



Программа Сетевой академии
Cisco CCNA® 3 и 4
Вспомогательное руководство
Третье издание

Одобрено Cisco Systems, Inc. в качестве учебного пособия для
программы Сетевой академии

© 2008 Cisco и/или ее дочерние компании.
Все права защищены.
Cisco, Cisco Press и CCNA являются
торговыми марками Cisco Systems, Inc.

ISBN 978-0-7897-5304-0
0-7897-5304-0



Cisco Networking Academy Program CCNA® 3 and 4 Companion Guide

Third Edition

Cisco Systems, Inc.
Cisco Networking Academy Program

Cisco Press

800 East 96th Street
Indianapolis, Indiana 46240 USA
www.ciscopress.com

ББК 32.973.26-018.2.75

П78

УДК 681.3.07

Издательский дом "Вильямс"

Зав. редакцией С.Н. Тригуб

Перевод с английского и редакция А.Н. Крикуна

По общим вопросам обращайтесь в Издательский дом "Вильямс" по адресу:

info@williamspublishing.com, <http://www.williamspublishing.com>

127055, Москва, а/я 783; 03150, Киев, а/я 152

Cisco Systems, Inc.

П78 Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство. : Пер. с англ. — М. : ООО "И.Д. Вильямс", 2007. — 994 с. : ил. — Парал. тит. англ.

ISBN 5-8459-1120-6 (рус.)

Третье издание "Руководства к программе курса Сетевой академии Cisco для подготовки к сертификационному экзамену CCNA (часть 3 и 4)" дополняет учебные материалы и лабораторные работы программы Сетевой академии Cisco. Этот учебный курс позволяет читателю успешно работать или продолжить обучение и получение практических навыков в сфере компьютерных сетей. Настоящая книга является дополнением электронных материалов, уже использованных в данной программе. В ней также затрагиваются темы, относящиеся к экзамену на получение сертификата Cisco Certified Network Associate (CCNA). Изложение материала в книге строго следует стилю и формату учебного курса Cisco. Кроме того, к книге прилагается компакт-диск (CD-ROM), который содержит образовательные видеоклипы, лабораторные работы и фотографии, а также практические вопросы для подготовки к экзамену; все эти материалы представлены в интерактивном мультимедийном формате как справочные образовательные материалы.

ББК 32.973.26-018.2.75

Все названия программных продуктов являются зарегистрированными торговыми марками соответствующих фирм.

Никакая часть настоящего издания ни в каких целях не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, включая фотокопирование и запись на магнитный носитель, если на это нет письменного разрешения издательства Cisco Press.

Authorized translation from the English language edition published by Cisco Press, Copyright © 2004 Cisco Systems, Inc.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from the Publisher.

Russian language edition published by Williams Publishing House according to the Agreement with R&I Enterprises International, Copyright © 2007

Книга подготовлена при участии Региональной сетевой академии Cisco, <http://www.academy.ciscopress.ru>.

ISBN 5-8459-1120-6 (рус.)

ISBN 1-58-713113-7 (англ.)

© Издательский дом "Вильямс", 2007

© Cisco Systems, Inc., 2004

Оглавление

Часть I. Обзор	41
Глава 1. Эталонная модель OSI и маршрутизация	43
Часть II. CCNA 3: Основы коммутации и промежуточной маршрутизации	75
Глава 2. Начальные сведения о маршрутизации по адресам без классов	77
Глава 3. Протокол OSPF для отдельной зоны	107
Глава 4. Усовершенствованный протокол маршрутизации внутреннего шлюза	147
Глава 5. Коммутация в локальных сетях и проектирование локальных сетей	177
Глава 6. Коммутаторы	235
Глава 7. Конфигурирование коммутаторов	259
Глава 8. Протокол связующего дерева STP	291
Глава 9. Виртуальные локальные сети	319
Глава 10. Магистральный протокол VLAN	347
Часть III. CCNA 4: Технологии распределенных сетей WAN	377
Глава 11. Масштабирование IP-адресов	379
Глава 12. Технологии распределенных сетей WAN	411
Глава 13. Протокол PPP	465
Глава 14. Технология ISDN и маршрутизация DDR	501
Глава 15. Протокол Frame Relay	541
Глава 16. Введение в сетевое администрирование	575
Часть IV. Дополнительный материал для теста CCNA	619
Глава 17. Основы оптических сетей	621
Глава 18. Управление сетями	651
Глава 19. Обзор тем и программа экзамена Network+	697
Глава 20. Программа экзамена на сертификат CCNA	767
Глава 21. Начальные сведения о конвергированных сетях	825
Глава 22. Разработка стратегии обеспечения безопасности и управления сетью	843
Глава 23. Виртуальные частные сети	865
Часть V. Приложения	883
Приложение А. Глоссарий	885
Приложение Б. Ответы на контрольные вопросы	911
Предметный указатель	929

Содержание

Студентам	27
О технических редакторах	27
Пиктограммы сетевых устройств и соединений, используемые корпорацией Cisco Systems	29
Обозначения, используемые в командах	30
Цели книги	33
Для кого предназначена эта книга	33
Организация материала книги	34
Структура книги	34
Прилагаемый компакт-диск	37
От издательского дома "Вильямс"	38
Часть I. Обзор	41
Глава 1. Эталонная модель OSI и маршрутизация	43
Многоуровневая модель сети: эталонная модель OSI	44
Обмен информацией между устройствами одного ранга	45
Инкапсуляция данных	47
Физический уровень	48
Физические соединения сетей Ethernet 802.3	49
Канальный уровень	50
Интерфейс сети Ethernet/802.3	51
Сетевой уровень	51
IP-адресация и подсети	51
Определение пути	52
Обмен информацией о путях	53
Протокол ICMP	54
Протокол ARP	55
Маршрутизация	56
Маршрутизируемые протоколы и протоколы маршрутизации	59
Конфигурирование IP-маршрутизации	62
Транспортный уровень	63
Сегментирование приложений верхнего уровня	64
Установка соединения	64
Передача данных	65
Повышение надежности передачи путем создания окон	66
Способы подтверждения	66

Резюме	67
Основные термины	68
Контрольные вопросы	72
Часть II. CCNA 3: основы коммутации и промежуточной маршрутизации	75
Глава 2. Начальные сведения о маршрутизации по адресам без классов	77
Обзор маршрутизации по адресам без классов	77
Для чего используется адресация CIDR?	77
Обобщение маршрутов и создание суперсетей	78
Суперсети и выделение адресов	80
Использование масок подсети переменной длины	81
Функции масок VLSM	81
Вычисление масок VLSM	84
Конфигурирование маски VLSM	86
Использование масок VLSM протоколами RIP и IGRP	87
Обобщение маршрутов	88
Обобщение маршрутов в октете	90
Обобщение маршрутов во фрагментарной сети	90
Флэппинг маршрутов	91
Протокол RIP версии 2	92
Краткая история протокола RIP	92
Функции протокола RIP версии 2	93
Сравнение протоколов RIPv1 и RIPv2	94
Конфигурирование протокола RIP версии 2	95
Тестирование протокола RIP V2	97
Устранение ошибок конфигурирования протокола RIP	99
Стандартные маршруты	100
Резюме	102
Глоссарий	103
Контрольные вопросы	103
Глава 3. Протокол OSPF для отдельной зоны	107
Основные понятия протокола OSPF для одной зоны	107
Обзор протокола OSPF	108
Терминология протокола OSPF	108
Состояния протокола OSPF	110
Сравнение протокола OSPF с дистанционно-векторными протоколами маршрутизации	114
Алгоритм выбора кратчайшего пути	116
Типы сетей протокола OSPF	116
Протокол приветствия (Hello) стека протоколов OSPF	118
Операции протокола OSPF	119

