)

Технология сетевого уровня OSI ISO 7498, которая может быть использована для построения высокоскоростных соединений между ЛВС.

SMF (Single Mode Fiber)

Одномодовое оптическое волокно.

SNMP (Simple Network Management Protocol)

Протокол прикладного уровня, обеспечивающий мониторинг и управление значениями параметров удаленного узла сети Интернет.

SNR (Signal/Noise Ratio)

Выраженное в децибелах отношение мощностей полезного сигнала и шума в линии.

Sprite (Спрайт)

Спрайт — неподвижная фоновая область панорамного видеоизображения.

SRP (Spatial Reuse Protocol)

Протокол, разработанный специалистами компании Cisco Systems для передачи данных по кольцевым магистралям в сетях с коммутацией пакетов.

SS (Subscriber Station)

Беспроводное абонентское устройство, которое подключается к базовой станции по технологии IEEE 802.16.

STCP (Stream Control Transmission Protocol)

Протокол управления передачей потоков, основным назначением которого является передача сигнальных сообщений, формируемых в сетях пакетной телефонии, по сетям Интернет.

STA (Spanning Tree Algorithm)

Алгоритм связующего дерева, используемый в ЛВС для автоматического построения ациклических структур (активных топологий) соединения коммутаторов.

STP (Spanning Tree Protocol)

Протокол, предназначенный для реализации STA-алгоритма связующего дерева.

STB (Set-Top-Box)

Распространенное и обобщенное наименование приставки к телевизионному приемнику.

T

TACACS (Terminal Access Controller Access-Control System)

Приложение, используемое для установления подлинности (аутентификации) удаленного абонента.

TDD (Time Division Duplex)

Способ организации дуплексного режима в беспроводных сетях, при использовании которого принимаемый и передаваемый сигналы разделяются по времени.

TDM (Time Division Multiplexing)

Способ разделения пропускной способности, при котором каждому из компонентов трафика, передаваемых по каналу, отводится фиксированная доля полосы пропускания этого канала.

TCP (Transmission Control Protocol)

Протокол транспортного уровня, обеспечивающий гарантированную доставку данных в сети Интернет.

Telnet (Протокол виртуального терминала)

Протокол прикладного уровня, предназначенный для управления сетевыми узлами Интернета при помощи виртуального терминала.

TFTP (Trivial File Transfer Protocol)

Протокол прикладного уровня, применяемый для организации простейшего файлового обмена в сети Интернет.

Token Ring

Технология, используемая корпорацией IBM для построения локальных вычислительных сетей с использованием маркерного доступа к разделяемой среде передачи данных.

TOS (Type of Service)

Поле блока данных сетевого уровня протокола IPv4, предназначенное для указания уровня обслуживания, который должен использоваться для обработки этого блока на узлах сети.

TIA (Telecommunications Industry Association)

Некоммерческая национальная организация США, занимающаяся разработкой и внедрением стандартов в области телекоммуникаций.

TTL (Time To Live)

Время "жизни" — продолжительность существования блока данных в сети или буферной памяти шлюза.

U

UAC (User Agent Client)

Клиентская часть абонента SIP.

UAS (User Agent Server)

Серверный компонент абонента SIP.

UDP (User Datagram Protocol)

Протокол транспортного уровня, используемый для негарантированной доставки данных в сети Интернет.

UGS (Unsolicited Grant Service)

Обозначение типа трафика, для обслуживания которого в беспроводных сетях WiMAX выделяется гарантированная пропускная способность канала.

UHDV (Ultra High Definition Video)

Цифровое телевидение сверхвысокой четкости.

Unicast (Индивидуальный обмен)

Режим адресации, который используется для передачи блоков данных сетевого уровня только указанному узлу сети.

UTP (Unshielded Twisted Pair)

Неэкранированная витая пара — тип многожильного медного кабеля, который применяется при построении локальных сегментов вычислительных сетей.

URI (Uniform Resource Identifier)

Обозначение идентификатора сетевого ресурса, используемого в сети, основанной на протоколе SIP.

V

VAD (Voice Activity Detector)

Процедура, предназначенная для повышения эффективности использования канала передачи данных путем выделения интервалов активности абонентов.

VACL (VLAN Access Control List)

Список, применяемый для управления информационным обменом между абонентами, расположенными в различных виртуальных сетях — VLAN.

VLAN (Virtual Local Area Network)

Виртуальная локальная сеть.

VLBV (Very Low Bit-rate Video)

Видеоизображения, формируемые приложениями с невысокой информационной скоростью. Частота смены кадров — не более 15 Гц, размер видеоизображения VLBV обычно не превышает стандартного формата CIF.