Установка отношений смежности	119
Выбор назначенного маршрутизатора и резервного назначенного маршрутизатора	120
Обнаружение маршрутов	122
Выбор наилучшего маршрута	122
Поддержка информации о маршрутах	123
Конфигурирование протокола OSPF для одной зоны	125
Конфигурирование адреса петлевого интерфейса	126
Изменение приоритета OSPF-маршрутизатора	127
Изменение метрики, используемой протоколом OSPF для присвоения оценки каналу	129
Конфигурирование аутентификации в протоколе OSPF	130
Конфигурирование таймеров протокола OSPF	131
Конфигурирование протокола OSPF в сетях NBMA	131
Полносвязные сети Frame Relay	133
Сети Frame Relay с частично-связной топологией	135
OSPF-сеть типа "точка-несколько точек"	137
Распространение в сети маршрута по умолчанию	138
Общие вопросы конфигурирования протокола OSPF	139
Тестирование конфигурации протокола OSPF	140
Резюме	140
Глоссарий	142
Контрольные вопросы	143
Глава 4. Усовершенствованный протокол маршрутизации внутреннего шлюза	147
Обзор протокола EIGRP	147
Процессы и технологии протокола EIGRP	148
Преимущества использования протокола EIGRP:	150
Независимость от маршрутизируемых протоколов	151
Терминология протокола EIGRP	151
Таблица соседних устройств	151
Топологическая таблица	152
Первичные маршруты	154
Резервные маршруты	154
Выбор первичного маршрута и резервных маршрутов	154
Застревание активных маршрутов	156
Таблица маршрутизации	156
Создание тегов для маршрутов	156
Функции и технологии протокола EIGRP	157
Обнаружение соседних устройств и восстановление утраченной с ними связи	158
Надежный транспортный протокол	159
Машина конечных состояний алгоритма DUAL	159
Модули PDM	160

Типы пакетов протокола EIGRP	161
Пакеты приветствия	161
Пакеты подтверждения	162
Пакеты обновлений маршрутов	162
Пакеты запросов и ответов на запросы	163
Конвергенция протокола EIGRP	163
Конфигурирование протокола EIGRP	165
Конфигурирование протокола EIGRP для IP	165
Конфигурирование полосы пропускания в сетях NBMA	167
Конфигурирование полосы пропускания в многоточечной сети	167
Конфигурирование полосы пропускания в гибридной многоточечной сети	168
Использование команды <code>ip bandwidth-percent</code>	168
Конфигурирование обобщения маршрутов протокола EIGRP	170
Тестирование базовой конфигурации протокола EIGRP	171
Резюме	172
Глоссарий	173
Контрольные вопросы	174
 Глава 5. Коммутация в локальных сетях и проектирование локальных сетей	 177
Локальные сети спецификации Ethernet/802.3	177
История развития сетей Ethernet/802.3	177
Факторы, влияющие на производительность сети	182
Элементы сетей Ethernet/802.3	183
Полудуплексные сети Ethernet	183
Дуплексные сети Ethernet	184
Начальные сведения о коммутации в локальных сетях	185
Сегментация в локальных сетях	186
Сегментация с использованием мостов	188
Сегментация с использованием маршрутизаторов	189
Сегментация с использованием коммутаторов	190
Основные операции коммутатора	192
Задержка в коммутаторах сетей Ethernet	195
Коммутация на 2-м и 3-м уровнях	195
Смысл коммутации 2-го и 3-го уровня	197
Симметричная и асимметричная коммутация	198
Буфер памяти	199
Проектирование локальных сетей	199
Цели проекта локальной сети	200
Компоненты сетевого проекта	201
Функции и размещение серверов	201
Сегментация	202
Методология проектирования сети	203

Доступность и поток данных в сети	205
Проектирование сетевой топологии	205
Проектирование на 1-м уровне	205
Проектирование 2-го уровня топологии локальной сети	212
Использование маршрутизаторов для логического структурирования	220
Основы применения мостов и коммутаторов на 2-м уровне	223
Фильтрация фреймов коммутаторами и мостами	225
Типы фильтрации	225
Резюме	226
Ключевые термины	227
Контрольные вопросы	230
Глава 6. Коммутаторы	235
Обзор коммутаторов	235
Включение коммутатора	236
Включение коммутатора Catalyst	236
Светодиодные индикаторы коммутатора	238
Поведение индикаторов порта LED во время автотестирования коммутатора	240
Вывод информации о первоначальной загрузке коммутатора	241
Получение справки из командной строки интерфейса коммутатора	244
Коммутаторы сетей и иерархическое проектирование сети	246
Базовый уровень	248
Уровень распределения	248
Уровень доступа	248
Обзор уровня доступа в коммутируемых локальных сетях	248
Коммутаторы уровня доступа	249
Обзор уровня распределения	250
Коммутаторы уровня распределения	251
Обзор базового уровня	253
Коммутаторы базового уровня	253
Резюме	255
Глоссарий	255
Контрольные вопросы	256
Глава 7. Конфигурирование коммутаторов	259
Микросегментация	259
Микросегментация	261
Как коммутатор узнает адреса устройств	263
Пересылка данных коммутатором	265
Пересылка данных с промежуточным хранением	265
Сквозная пересылка	266
Симметричная коммутация	267
Асимметричная коммутация	268
Использование буфера памяти	268

Коммутаторы и коллизийные домены	269
Коммутаторы и широкополосные домены	270
Связь между коммутаторами и персональными компьютерами	273
Передача данных от персонального компьютера к коммутатору	273
Осуществление связи между коммутаторами	273
Тестирование начальной конфигурации коммутатора Catalyst	274
Тестирование стандартной конфигурации коммутатора Catalyst	274
Свойства портов коммутатора	275
Свойства виртуальной локальной сети VLAN	276
Флэш-каталог (Flash Directory)	276
Отображение информации о версии операционной системы IOS	277
Преимущества использования стандартной конфигурации	278
Изменение сетевых установок коммутатора Catalyst	278
Изменение стандартных установок коммутатора	278
Назначение коммутатору имени и задание паролей	279
Назначение коммутатору IP-адреса и шлюза по умолчанию	279
Установка характеристик порта	279
Web-интерфейсы	281
Работа с таблицей MAC-адресов	281
Конфигурирование статических MAC-адресов	283
Меры безопасности для портов коммутаторов	283
Добавление, перемещение и изменение подключения устройств к коммутатору	284
Управление образами операционной системы и файлами конфигурации устройств	285
Восстановление пароля на коммутаторах серий 1900/2950	286
Обновление микропрограммы и IOS коммутаторов 1900/2900	286
Резюме	286
Глоссарий	287
Контрольные вопросы	288
Глава 8. Протокол связующего дерева STP	291
Обзор топологий с избыточностью	291
Что понимается под избыточностью в сети	291
Топологии с избыточностью	292
Избыточность в сетях с коммутацией	292
Широкополосные штормы	293
Множественная передача фреймов	294
Неустойчивость базы данных MAC-адресов	295
Обзор протокола связующего дерева	295
Работа протокола связующего дерева	297
Использование связующего дерева для создания свободной от петель топологии сети	298
Расширенные функции протокола STP	299

Выбор корневого моста	300
Последовательность состояний порта в протоколе связующего дерева	302
Выбор назначенных портов	304
Оценка маршрута	307
Таймеры протокола STP	308
Перерасчет связующего дерева	311
Конвергенция сети	311
Протокол RSTP	312
Состояния портов в протоколе RSTP	312
Переход в состояние пересылки	313
Резюме	314
Глоссарий	314
Контрольные вопросы	315
Глава 9. Виртуальные локальные сети	319
Начальные сведения о сетях VLAN	319
Широковещательные домены в сетях VLAN и маршрутизаторы	322
Функционирование сети VLAN	323
Сквозные VLAN-сети	326
Географические VLAN-сети	327
Преимущества сетей VLAN	327
Изменения в системе управления сетью	327
VLAN-сети и безопасность	328
Использование концентраторов в сетях VLAN	330
Типы VLAN-сетей	331
Идентификация фреймов в сетях VLAN	331
Теги фреймов в спецификации IEEE 802.1Q	331
Протокол межкоммутаторного канала	332
Спецификация FDDI 802.10	332
Эмуляция локальной сети	333
Конфигурирование VLAN	334
Конфигурирование статических VLAN-сетей	334
Тестирование конфигурации VLAN-сети	336
Сохранение конфигурации VLAN	336
Удаление конфигурации VLAN-сети	337
Устранение ошибок в конфигурации VLAN-сети	338
Резюме	340
Глоссарий	341
Контрольные вопросы	342
Глава 10. Магистральный протокол VLAN	347
Магистральные соединения	347
Понятие магистральной	348

Функционирование магистралей	349
Сети VLAN и магистральные каналы	350
Интерфейс командной строки коммутатора	351
Реализация магистральных соединений	352
Протокол магистральных соединений виртуальных локальных сетей VLAN	354
История протокола VTP	354
Общие положения протокола VTP	355
Преимущества использования протокола VTP	355
Домен протокола VTP	356
Режимы протокола VTP	356
Реализация протокола VTP	358
Конфигурирование протокола VTP	360
Отсечение каналов в протоколе VTP	364
Межсетевая VLAN-маршрутизация	365
Взаимодействие между VLAN-сетями и решение возникающих проблем	366
Изолированные широковебательные домены	367
Нахождение маршрута между VLAN-сетями	369
Физические и логические интерфейсы	370
Создание подынтерфейсов на физическом интерфейсе	370
Конфигурирование маршрутизации между VLAN-сетями	370
Резюме	372
Глоссарий	372
Контрольные вопросы	373
Часть III. CCNA 4: технологии распределенных сетей WAN	377
Глава 11. Масштабирование IP-адресов	379
Обзор протокола Internet	379
Адресации NAT и PAT	382
Функции NAT и PAT	386
Конфигурирование NAT и PAT	387
Тестирование конфигурации NAT и PAT	392
Поиск и устранение ошибок в конфигурировании NAT и PAT	393
Преимущества и недостатки NAT	395
Обзор протокола DHCP	396
Установка в сети протокола DHCP	397
Различия между протоколами BOOTP и DHCP	399
Функции протокола DHCP	399
Функционирование протокола DHCP	400
Конфигурирование протокола DHCP	402
Тестирование работы протокола DHCP	403
Поиск и устранение ошибок в конфигурации DHCP	404
Передача DHCP	404

Резюме	407
Глоссарий	408
Контрольные вопросы	408
Глава 12. Технологии распределенных сетей WAN	411
Обзор технологий распределенных сетей WAN	411
Устройства сетей WAN	414
Стандарты сетей WAN	416
Инкапсуляция в распределенных сетях	418
Варианты соединений WAN-сетей	419
Соединения с коммутацией каналов	419
Соединения с коммутацией пакетов	419
Коммутация пакетов и каналов	420
Технологии WAN-сетей	422
Аналоговые соединения удаленного доступа	423
Технология ISDN	424
Выделенные линии	425
Технология X.25	426
Технология Frame Relay	427
Технология ATM	428
Технология DSL	429
Кабельные модемы	430
Осуществление связи в распределенных сетях	432
Интеграция локальных и распределенных сетей	436
Идентификация и выбор модели сети	438
Иерархическая модель проектирования сети	439
Трехуровневая модель проектирования	439
Компоненты трехуровневой модели	442
Преимущества иерархического подхода к проектированию сети WAN	445
Размещение серверов	446
Проектирование распределенных сетей WAN	449
Этапы проектирования распределенной сети WAN	449
Сбор требований	452
Анализ требований пользователей	453
Тестирование чувствительности сети	455
Топологии распределенных сетей	455
Идентификация сети и выбор сетевых возможностей	457
Другие аспекты проектирования WAN-сети	458
Резюме	459
Глоссарий	460
Контрольные вопросы	461
Глава 13. Протокол PPP	465
Уровневая архитектура протокола PPP	466
Установка сеанса протокола PPP	470

Протоколы аутентификации сеанса PPP	471
Протокол аутентификации по паролю PAP	472
CHAP	472
Инкапсуляция протокола PPP и процесс аутентификации	473
Последовательные каналы типа "точка-точка"	477
Мультиплексирование с разделением времени	478
Точка демаркации	479
Устройства DTE и DCE	480
Инкапсуляция по протоколу HDLC	482
Конфигурирование инкапсуляции протокола HDLC	483
Устранение ошибок и неисправностей на серийном интерфейсе	484
Конфигурирование протокола PPP	490
Конфигурирование инкапсуляции протокола PPP	491
Конфигурирование аутентификации протокола PPP	492
Тестирование конфигурации инкапсуляции PPP в последовательном канале	494
Устранение ошибок конфигурирования инкапсуляции PPP в последовательном канале	495
Резюме	496
Глоссарий	497
Контрольные вопросы	497
Глава 14. Технология ISDN и маршрутизация DDR	501
Стандарты ISDN	501
Обзор технологии ISDN	502
Стандарты ISDN и методы доступа	506
3-уровневая модель ISDN и протоколы	508
Установка вызова ISDN	510
Функции ISDN и контрольные точки	513
Определение ISDN-интерфейса на маршрутизаторе	515
Типы коммутаторов ISDN	515
Конфигурирование интерфейса BRI ISDN	517
Конфигурирование PRI-интерфейса ISDN	520
Тестирование конфигурации ISDN	522
Устранение ошибок в конфигурации ISDN	524
Маршрутизация DDR	525
Функционирование маршрутизации DDR	526
Унаследованная DDR	527
Задание статических маршрутов для DDR	527
Задание критериев для представляющих интерес данных	528
Конфигурирование информации номеронабирателя DDR	529
Профили набора	531

Конфигурирование профилей набора	532
Тестирование конфигурации DDR	533
Резюме	534
Глоссарий	535
Контрольные вопросы	536
Глава 15. Протокол Frame Relay	541
Обзор протокола Frame Relay	541
Терминология протокола Frame Relay	542
Функционирование протокола Frame Relay	545
Формат фрейма протокола Frame Relay	547
Адресация протокола Frame Relay	548
Реализация протокола Frame Relay в маршрутизаторах Cisco — LMI	548
Функционирование LMI	549
Дополнительные возможности интерфейса локального управления (LMI)	549
Формат LMI-фрейма	550
Глобальная адресация	551
Многоадресная передача	551
Инверсный протокол ARP	552
Отображение в протоколе Frame Relay	552
Таблицы коммутации протокола Frame Relay	553
Развертывание службы протокола Frame Relay	554
Подынтерфейсы протокола Frame Relay	555
Среды с расщеплением горизонта	556
Разрешение проблем достижимости посредством использования подынтерфейсов	557
Базовая конфигурация протокола Frame Relay	558
Конфигурирование последовательного интерфейса для подключения по протоколу Frame Relay	559
Проверка работоспособности протокола Frame Relay на последовательном интерфейсе	559
Тестирование протокола Frame Relay	560
Проверка работоспособности канала	561
Проверка наличия карты отображения	562
Проверка связи с маршрутизатором центрального сайта	562
Конфигурирование подынтерфейсов	563
Необязательные команды конфигурирования	565
Резюме	567
Глоссарий	567
Контрольные вопросы	569
Глава 16. Введение в сетевое администрирование	575
Обзор настольных компьютеров и серверных операционных систем	575
Рабочие станции	576