VLC (Variable Length Coding)

Способ, применяемый для вычисления коэффициентов дискретного преобразования видеоизображения в коды переменной длины для их последующей отправки по каналу передачи данных.

VoIP (Voice over IP)

(Голос по IP) Неофициальное наименование комплекса технологий, обеспечивающих передачу оцифрованного голосового сигнала по сетям с коммутацией пакетов.

VOD (Video On Demand)

"Видео по запросу" — режим использования телевизионной системы, который позволяет абоненту заказать доставку или трансляцию выбранного видеофильма или видеопрограммы.

VOP (Video Object Plane)

План визуального объекта — логически завершенный и независимый компонент многослойной сцены видеоизображения, преобразованного по алгоритмам и правилам MPEG-4.

VRML (Virtual Reality Modeling Language)

Язык, применяемый для описания и построения объектов виртуальной реальности.

VRRP (Virtual Router Redundancy Protocol)

Стандартный протокол, предназначенный для обеспечения горячего резервирования маршрутизаторов ответственных сетевых узлов.

VTP (VLAN Trunk Protocol)

Протокол, используемый для управления конфигурациями VLAN в ЛВС, построенных на коммутаторах Cisco Systems.

W

WAN (Wide Area Network)

Глобальная сеть.

WDM (Wavelength Division Multiplexing)

Технологии волнового мультиплексирования, применяемые для повышения эффективности использования пропускной способности магистральных волоконно-оптических каналов.

Wi-Fi (Wireless Fidelity)

Неформальное наименование комплекса технологий беспроводной передачи данных IEEE 802.11.

WiMAX (Worldwide Interoperability for Microwave Access)

Неформальное наименование комплекса технологий беспроводной передачи данных IEEE 802.16.

X

X.25

Технология построения сетей пакетной коммутации общего назначения, ориентированных на обмен символьными данными.

XML (Extensible Markup Language)

Язык, используемый для построения и описания информационных продуктов.

XRN (eXpandable Resilient Networking)

Технология, применяемая компанией 3COM для повышения надежности и производительности магистральных компонентов ЛВС путем объединения их в распределенные отказоустойчивые стеки.

Предметный указатель

#

10Gigabit Ethernet 468, 469, 473, 475, 477
2B1Q 16
3Play 1

A

A/BPON 47
AAL 541
AAL1 30
AAL3/4 30
AAL5 30
ABR 28
Access Layer 541
ACK 541
ACL 257, 409, 541
ADPCM 60, 541
Advanced Coding Efficiency (ACE) 101
Advanced Core Profile 101
Advanced Real-Time Simple Profile (ARTS) 101
Advanced Scaleable Texture Profile 101
A-Law 57
AN-MP 489
ANSI 541
AN-UP 489
AOEN 46
AP 542
APON 47, 542
Application Layer 178
ARP 542
ASN.1 507
ATM 2, 3, 11, 25— 30, 47, 48, 541
ATSC 112, 542
Auto QoS VoIP 408
Auto-Negotiation 542
AVF 332—334
AVG 332—334

B

B2B hosting 114
Bandwidth 390
Basic Animated 2-D Texture Visual Profile 100
Bc 411
Be 411
BE 43
BIFS 542
BPDU 278, 542
BPON 47, 48, 542
BRI 13, 542
Bridge Identifier 273
Broadcast 183, 215, 225, 365
◊ Broadcast-штормы 268, 269
BS 41, 43, 44, 542

C

C2C hosting 114
CableLabs 33
CableNET 33
Call-центр 77, 528
CAM 204, 543
CAR 410

CARP 543
CBR 28—30
CDP 543
CELP 59, 60, 543
CGMP 543
CHAP 543
CIF 543
CIR 23, 410, 543
CIST 306
CLP 27
CM 32, 543
CMTS 32—36, 38, 43, 543
Codec 57, 544
Core Layer 544
Core Scalable Profile 101
Core Visual Profile 100
CoS 391, 544
CPE 25
CS 111
CS-ACELP 60
CSMA/CD 317, 544
CST 304, 305
CWND 171, 544

D

Data 180
Data Link Layer 179
Datagram 544
DCE 544
DCT 545
DDL 544
DE 22, 23, 28
Default Gateway 544
Delay 390
Delay variation 390
Dense mode 544
DES 252
DHCP 545
DID 106
DiffServ 545
Digital Item 545
DII 106
Distribution Layer 545
DLCI 19—24, 545
DNS 140
DOCSIS 3, 11, 33—39, 42, 48, 545
◊ универсальный шлюз (DSG) 37, 545
DOCSIS v1.0 33
DOCSIS v1.1 33
DOCSIS v2.0 34
DOCSIS v3.0 34
DOWNSTREAM 33, 35, 47, 50
DSCP 405
DSG 37—39, 545
DSG Agent 38
DSG Client 38
DSG Client Controller 38
DSG Server 38
DSG Tunnel 38
DSSS 40, 545
DVB 112, 545
DVMRP 546