Серверы	578
Связи между клиентами и серверами	581
Сетевые операционные системы NOS	584
Операционные системы Windows NT, Windows 2000 Windows .NET	587
Операционные системы UNIX и Linux	590
Операционная система Macintosh OS X	595
Концепция серверной службы	596
Совместное использование файлов	597
Протокол FTP и передача файлов	597
Web-службы	597
Служба DNS	598
Служба DHCP	598
Управление сетью	598
Эталонная модель OSI и модель управления сетью	600
Стандарты: SNMP и CMIP	601
Функционирование протокола SNMP	601
Структура информации управления сетью и баз данных MIB	606
Протокол SNMP	607
Конфигурирование протокола SNMP	611
Удаленный мониторинг (RMON)	612
Утилита Syslog	613
Резюме	615
Глоссарий	615
Контрольные вопросы	615
Часть IV. Дополнительный материал для теста CCNA	619
Глава 17. Основы оптических сетей	621
Основные элементы оптических сетей	621
Движущие силы развития технологий оптических сетей	621
Оптоволоконные системы	622
Система передачи данных по оптоволоконному кабелю	623
Свет	624
Типы оптоволоконных кабелей	629
Геометрия оптоволоконного кабеля	630
Ослабление сигнала	633
Оптические фильтры	634
Оптические усилители	635
Оптическая передача и мультиплексирование	636
Технология SONET	636
Иерархия мультиплексирования SONET	640
Системы DWDM	640
Резюме	644
Глоссарий	645
Контрольные вопросы	647

Глава 18. Управление сетями	651
Сетевая документация	651
Схемы главного и промежуточного распределительного шкафа	652
Подробности конфигурации сервера и рабочей станции	652
Перечни установленного программного обеспечения	652
Регистрация работ по обслуживанию компьютера	652
Меры по обеспечению безопасности в сети	653
Политика безопасности в отношении пользователей	656
Обеспечение безопасности сети	657
Восстановление данных	657
Операции резервирования данных	658
Избыточность	660
Внешние факторы	662
Требования к электрическому питанию	663
Электромагнитные наводки и радиопомехи	663
Компьютерные вирусы	663
Производительность сети	664
Администрирование серверов	666
Сеть "Клиент-сервер"	667
Управление сетью	670
Административный аспект управления сетью	672
Границы сети	673
Затраты на сеть	673
Регистрация проблем при работе сети	674
Мониторинг сети	674
Мониторинг сетевых соединений	675
Мониторинг передаваемых данных	675
Протокол SNMP	676
Удаленный мониторинг	677
Устранение ошибок в сети	680
Процесс поиска и устранения причин сбоев в сети	681
Методы устранения неисправностей	682
Программные средства устранения неисправностей	688
Команда ping	688
Команда telnet	690
Команда netstat	690
Команда arp	691
Резюме	692
Глоссарий	693
Глава 19. Обзор тем и программа экзамена Network+	697
Базовые топологии сетей	697
Звездообразная топология	698
Шинная топология	698

Сеточная топология	699
Кольцевая топология	700
Топология беспроводной сети	701
Сегменты и магистрали	702
Сегменты	702
Магистрали	702
Основные сетевые операционные системы	702
Операционная система Microsoft Windows 2000 Server	703
Операционная система Windows XP	705
Операционная система Novell NetWare	706
Операционная система UNIX	707
Операционная система Linux	707
Операционная система MAC OS X	709
Службы каталогов Windows	709
Организационные модули ОС Windows 2000	710
Активный каталог и система доменных имен	710
Серверы активного каталога	710
Репликация активного каталога	711
Безопасность активного каталога	711
Совместимость службы активного каталога с другими службами	712
Службы каталогов Novell NetWare	712
Служба каталогов UNIX	712
Протоколы IP, IPX и NetBEUI: их связь с выполняемыми функциями	712
Протокол IP	712
Протокол IPX	713
Расширенный интерфейс пользователя NetBIOS	713
Обзор избыточного массива недорогих дисков RAID	713
Система RAID нулевого уровня	714
Система RAID 1-го уровня	715
Система RAID 2-го уровня	716
Система RAID 3-го уровня	716
Система RAID 4-го уровня	717
Система RAID 5-го уровня	717
Система RAID 0/1	717
Зеркальное копирование	718
Дуплексирование диска	718
Расслоение данных	719
Тома	719
Эталонная модель OSI	719
Уровень приложений	719
Уровень представления данных	720
Сеансовый уровень	720
Транспортный уровень	721
Сетевой уровень эталонной модели OSI	721
Канальный уровень эталонной модели OSI	722

Физический уровень эталонной модели OSI	723
Сетевая среда передачи сигналов	723
Коаксиальный кабель	723
Кабель UTP 3-й категории и экранированная витая пара	724
Кабель UTP 5-й категории и экранированная витая пара	724
Оптоволоконный кабель	724
Неэкранированная витая пара	725
Экранированная витая пара	726
Узкополосная передача сигналов	727
10BASE-2	727
10BASE-5	727
10BASE-T	727
100BASE-T	728
Технологии 100BASE-TX и 100BASE-T4	728
Технология 100BaseVG-AnyLAN	728
Технологии 100BASE-FX и Gigabit Ethernet	728
Дуплексный и полудуплексный режимы передачи	729
Распределенные сети WAN и локальные сети LAN	729
Серверы, рабочие станции и узлы	729
Сети на основе серверов и одноранговые сети	729
Кабели, карты сетевого интерфейса и маршрутизаторы	730
Широкополосная и узкополосная сигнализация	730
Шлюзы	731
Анализ работы физического уровня сети	731
Концентраторы	733
Модули множественного доступа	734
Коммутирующие концентраторы	734
Повторители	734
Трансиверы	734
Канальный уровень эталонной модели OSI	735
Управление логическим каналом по стандарту 802.2	735
Стандарт 802.3 Ethernet	735
Стандарт 802.5 Token Ring	735
Беспроводные сети спецификации 802.11b	736
Функции и характеристики MAC-адресов	736
Сетевой уровень	736
Маршрутизатор	737
Брутеры	737
Различия между маршрутизируемыми и немаршрутизируемыми протоколами	737
Стандартный шлюз и подсети	737
Причины использования уникальных сетевых адресов	738
Различия между статической и динамической маршрутизацией	738
Транспортный уровень	739
Цели преобразования имен и адресов	739

Основы стека протоколов TCP/IP	739
Стандартные шлюзы	740
Протоколы DHCP, DNS, WINS и файлы хостов	740
Служба DNS	740
Служба имен Internet в Windows (WINS)	740
Файлы HOSTS	741
Протокол TCP	741
Протокол IP	743
Система доменных имен Internet	743
Адреса классов А, В и С и их стандартные маски подсетей	743
Номера портов	745
Прокси-серверы и причины их использования	745
Конфигурирование рабочей станции	745
IP-адреса и маски подсетей	745
Стандартные шлюзы и их маски подсетей	746
Имя узла	746
Имя домена в Internet	746
Стек протоколов TCP/IP: утилиты	746
Использование протокола Telnet для тестирования, и устранения ошибок в соединениях протокола IP	747
Использование nbtstat для тестирования и устранения ошибок в соединениях протокола IP	747
Использование команды tracert для тестирования и устранения ошибок в соединениях протокола IP	747
Использование команды netstat для тестирования и устранения ошибок в соединениях протокола IP	748
Использование команд ipconfig/winipconfig для тестирования, объявления действительными и устранения ошибок в соединениях протокола IP	749
Использование протокола FTP для тестирования и устранения ошибок в соединениях протокола IP	749
Использование команды ping для тестирования и устранения неисправностей в IP-соединениях	750
Протоколы PPP и SLIP	750
Назначение и функции протокола PPTP	751
ISDN и PSTN (POTS)	751
Конфигурация модема для работы в коммутируемой сети	752
Требования для удаленного соединения	752
Безопасность	752
Стандартные приемы и процедуры создания паролей	753
Шифрование данных	754
Использование брандмауэра	754
Администрирование	754
Влияние факторов окружающей среды на компьютерные сети	755
Общие внешние порты	756

Внешние SCSI-соединения	756
Серверы печати	756
Коммутационные панели	756
Источники бесперебойного питания	756
Сетевые платы	757
Обслуживание и поддержка сети	758
Стандартные процедуры резервного копирования и практика использования резервных накопителей	758
Необходимость периодического применения исправлений и обновлений программного обеспечения в сети	759
Необходимость устанавливать антивирусное программное обеспечение на сервере и рабочей станции	759
Необходимость частого обновления сигнатур вирусов	760
Поиск и устранение неисправностей сети	760
Определение принадлежности проблемы (проблема оператора или проблема системы)	760
Проверка физических и логических индикаторов неисправности	761
Определение проблемы при известных обстоятельствах сетевой неполадки	762
Резюме	762
Глоссарий	763
Глава 20. Программа экзамена на сертификат CCNA	767
Эталонная модель OSI	767
Уровень приложений	767
Уровень представления данных	768
Сеансовый уровень	768
Транспортный уровень	768
Сетевой уровень	769
Канальный уровень	769
Физический уровень	770
Применение мостов и коммутаторов	770
Дуплексный и полудуплексный режимы Ethernet	770
Различия между сквозной коммутацией в сети LAN и коммутацией с промежуточным хранением	772
Функционирование и преимущества виртуальных локальных сетей	773
Маршрутизируемые протоколы	774
Использование различных классов IP-адресов, включая адреса подсетей и частные адреса	774
Подсети	775
Преобразование чисел в двоичный, десятичный и шестнадцатеричный формат	779
Протоколы маршрутизации	781
Внешние и внутренние протоколы маршрутизации	785
Включение на маршрутизаторе протоколов RIP и IGRP	786
Вычисление метрик маршрутизации в протоколах IGRP и RIP	787

Сравнение дистанционно-векторных протоколов, протоколов состояния канала связи и гибридных протоколов и их основных операций	788
Протоколы распределенных сетей WAN	792
Ключевые термины и функции протокола Frame Relay	792
Различия между технологиями LAPB, Frame Relay, ISDN/LAPD, HDLC, PPP и DDR	793
Конфигурирование интерфейса BRI ISDN и унаследованной DDR	795
Управление файлом конфигурации с использованием протокола TFTP	796
Как загрузить резервную копию образа программного обеспечения?	798
Управление файлом конфигурации	798
Управление образами IOS с помощью протокола TFTP	800
Протокол управляющих сообщений Internet	801
Доставка сообщений протокола ICMP	802
Сообщения об ошибках и их исправление	803
Недостижимые сети	803
Использование команды ping для тестирования достижимости пункта назначения	805
Списки управления доступом	807
Обзор списков управления доступом	807
Причины создания списков управления доступом	808
Оборудование Cisco, программное обеспечение IOS и основы функционирования сети Cisco	809
Вывод первоначальной информации при загрузке маршрутизатора	810
Установка сеанса программы HyperTerminal	811
Вход на маршрутизатор	812
Получение справки с клавиатуры	812
Команды редактирования операционной системы Cisco IOS	815
История выполненных на маршрутизаторе команд	815
Устранение ошибок в командах	816
Назначение операционной системы Cisco IOS	817
Функционирование Cisco IOS	817
Функции Cisco IOS	818
Команда show version	818
Пользовательский интерфейс маршрутизатора	819
Устранение ошибок в Cisco IOS	820
Резюме	822
Глоссарий	822
Глава 21. Начальные сведения о конвергированных сетях	825
Введение	825
Традиционные сети	825
Начальные сведения о сетях для передачи голосовых и обычных данных	825
Передача голосовых данных по сети Frame Relay	827
Передача голосовых данных по сетям ATM	828
Передача голосовых данных по сетям IP	829

Сравнение различных технологий передачи голоса по сетям передачи данных	830
Сети передачи голосовых, видео и обычных данных	830
Архитектура AVVID Cisco	831
Приложения конвергированных сетей	833
Общие вопросы качества обслуживания QoS	836
Задержка	836
Дребезжание звука	837
Утерянные пакеты	838
Эхо-сигнал	838
Технология качества обслуживания QoS в программном обеспечении IOS Cisco	839
Резюме	839
Глоссарий	840
Глава 22. Разработка стратегии обеспечения безопасности и управления сетью	843
Разработка мер обеспечения безопасности в сети	843
Идентификация сетевого оборудования и анализ рисков	844
Анализ требований безопасности и возможных компромиссных решений	844
Разработка плана действий по обеспечению безопасности	845
Разработка политики безопасности	846
Компоненты политики безопасности	846
Разработка процедур обеспечения безопасности	847
Механизмы обеспечения безопасности	847
Аутентификация	847
Авторизация	848
Учет и аудит	848
Шифрование данных	849
Фильтры пакетов	851
Брандмауэры	852
Обнаружение вторжений в сеть	853
Физическая безопасность	853
Выбор средств для решения проблем безопасности	854
Обеспечение безопасности Internet-соединений	854
Защита службы системы доменных имен	855
Логическое проектирование сети и Internet-соединения	855
Протокол IP Security	856
Обеспечение безопасности соединений удаленного доступа	857
Обеспечение безопасности сетевых служб	858
Обеспечение безопасности служб пользователя	859
Резюме	860
Глоссарий	860

Глава 23. Виртуальные частные сети	865
Функционирование виртуальных частных сетей	865
Преимущества использования частных виртуальных сетей	865
Типы виртуальных частных сетей	866
Соглашения об уровне обслуживания	867
Пример виртуальной частной сети	868
Виртуальная частная сеть, состоящая из узлов сети А	868
Реализация виртуальных частных сетей	869
Аудит безопасности	869
Сфера действия сети и требования приложений	870
Документация	870
Политика безопасности	870
Проектирование VPN-сетей с использованием аппаратного и программного обеспечения Cisco	871
Обзор технологии создания туннелей	871
Службы виртуального удаленного доступа Cisco	873
Реализация Cisco протокола L2TP	873
Процесс виртуального удаленного доступа на всем протяжении маршрута следования данных	875
Особые свойства службы виртуального удаленного доступа	876
Аутентификация и безопасность сети	876
Авторизация	877
Выделение адресов	878
Учет	878
Резюме	878
Глоссарий	879
Часть V. Приложения	883
Приложение А. Глоссарий	885
Приложение Б. Ответы на контрольные вопросы	911
Предметный указатель	929

Студентам

Третье издание этой книги было специально написано для поддержки и дополнения программы онлайн-курса Сетевой академии Cisco. Оно было разработано экспертами корпорации Cisco Systems с целью максимально увеличить время практического освоения программы Сетевой академии. В разделе “Содержание” приведен список всех учебных занятий, проходящих в режиме on-line; иллюстрации в настоящей книге и видеоклипы на диске CD-ROM аналогичны онлайн-материалам и способствуют более глубокому пониманию используемых терминов и концепций.