E

EAPOL 546
EAS 37, 546
EFM 48, 546
EIA 546
EPG 37, 114, 546
EPON 3, 11, 48—51
Ethernet 44, 46, 48—50, 546

F

FCS 546
FDD 42, 546
FDDI 546
FDDI-PCM 443
FIFO 416
FR 19
FR switch 19
FRAD 19, 547
Frame 547
Frame Relay 2, 3, 11, 19, 21—26, 28, 30, 547
Frame Relay Forum 19
FRF 19
FSAN 47
FTP 547
FTTB 46, 547
FTTC 46, 547
FTTH 46, 547
FTTN 46, 47, 547
FXO 547
FXS 547

G

GARP 548
Gatekeeper 548
Gateway 548
GBIC 548
GDA 372
General Slice Structure 94
Gigabit Ethernet 452—454
GLBP 548
GOB 548
GOP 548
GPON 47, 48, 548
GRE 548
GVRP 549

H

HDLC 549
HDTV 108, 549
Header 180
HEC 27
HFC 31, 33, 39, 42, 549
Hop-By-Hop 205
HSRP 549
HTTP 549
Hybrid Visual Profile 100

I

IANA 549
ICMP 549
IEEE 802.11 39—41, 44
IEEE 802.16 41—44
IEEE 802.3 47, 50
IETF 247, 549
IGMP 550
Intellectual Property (IP) 550
IntServ 550
IP 550
IPCP 550
IPMP 106, 550
IPTV 4, 113, 550
IPv4 550
IPv6 550
IP-телефон 67
ISDB 112, 550
ISDN 2, 3, 11—19, 21, 24, 25, 30, 550
ISL 219, 302, 550
ISO 85, 551
IST 305
ITU 551
ITU-T 85
IVR 75, 533, 551

L

L2TP 551
LACP 551
LAN 551
LAPD 17
LCP 551
LCT 443
LD-CELP 59, 60
LED 459, 551
Link Codeword (LCW) 487, 489
LLC 182, 551
◊ LLC-frame 441
LMI 24, 551
Load Balancing 552
LT 14

M

MAC 182, 552
◊ MAC-frame 441
◊ MAC-адрес 214
Main Visual Profile 100
Management Interface 484
Mapping 385
MCU 552
MEGACO 552
MG 70, 142
MGC 70, 142
MGCP 552
MIB 507— 511, 513, 519, 520, 552
MIB Browser 518
MII 552
MMF 552
MMPE 552
MOD 114, 552
MPCP 49, 553
MPEG 85, 552
MPEG-1 91
MPEG-2 92
MPEG-21 105

MPEG-4 96, 97
MPEG-7 104
MP-MLQ 58, 60
MS 111, 553
MSTI 304—306
MSTP 266, 553
MTU 188, 553
Multicast 38, 50, 183, 215, 225, 365, 553
◊ Multicast-группа 370

N

NAT 553
N-Bit Visual Profile 100
NCP 553
NetFlow 553
NetFlow Cache 521, 524
Network Layer 179
NGN 1
NMS 508, 517—520, 553
NNI 24, 25, 553
Non-Unicast 215
nrtPS 43
Nrt-VBR 28
NT 14
NTP 553
NTSC 554

O

OFDM 40, 42, 44, 554
OFDMA 42, 44
OLT 46, 49, 50, 554
ONT 49
ONU 46, 49, 50, 554
OOB 37
OSI 178, 554
OSI ISO 7498 17, 19, 28, 29, 30
OSPF 554

P

P2MP 48, 554
PAL 554
PAM5 464, 554
PAP 554
PCM 54, 60, 555
PCS 555
PD 497—500
PDH 65, 555
PDU 180, 555
Physical Layer 179
PKM 44, 555
PMA 555
PoE 74, 555
PON 45—48, 50, 555
Port Security 256, 257, 555
PPP 555
PPPoE 556
PPTP 556
Presentation Layer 178
PRI 13, 556
PRI/E1 67
PSE 497, 498, 500
PSK 112, 556
PSNR 556
PSTN 50, 65, 556
PT 27
PTP 45—47, 556
PVC 19, 556
PVR 114, 556
PVST 556

Q

QAM 112, 557
QAM-128 34
QAM-256 34
QAM-64 34
QCIF 557
QoS 389, 557
◊ QoS-домен 402, 407, 408