Это руководство позволяет продолжать занятия даже в том случае когда компьютер по каким-либо причинам недоступен. Специалисты Cisco Systems, разработавшие онлайн-курс, настоятельно рекомендуют использовать данное руководство для максимального использования возможностей обучения.

После прохождения состоящего из четырех семестров курса Сетевой академии Cisco читатель будет готов к сдаче экзамена на сертификат CCNA (Cisco Certified Network Associate). Вопросы экзамена CCNA подготовлены теми же специалистами, которые подготовили материалы этой книги и онлайн-курса. Вследствие этого настоящее руководство является прекрасным помощником при подготовке к экзамену CCNA. Оно также является прекрасным справочным пособием для читателя, начинающего реально работать в сфере сетевых технологий. Книги и материалы, которые использовались в процессе обучения, будут полезны и в дальнейшей работе.

О технических редакторах

Рональд Бодчер (Ronald Bodtcher) связан с компьютерными сетями еще со времен обучения в колледже, где он реализовал простую версию сети SneakerNet, программируя на IBM-360 с помощью перфокарт. После окончания университета BYU и получения степеней бакалавра и магистра в бухгалтерской сфере Рон фактически стал компьютерным специалистом и работал в качестве менеджера и компьютерного специалиста в налоговой сфере компании KPMG Peat Marwick. В настоящее время Рон является консультантом компании CPAide, предоставляющей Web-службы профессиональным бухгалтерам. Рон является сертифицированным бухгалтером и имеет IT-сертификаты A+, Network+ и CCNA. Он также является членом Internet-общества (Internet Society), ассоциации вычислительных устройств (Association for Computing Machinery) и группы IEEE. Окончив программу Сетевой академии Cisco в колледже Canyons города Санта-Кларита, штат Калифорния, Рон имеет первоклассный опыт освоения основ сетевых технологий и блестяще сдал экзамен на сертификат CCNA. Свое свободное время Рон проводит за восстановлением ископаемых останков ледового периода в палеонтологической лаборатории в LaBrea Tar Pits и в прогулках по национальному парку Уотертона (Waterton National Park) со своей женой Сарой и тремя дочерьми: Сарой-младшей, Алисой и Рональей.

К. Р. Киркендаль (K. R. Kirkendall) работает преподавателем в университете города Буаз (Boise), штат Айдахо, имеет степень бакалавра по коммерческому администрированию, полученную в колледже St. Leo College и работает над диссертацией MIS в университете города Буаз. В этом университете Киркендаль читает курсы Cisco,

Microsoft и курс безопасности в сетях. Он имеет несколько промышленных сертификатов, включая сертификаты CCNP, CCNA, CCAI, CCDA, MCP, CNA, A+, Network+, and Server+. Он и его жена Жанин имеют пять прекрасных детей и двух восхитительных внуков, Исайю и Кдрена. В последние пять лет Киркендаль работал в Сетевой академии Cisco в отделе оценки знаний студентов, который разрабатывает вопросы для программы Сетевой академии Cisco и для сертификационных экзаменов Cisco.

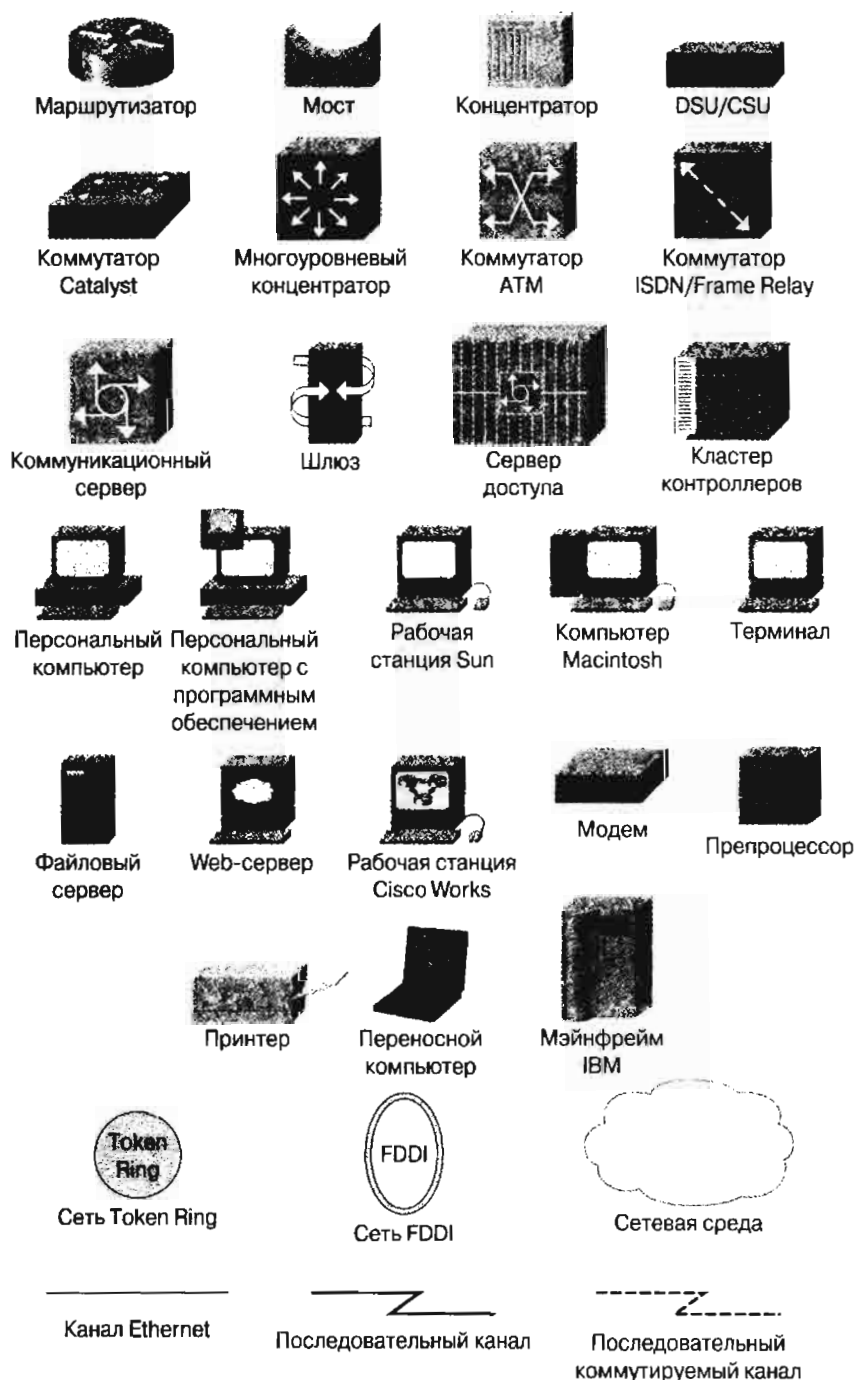
Джим Лоренц (Jim Lorenz) работает над технической документацией и разрабатывает учебный курс для программы Сетевой академии Cisco. Он имеет более чем 20-летний опыт работы с информационными системами и занимал различные должности в сфере использования информационных технологий в компаниях Fortune 500, включая компании Honeywell и Motorola. Джим разрабатывал и преподавал компьютерные и сетевые курсы в государственных и частных учебных заведениях на протяжении более 15 лет. Он также является редактором пособий по лабораторным работам (Lab Companion) для программы Сетевой академии Cisco. Джим имеет сертификаты Novell NetWare Engineer (CNE), Microsoft Certified Trainer (MCT), и Cisco Certified Academy Instructor (CCAI). Он также получил степень бакалавра в сфере компьютерной информации в Prescott-колледже.

Рик МакДональд (Rick McDonald) получил сертификат CCNP в 2002 году и в настоящее время преподает курс CCNP и другие компьютерные курсы в колледже Central Piedmont Community College города Шарлотт штата Северная Каролина. Он получил степень бакалавра по английскому языку и степень магистра в университете Gonzaga города Споукейн, штат Вашингтон.

Рик — заядлый велосипедист, а также любит читать, но его любимое занятие — путешествовать с женой Бекки и сыновьями Греггом, Полем и Сэмом.

Пиктограммы сетевых устройств и соединений, используемые корпорацией Cisco Systems

Корпорация Cisco Systems, Inc. использует стандартизованный набор пиктограмм для представления на иллюстрациях устройств, образующих сетевую топологию. Ниже приводятся наиболее часто используемые пиктограммы, которые можно встретить в настоящей книге.



Обозначения, используемые в командах

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

- Вертикальная черта (|) используется для разделения альтернативных, исключających друг друга элементов;
- Квадратные скобки ([]) указывают на необязательный характер ключевых слов или аргументов.
- Фигурные скобки ({ }) указывают на обязательность выбора какого-либо из приведенных значений.
- Круглые скобки внутри квадратных скобок [()] указывают на обязательность выбора одного из значений внутри необязательного элемента.
- Команды и ключевые слова набраны полужирным шрифтом.
- Названия аргументов, которые должны быть заменены значениями, вводимыми пользователем, выделены *курсивом*.

Предисловие

Во всем мире глобальная сеть Internet принесла огромные новые возможности пользователям и их работодателям. Вкладывая средства в надежные сетевые технологии коммерческие компании и другие организации получают радикальное повышение производительности труда. Некоторые исследования показали значительное повышение производительности в целых отраслях экономики. Надежды на повышение эффективности, доходности и уровня жизни реальны и продолжают расти. Однако такое повышение продуктивности не может быть достигнуто просто закупкой соответствующего сетевого оборудования. Кроме этого необходимы профессионалы, которые могут спланировать, спроектировать, установить, разместить, сконфигурировать, запустить и поддерживать работу сети, а также устранять ошибки и сбои в современных сетях. Сетевые менеджеры должны обеспечить безопасность сети и ее продолжительное эффективное функционирование. Проектирование сети должно обеспечить необходимый данной организации уровень производительности сети. Оно также должно обеспечивать реализацию в сети новых возможностей по мере ее роста и повышения зависимости работы организации от надежной работы сети.

Для удовлетворения образовательных потребностей сетевого сообщества корпорация Cisco Systems разработала программу Сетевой академии Cisco (Cisco Networking Academy). Сетевая академия представляет всеобъемлющую образовательную программу, дающую своим студентам все необходимые знания и навыки для применения сети Internet в глобальной экономике. Программа Сетевой академии объединяет персональное (индивидуализированное) обучение, Web-материалы, онлайн-овую оценку приобретенных знаний и навыков, регистрацию уровня владения материалом, лабораторные работы, обучение и поддержку инструкторов и подготовку к получению сертификатов промышленного стандарта.

Сетевая академия постоянно повышает уровень своих сертифицированных обучающихся и образовательных процессов. Системы оценки знаний и навыков по сети Internet и поддержки инструкторов являются наиболее обширными и проверены временем. К ним, в частности, относится служба пользователя 24/7 для инструкторов Сетевой академии. Осуществляя обратную связь с сетевым сообществом и оценку знаний студентов через Internet, Сетевая академия при необходимости адаптирует учебный курс для повышения качества обучения. Глобальная образовательная сетевая инфраструктура Cisco, предназначенная для Сетевой академии, предоставляет студентам во всем мире глубокий, интерактивный и персонализированный учебный курс. Сеть Internet способна существенно изменить характер работы, обучения, развлечений и образ жизни человека и программа Сетевой академии находится на переднем плане такой трансформации.

Книги по компьютерным сетям издательства Cisco Press представляют собой одну из наиболее популярных серий для программы Сетевой академии Cisco. Созданные авторами издательств Cisco Worldwide Education и Cisco Press, эти книги обеспечивают интегрированную поддержку обучающихся онлайн-овых материалов, которые доступны отделениям Сетевой академии Cisco во всем мире. Эти книги издательства Cisco Press являются единственными авторизованными изданиями Cisco Systems для Сетевой академии и пре-

доставляют печатные материалы и материалы на компакт-дисках (CD-ROM), которые обеспечивают максимальные возможности обучения студентам Сетевой академии.

Надеюсь, что вступив на путь изучения сетевых технологий с Cisco Systems и Internet, вы добьетесь успеха. Надеюсь также, что читатели этой книги продолжат свое обучение после завершения учебного курса Сетевой академии. Кроме книг программы Сетевой академии Cisco издательство Cisco Press публикует также обширный список публикаций по сетевым технологиям и сертификации, которые предоставляют обширные возможности для углубления знаний в сетевой сфере. Корпорация Cisco Systems также создала сеть профессиональных образовательных компаний, которые называются партнерами Cisco в сфере образования и предоставляют обширный диапазон образовательных курсов Cisco. Партнеры Cisco предлагают обучение в различных формах, включая обучение через электронную почту, индивидуальное обучение по удобному для студента графику и курсы, проводимые инструкторами. Эти инструкторы являются сертифицированными специалистами Cisco и их материалы подготовлены специалистами корпорации Cisco Systems. Если читатель готов начать обучение, то ему следует обратиться на Web-сайт Cisco.com корпорации Cisco, где можно более подробно познакомиться с предоставляемыми корпорацией Cisco и ее партнерами возможностями обучения.

Благодарю вас за выбор этой книги и программы Сетевой академии Cisco.

Кевин Уорнер (Kevin Warner)

Генеральный директор департамента всемирного обучения

Корпорация Cisco Systems, Inc

Введение

Третье издание *Программы Сетевой академии Cisco для подготовки к сертификационному экзамену CCNA (части 3 и 4)* дополняет учебные материалы и лабораторные работы программы Сетевой академии Cisco. Этот учебный курс позволяет читателю успешно работать или продолжить обучение и получение практических навыков в сфере компьютерных сетей. Настоящая книга является дополнением онлайн-материалов, уже использованных в данной программе. В ней также затрагиваются темы, относящиеся к экзамену на получение сертификата Cisco Certified Network Associate (CCNA). Изложение материала в книге строго следует стилю и формату учебного курса Cisco. Кроме того, к книге прилагается компакт-диск (CD-ROM), который содержит образовательные видеоклипы, лабораторные работы и фотографии, а также практические вопросы для подготовки к экзамену; все эти материалы представлены в интерактивном мультимедийном формате как справочные образовательные материалы.

Данная книга расширяет знания и практические навыки обучающихся в области проектирования, конфигурирования и поддержки коммутаторов, локальных сетей (local-area network — LAN) и виртуальных локальных сетей (virtual local-area network — VLAN). Изложенные в книге понятия и концепции позволят читателю приобрести практический опыт в конфигурировании сетей локальных сетей LAN, распределенных сетей (wide-area network — WAN), протокола маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP) и расширенного протокола маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol — EIGRP). В дополнение к этому книга позволяет расширить знания и практические навыки в сфере использования распределенных сетей WAN, сети интегрированных служб (Integrated Services Data Network — ISDN), протокола “точка-точка” (Point-to-Point Protocol — PPP), а также проектирования, конфигурирования и поддержки сетей протокола Frame Relay.