R

RADIUS 557
RAID 339, 557
RAS 126, 557
RDD 106, 557
REL 106, 557
Remote Fault Indication 484
Restricted Slice Structure 93
RFC 557
Router 557
RPC 558
RPF 558

RPR 5, 447, 558
RSpec 393
RSTA 292, 296, 297, 299
RSTP 558
RSVP 558
RTCP 558
RTP 558
rtPS 43
Rt-VBR 28
RWND 171, 558

S

SAP 558
SAP-Cache 537
SC 42
Scalable Texture Visual Profile 100
SDH 65, 558
SDP 559
SDTV 108, 558
SEAL 30, 559
SECAM 559
Session Layer 178
SFP 559
Simple Facial Animation Visual Profile 100
Simple Scalable Visual Profile 100
Simple Visual Profile 100
SIP 559
SLIP 559
SMDS 30, 559
SMF 559
SMT-frame 441
SNMP 559
SNR 53, 559
SPE 476
Sprite 559
SRP 559
SS 41, 111, 560
STA 270, 285, 560
STB 37, 560
STCP 560
STP 560

T

T 411
TA 14
TACACS 560
TCP 560
TDD 42, 560
TDM 12, 25, 48, 49, 153, 560
TE1 14
TE2 14
TEI 17
TELNET 560
TFTP 44, 561
TIA 561
Token Ring 561
TOS 403, 561
Transceiver 477
Transport Layer 179
TS 111
TSpec 393
T-VOD 110

U

UA 135
UAC 135, 561
UAS 135, 561
UBR 28
UCD 36
UDP 561
UGS 43, 561
UHDV 108, 561
UNI 25
Unicast 183, 215, 365, 561
Unknown Unicast 225
UPSTREAM 33, 47, 50
URI 140, 562
UTP 425, 562

V

VACL 206, 562
VAD 60, 562
VC 26
VCI 26, 27
Vendor code 183
VHF-H 31
VLAN 4, 206, 212, 213, 215—217, 562
◊ списки доступа 206
◊ типы портов 222
VLBV 562
VLC 562

Vocoder 57
VOD 110, 114, 562
VoIP 3, 38, 62, 562
VOP 562
VPI 26, 27
VRID 324
VRML 563
VRRP 563
VSB 112
VTP 563

W

WAN 563
WDM 563
Wi-Fi 39, 563
WiMAX 3, 11, 41, 42, 48, 563

X

X.25 563
XML 563
XRN 563

μ

μ-Law 57

А

Абонентская станция (SS) 41, 560
Автоматические телефонные станции (АТС) 65
Адаптивная дифференциальная импульсно-кодовая модуляция 60
Адаптивная дифференциальная импульсно-кодовая модуляция (АДИКМ) 58
Активная топология ЛВС 271
Алгебраическая экстраполяция с кодовым инициированием 60
Алгоритм:
◊ DCT 545
◊ Echo Cancellation 463
◊ HMAC-MD5 307
◊ Leaky Bucket 410
◊ Rapid Spanning Tree Algorithm (RSTA) 292, 296, 297, 299
◊ RPF 383, 384, 558
◊ Spanning Tree 267
◊ Spanning Tree (STA) 270—272, 290, 291, 560
  ▫ изменение активной топологии 288
  ▫ практическая реализация 278
  ▫ состояния и режимы портов 285
◊ SPQ 416
◊ WRR 416
◊ кодирования DES 252

Б

Базовая станция (BS) 41
Биллинг 232
Блок данных 180

В

Видеоизображение:
◊ GOB 86, 548
◊ GOP 92, 548
◊ MB 86

Видеоизображение *(прод.)*:
◊ видеоприложения 107
  ▫ коммерческие 107
  ▫ некоммерческие 115
◊ визуальный объект (VO) 97
◊ графическая сетка 96
◊ идентификация цифрового продукта (DII) 106
◊ кадр 80
◊ кинескоп 80
◊ кодирование:
  ▫ объектно-ориентированное 96
  ▫ SAC 90
  ▫ VLC 89, 562
◊ определение цифрового продукта (DID) 106
◊ планы визуальных объектов (VOP) 97, 562
◊ поток:
  ▫ PES 95
  ▫ программный 95
  ▫ транспортный 95
◊ преобразование DCT 88
◊ приложения:
  ▫ High Bit Rate 102
  ▫ VLBV 102, 562
◊ профили для кодирования объектов 99
◊ профиль:
  ▫ базовый визуальный 100
  ▫ визуальный двумерной текстуры 100
  ▫ визуальный для расширяемой текстуры 100
  ▫ гибридный визуальный 100
  ▫ основной визуальный 100
  ▫ простой визуальный 100
  ▫ простой лицевой анимации 100
  ▫ простой расширенный визуальный 100
  ▫ расширенный базовый 101
  ▫ расширенный повышенной эффективности кодирования 101
  ▫ расширенный простой реального времени 101
  ▫ расширенный текстурный масштабируемый 101
  ▫ узкополосный визуальный 100
  ▫ центральный масштабируемый 101
◊ режим:
  ▫ INTER Mode 88, 89
  ▫ INTRA Mode 88
  ▫ общей структуры 94
  ▫ ограниченной структуры 93
◊ сообщение:
  ▫ ECM 95
  ▫ EMM 95
◊ соотношение сигнала и шума (PSNR) 103, 556
◊ спецификация:
  ▫ MPEG-1 91
  ▫ MPEG-2 92
  ▫ MPEG-21 105
  ▫ MPEG-4 96, 97
  ▫ MPEG-7 104
◊ спрайт 97, 559
◊ срез 93
◊ степень сжатия 102
◊ строка 80
◊ сцена 97
◊ формат:
  ▫ 16CIF 84
  ▫ 4CIF 83
  ▫ BIFS 101
  ▫ CIF 83
  ▫ QCIF 83, 557
  ▫ SQCIF 84
◊ язык DDL 104
Вокодер 57
Волоконно-оптические линии связи (ВОЛС) 45

Д

Дейтаграмма 189, 544
Дерево распространения группового трафика 381

З

Заголовок 180

И

Идентификатор виртуального маршрутизатора (VRID) 324

Импульсно-кодовая модуляция (ИКМ) 54, 60
Импульсы:
◊ FLP 483, 484
◊ NLP 481, 482, 485, 488
Инкапсуляция 181
Инстанция (план) 304
Интерактивное голосовое меню (IVR) 75, 551
Интернет 19, 31—33, 36—38, 41, 43, 50, 51
Интерфейс:
◊ FXO 73, 547
◊ FXS 73, 547
◊ LMI 551
◊ MDI 453
◊ MDI/MDIX 467
◊ MII 453, 552
◊ XGMII 469, 470
Информационная подсистема предприятия 147
Источник питающего напряжения (PSE) 497, 498, 500

К

Кабель:
◊ MMF 472, 552
◊ SMF 472, 559
Кабельный модем 543
Кадр 547
◊ Ethernet IEEE 802.1Q 220
Канал:
◊ агрегированный (объединенный) 340, 342, 344
▫ пример использования 347
▫ создание и удаление 345
Канальный шлюз (MG) 142
◊ контекст 143
◊ окончание 142
Качество обслуживания (QoS) 389
◊ модель:
▫ DiffServ 391, 401, 545
▫ IntServ 391, 392, 550
Кластер серверов 338
Кодек 57, 544
Кодирование:
◊ многоуровневое амплитудно-импульсное (PAM5) 464, 554
Кодовые страницы канала 488
Коммутатор 199
◊ многоуровневая коммутация 210
◊ способы построения 202
◊ таблица CAM 204
◊ функции 200
Конвертер:
◊ GBIC 478
◊ SFP 478, 559
Контроллеры физических шлюзов (MGC) 70
КТВ 34, 37—39

Л

ЛВС:
◊ топология 424
▫ иерархическая 424, 426, 427, 430, 432, 433, 541
▫ кольцевая 424, 434
▫ общей шины (ОШ) 426
▫ шинная 424, 425
Линейная экстраполяция с кодовым инициированием 59, 60
Линейная экстраполяция с кодовым инициированием и малыми задержками 59, 60
Линия:
◊ бюджет оптической мощности 461
◊ ресурс 461
Люминофор 80

М

Маршрут:
◊ корневой 275
▫ стоимость 276
Маршрутизатор 199, 557
◊ аппаратный 199
◊ запасной 320
◊ принцип Hop-By-Hop 205
◊ программный 200
◊ резервирующая группа 317, 318

Маршрутизатор *(прод.)*:
◊ резервный 320
◊ функции:
▫ дополнительные 206
▫ основные 204
Маршрутизация:
◊ динамическая 205
◊ статическая 205
Многоимпульсное многоуровневое квантование 58, 60
Мобильные станции 39, 553
Модель:
◊ OSI 178
▫ канальный уровень 179
▫ сеансовый уровень 178
▫ сетевой уровень 179
▫ транспортный уровень 179
▫ уровень представления 178
▫ уровень приложения 178
▫ физический уровень 179
Мост 199
◊ идентификатор 273
◊ корневой 272
◊ назначенный 277
◊ прозрачный 201
◊ способы построения 202
◊ функции 200
MCC 11
Мультисервисная сеть (MCC) 1
◊ беспроводного доступа 39
◊ гибридные широкополосного доступа 31
◊ локальные на основе Ethernet 44
◊ принципы создания 30

H

HEC 28

O

Общее связующее дерево (CST) 304
Оповещение об изменениях топологии 289
Определение активности голосового канала 60

П

Пакетная телефония 61
◊ иерархические системы 70
◊ компоненты 72
◊ преимущества 61
◊ преобразование голоса 62
◊ распределенные системы 68
Пиксел 83
Повторитель 198
Полезная нагрузка 180
Порт:
◊ активный режим 287
◊ в выключенном состоянии 288
◊ граничный 296, 297
◊ заблокированный 277
◊ запасной 284
◊ корневой 275
◊ назначенный 277
◊ режим блокировки 286
◊ режим обучения 287
◊ режим прослушивания 286
Потребитель электроэнергии (PD) 497—500
Привратник 68, 548
◊ зона ответственности 124
◊ основные и дополнительные функции 124
Проверка целостности линии 481
Программное обеспечение:
◊ Axon 529
◊ виртуальная АТС Axon 529, 530
◊ звукозаписывающая система VRS Recording System 534, 535
◊ программный IP-телефон Express Talk 531, 532
◊ программный мультимедийный плеер VLC 539, 540
◊ технологическое 505
◊ формирователь мультимедийных потоков VLC 538
◊ функциональное 527
Программный комплекс:
◊ NeTraMet 526, 527
◊ SNMPc 517, 520
Пропускная способность канала передачи данных 180

Протокол 179
◊ ARP 185, 542
◊ CARP 315, 331, 335, 543
  ▫ области применения 337
  ▫ особенности 336
◊ CDP 184, 543
◊ CGMP 543
◊ CHAP 239, 543
◊ DHCP 36, 317, 545
◊ DVMRP 546
◊ EAPOL 255, 546
◊ Ethernet 181
  ▫ MAC-адрес 183
  ▫ режимы передачи 183
  ▫ структура кадра 184
◊ FTP 190, 547
◊ GARP 226, 227, 548
◊ GLBP 315, 331, 333, 334, 548
  ▫ выравнивание нагрузки 334
  ▫ назначение 332
  ▫ особенности применения 335
◊ GMRP 227
◊ GRE 250, 548
◊ GVRP 226—229, 549
◊ HDLC 549
◊ HSRP 315, 316, 320, 321, 324, 328, 329, 332, 549
  ▫ особенности применения 323
  ▫ параметры 319
  ▫ принципы реализации 317
  ▫ формат и типы сообщений 322
◊ HTTP 190, 549
◊ ICMP 188, 372, 549
◊ IEEE 802.1X 234, 253, 254, 256
  ▫ компоненты 254
  ▫ сообщения 255
◊ IGMP 188, 372, 373, 550
  ▫ практическая реализация 377
  ▫ прослушивание сообщений 378, 379
  ▫ сообщения 373—375
◊ IGMP v3 377
◊ IGRP 189
◊ IP 181, 182, 186, 235, 550
◊ IP v4 185, 550
◊ IP v6 185, 550
◊ IPCP 235, 550
◊ IPSTB 324
◊ L2P 251
◊ L2TP 247, 250—252, 551
◊ LACP 345, 347, 350, 362, 551
  ▫ ведомый партнер 351
  ▫ ведущий партнер 351
  ▫ взаимодействие партнеров 357
  ▫ ключ 352
  ▫ компоненты 351
  ▫ партнер 351
  ▫ структура блока данных 353
◊ LCP 235, 237, 551
◊ Manchester-II 197
◊ MEGACO 142, 552
◊ MGCP 142, 143, 552
  ▫ агент вызова 144
  ▫ оконечная точка 144
  ▫ соединения канального шлюза 144
◊ MMPE 248, 552
◊ MPCP 48, 553
◊ MPPE 250
◊ MS-CCP 250
◊ MS-CHAP 248, 250
◊ MSTP (IEEE 802.1Q) 4, 301, 303, 305, 307, 310, 431, 553
  ▫ принципы реализации 306
  ▫ регион 304
  ▫ сообщения 308
◊ NCP 235, 553
◊ NTP 36, 190, 553
◊ OSPF 189, 554
◊ PAP 239, 554
◊ PIM 383
  ▫ режим DENSE 383
  ▫ режим SPARSE 384
◊ PoE 496—499, 501
◊ PoEP 501—504
◊ POP3 190
◊ PPP 185, 234, 239, 555
  ▫ функции 234
◊ PPPoE 185, 234, 241, 243—245, 247, 556
◊ PPTP 234, 247—250, 252, 556
◊ PVST 301, 302, 556
◊ PVST+ 301, 302

Протокол *(прод.)*:
◊ RADIUS 190, 233, 239, 557
◊ RPC 178, 558
◊ RSTP 4, 266, 291—296, 300, 310, 558
  ▫ сообщения 292
◊ RSVP 189, 391—395, 558
  ▫ сообщения 397, 399
◊ RTCP 126, 161, 164, 558
  ▫ типы сообщений 168
◊ RTP 4, 126, 160, 161, 182, 558
  ▫ источник синхронизации 163
  ▫ сеанс 162
◊ SAP 369, 535—537, 539, 558
◊ SDP 140, 369, 559
◊ SIP 4, 70, 134, 529, 559
◊ SLIP 559
◊ SMTP 190
◊ SNMP 5, 185, 190, 506—509, 511, 514, 515, 559
  ▫ агент 508
  ▫ сообщения 514
◊ SRP 445, 447, 559
◊ STCP 4, 170, 560
  ▫ ассоциация 171
  ▫ механизм скользящего окна 171
  ▫ окно перегрузки (CWND) 171
  ▫ окно приемника (RWND) 171
  ▫ пакет 171
◊ STP 6, 266, 272, 279, 290, 292, 310, 360, 560
◊ TACACS 233, 560
◊ TACACS+ 239
◊ TCP 159, 179, 181, 182, 189, 190, 560
  ▫ флаги 193
◊ Telnet 178, 190, 560
◊ TFTP 190, 561
◊ TKP 435
◊ TXI 436
◊ UDP 160, 164, 179, 181, 182, 189, 515, 561
◊ VRRP 315, 316, 324, 332, 431, 563
  ▫ компоненты 324, 325
  ▫ особенности применения 327
  ▫ структура сообщений 325
◊ VTP 226, 229, 563
  ▫ домен 229
◊ многоплановый протокол Spanning Tree 301
◊ управления ключами (PKM) 44
Процедура:
◊ Auto-Negotiation 454, 463, 465, 466, 482—490, 492, 494, 542
  ▫ сообщения 486
◊ Link Integrity Test 481—483, 551
◊ Load Balancing 552

P

Регион 304
◊ мультиплановый (MR) 304
◊ мультиплановый (MST-Region) 304
Режим Auto QoS VoIP 408
Рекомендация:
◊ H.225.0 126
◊ ITU-T G.711 57
◊ ITU-T G.723.1 58
◊ ITU-T G.726 58
◊ ITU-T G.728 59
◊ ITU-T G.729 59
◊ ITU-T G.983 47
◊ ITU-T G.984 47
◊ ITU-T H.245 132
◊ ITU-T H.261 86
◊ ITU-T H.262 92
◊ ITU-T H.263 89
◊ ITU-T H.323 120
◊ ITU-T I.430 (11/95) 14
◊ ITU-T J.112 (03/01) 33
◊ ITU-T J.112 (03/98) 33
◊ ITU-T J.122 (12/02) 34
◊ ITU-T Q.921 (09/97) 17
◊ ITU-T Q.931 (05/98) 18
◊ ITU-T Q.931 (1993) 130
◊ ITU-T T.38 172
◊ T.120 122
Репитер 198
Роутер 199

C

Сегмент 196
◊ тип 197

Сеть:
◊ ATM 24
  ▫ виртуальный канал 26
  ▫ виртуальный путь 26
  ▫ интеграция трафика 28
  ▫ компоненты 25
  ▫ формат ячейки 27
◊ Frame Relay 19
  ▫ кадр 21
  ▫ особенности построения 19
  ▫ параметры качества обслуживания 23
  ▫ спецификация LMI 23
  ▫ структура кадра 21
◊ ISDN 12
  ▫ блок абонентского доступа 16
  ▫ взаимодействие абонентов 16
  ▫ интерфейс базовой скорости (BRI) 13
  ▫ интерфейс первичной скорости (PRI) 13, 556
  ▫ канал внеканальной сигнализации 12
  ▫ магистраль подключения 14
  ▫ принципы построения и компоненты 14
  ▫ протокол LAPD 17
  ▫ стандартный (элементарный) канал 12
  ▫ типы услуг 12
◊ LAN 551
◊ виртуальная локальная (VLAN) 212, 213, 215, 217
  ▫ асимметричная 257, 259
  ▫ динамическая 214, 227
  ▫ принципы построения 212
  ▫ распределенная 217
  ▫ статическая 213
  ▫ типы портов 222
  ▫ управление 224
  ▫ частная (Private VLAN) 260
◊ волоконно-оптическая/коаксиальная (HFC) 31, 549
◊ полностью-оптическая сеть Ethernet (AOEN) 46
◊ телефонная общего пользования (ТфОП) 65
Сигнальный шлюз (MGC) 142
Скорость модальная 460
Сообщения:
◊ BPDU 278
◊ BPDU-C 278—280
◊ BPDU-TCN 278, 280
Соотношение сигнал/шум 53, 559
Спецификация 1000Base X 454
Спрайт 559
Среда передачи данных (PMA) 459
Стандарт:
◊ IEEE 802.11 39
◊ IEEE 802.16 41
  ▫ WirelessMAN-OFDM 42
  ▫ WirelessMAN-OFDMA 42
  ▫ WirelessMAN-SC 41
  ▫ WirelessMAN-SCA 41
◊ ISO 7498 178
Страница:
◊ неформатированная (AN-UP) 489
◊ сообщения (AN-MP) 489
Стратегия:
◊ TD 418
◊ WRED 418
Структура SMI 511
Структурированная кабельная система (СКС) 480
Схема ортогонального частотного мультиплексирования (OFDM) 40, 554
Схема прямого расширения спектра (DSSS) 40, 545

T

Телевидение:
◊ ATSC 112
◊ DVB 112, 545
◊ IPTV 113, 550
  ▫ базовые (канальные) услуги 113
  ▫ интерактивные телематические услуги 113, 114
  ▫ расширенные (избираемые) услуги 113
◊ ISDB 112, 550
◊ высокой четкости (ТВЧ) 94
◊ квадратурная амплитудная модуляция (QAM) 112

Телевидение *(прод.)*:
◊ коаксиальные кабельные сети (CS) 111
◊ однополосная амплитудная модуляция (VSB) 112
◊ сети ближнего вещания (TS) 111
◊ сети высокочастотного вещания (MS) 111
◊ спутниковые каналы (SS) 111
◊ фазовая манипуляция (PSK) 112, 556
Технология:
◊ 1000Base-CX 454
◊ 1000Base-LX 454
◊ 1000Base-SX 454
◊ 1000Base-T 454
◊ ADPCM 541
◊ APON 542
◊ ATM 2, 24, 541
◊ BPON 542
◊ eXpandable Resilient Networking (XRN) 339, 563
◊ FDDI 439—442, 444
◊ Frame Relay (FR) 2, 19
◊ GPON 548
◊ IEEE 802.1Q 220
◊ ISDN 2, 12, 550
◊ ISL 219, 550
◊ NetFlow 521, 553
▫ особенности применения 522, 525
◊ SDH 474
◊ TDM 12, 560
◊ Token Ring/IEEE 802.5 435
◊ Wi-Fi 39, 563
◊ X.25 563
◊ волнового мультиплексирования (WDM) 471, 563
Точка доступа 39, 542
Трансивер 477, 478
Трансляция сетевых адресов 553
Трафик:
◊ групповой:
▫ режим DENSE 381
▫ режим SPARSE 382
◊ жесткий метод регулирования (policing) 391
◊ классы обслуживания (CoS) 391
◊ мягкий метод регулирования (shaping) 391
◊ одноадресный (Unicast-трафик) 212
◊ реального времени 161
◊ широковещательный (Broadcast-трафик) 212

У

Уровень:
◊ PCS 453, 455, 462, 468, 469, 474—476, 555
◊ PMA 453, 555
◊ PMD 453
◊ STM-64 476
◊ WIS 475, 476
◊ доступа 541
Утилита NETSTAT 215, 216

Ф

Физическая среда (PMD) 459
Физические шлюзы (MG) 70
Физический адрес Ethernet 183
Формат:
◊ BIFS 542
◊ CIF 543
Функция:
◊ Port Security 263, 555
◊ RPF 386

Ц

Цветное телевидение:
◊ стандарт:
▫ NTSC 81, 554
▫ PAL 82, 554
▫ SECAM 82, 559
Центр обработки вызовов 77
Цифровое телевидение:
◊ повышенной четкости (HDTV) 108, 109, 549
◊ сверхвысокой четкости (UHDV) 108, 561
◊ стандартной четкости (SDTV) 108, 109, 558

Ш

Шлюз 548
◊ по умолчанию 317
Шум квантования 56

Э

ЭИИМ 40
Эффективность использования пропускной способности канала передачи данных 181

Я

Язык:
◊ DDL 544
◊ VRML 563



АЛЕКСАНДР ФИЛИМОНОВ

ПОСТРОЕНИЕ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ ETHERNET

Формирование и кодирование потоков VoIP, IPTV

Регулирование и учет трафика абонентских соединений

Управление доступом к сетевым ресурсам

Резервирование каналов связи ЛВС с динамическим распределением нагрузки

Создание масштабируемых и высокопроизводительных магистральных соединений

СИСТЕМНЫЙ АДМИНИСТРАТОР