Данная книга позволяет читателю подготовиться не только к сертификационному экзамену CCNA, но и к сертификационному экзамену CompTIA Network+.

Цели книги

Целью настоящей книги является обучение читателя поддерживаемым Cisco сетевым технологиям и помощь в понимании того, как проектируются и реализуются сети и как конфигурируются маршрутизаторы Cisco. Книга может быть использована вместе с учебным курсом программы Сетевой академии Cisco или как отдельное справочное пособие.

Для кого предназначена эта книга

В основном книга предназначена для студентов, интересующихся сетевыми технологиями. В частности, книга предназначена для студентов, обучающихся по программе Сетевой академии Cisco. В учебной аудитории книга может служить дополнением к онлайн-учебному курсу. Книга также окажется полезной при обучении сотрудников компаний и для всех пользователей сетей. Дружественный по отношению к пользователю, не отягощенный техническими подробностями подход, надеемся, окажется идеальным для читателя, который не склонен пользоваться учебниками, требующими обширных технических познаний.

Организация материала книги

Настоящая книга организована таким образом, чтобы облегчить читателю понимание компьютерных систем и решение возникающих в них проблем.

- **Цели главы.** Каждая глава начинается с перечисления целей, которые должны быть достигнуты после ее изучения. Эти цели определяют концепции и понятия, освещаемые в главе.
- **Рисунки, примеры и таблицы.** В данной книге содержатся рисунки, примеры конфигураций и таблицы, которые помогают объяснять теоретические положения, концепции и команды и делают более наглядным содержание главы. Кроме того, конкретные примеры представляют реальные практические ситуации, подробно иллюстрирующие проблему и ее решение.
- **Резюме главы.** В конце каждой главы приводится краткий обзор, резюмирующий основные концепции, рассмотренные в главе. Этот обзор представляет собой краткий реферат главы и помогает в изучении материала главы. Рекомендуется использовать это резюме для оценки приобретенных знаний по вопросам, рассмотренным в главе.
- **Глоссарий.** Этот раздел содержит наиболее важные термины, использованные в главе. Эти термины облегчают усвоение материала. Они также углубляют понимание концепций, изложенных в главе. По мере появления таких терминов в материале главы (выделены голубым шрифтом) они определяются в разделе Ключевые термины”.
- **Контрольные вопросы.** Контрольные вопросы, приведенные в заключительной части глав 1-17, позволяют читателю самостоятельно оценить свой уровень усвоения материала глав. Эти вопросы углубляют понимание изложенных в главе понятий и концепций и помогают читателю оценить свой уровень знаний перед изучением новых глав.
- **Лабораторные работы.** На протяжении всей книги приводятся ссылки на рабочие листы и лабораторные работы, содержащиеся в пособии *Cisco Networking Academy Program CCNA 3 and 4 Lab Companion* (3-е издание). Эти лабораторные работы позволяют связать теоретические знания с практическими навыками.

Структура книги

Книга содержит 23 главы и 2 приложения.

Глава 1 представляет собой обзор, главы 2-10 соответствуют электронному курсу CCNA 3, а главы 11-16 — электронному курсу CCNA 4. Главы 17-23 представляют собой дополнительный материал, предназначенный для того, чтобы помочь читателю при подготовке к сертификационным экзаменам, таким как CCNA и CompTIA Network+, а также для знакомства с нарождающимися технологиями.

Ниже приводится краткий обзор отдельных частей книги.

- Глава 1 “Эталонная модель OSI и маршрутизация”. В этой главе приведено описание эталонной модели взаимодействия открытых систем (Open System Interconnection — OSI) и обзор методов планирования и проектирования сетей, относящихся к маршрутизации.

- Глава 2 “Начальные сведения о маршрутизации по адресам без классов”. В этой главе представлены базовые характеристики маски подсети переменной длины (variable length subnet mask — VLSM), а также причины и способы ее использования. В этой главе описано конфигурирование маски VLSM. В ней также приведена история протокола маршрутной информации (Routing Information Protocol — RIP) и базовые компоненты протокола RIPv2. В заключение в главе описано конфигурирование, тестирование и устранение ошибок протокола RIPv2.
- Глава 3 “Протокол OSPF для отдельной зоны”. В этой главе обсуждаются основы протоколов маршрутизации состояния канала, основные концепции протокола OSPF и конфигурирование этого протокола для отдельной зоны.
- Глава 4 “Усовершенствованный протокол маршрутизации внутреннего шлюза”. В этой главе представлены базовые концепции протокола EIGRP и выполнено его сравнение с протоколом IGRP. Также описаны этапы конфигурирования, тестирования и устранения ошибок.
- Глава 5 “Коммутация в локальных сетях и проектирование локальных сетей”. В этой главе описаны проблемы, возникающие в локальных сетях и возможные их решения, которые могут повысить производительность работы LAN-сети. Дополнительно в главе описаны преимущества и недостатки использования мостов, коммутаторов и маршрутизаторов для сегментации LAN-сетей, а также влияние этих устройств на пропускную способность сети. В заключение представлено описание технологий Ethernet, Fast Ethernet и виртуальных локальных сетей VLAN и их достоинства.
- Глава 6 “Коммутаторы”. В данной главе представлены LAN-сети спецификации 802.3, а также преимущества и недостатки сегментации при проектировании таких сетей. Кроме того, в этой главе описаны базовые функции применения мостов и коммутаторов на 2-м уровне.
- Глава 7 “Конфигурирование коммутаторов”. В этой главе описан процесс коммутации в LAN-сетях. В ней представлены этапы конфигурирования коммутатора и тестирования полученной конфигурации, а также восстановление пароля и процедуры модернизации сети.
- Глава 8 “Протокол связующего дерева STP”. В этой главе представлен обзор протокола связующего дерева и топологий с избыточными связями.
- Глава 9 “Виртуальные локальные сети”. В этой главе обсуждаются базовые концепции сетей VLAN и их преимущества. В ней также описано конфигурирование, тестирование, сохранение и удаление сетей VLAN и устранение ошибок в таких сетях.
- Глава 10 “Магистральный протокол VLAN”. В этой главе приведен обзор тем, связанных с использованием магистралей. Кроме того, в ней описаны основные концепции, функционирование и конфигурирование VTP. В заключение описаны основы маршрутизации между сетями VLAN.
- Глава 11 “Масштабирование IP-адресов”. В этой главе описаны принципы масштабирования сетей с помощью трансляции адресов NAT и PAT. В ней также обсуждается протокол DHCP, его функционирование, конфигурирование и устранение ошибок.

- Глава 12 “Технологии распределенных сетей WAN”. В этой главе представлены различные протоколы и технологии, используемые в среде распределенных сетей WAN. В ней описаны основы сетей WAN, включая основные WAN-технологии, типы служб, форматы инкапсулирования и каналные опции. В заключение в этой главе обсуждаются каналы типа “точка-точка”, коммутация каналов, коммутация пакетов, виртуальные каналы, службы удаленного доступа и устройства сетей WAN.
- Глава 13 “Протокол PPP”. В этой главе обсуждаются базовые компоненты, процессы и операции, определяющие характер коммуникации в PPP-сетях. Кроме того, в этой главе описано конфигурирование и тестирование протокола PPP, а также процесс аутентификации в этом протоколе.
- Глава 14 “Технология ISDN и маршрутизация DDR”. В этой главе представлены службы, стандарты, компоненты, функционирование и конфигурирование сетей ISDN.
- Глава 15 “Протокол Frame Relay”. В этой главе обсуждаются службы, стандарты, компоненты и функционирование протокола Frame Relay. Кроме того, в ней описаны задачи конфигурирования службы Frame Relay, а также команды мониторинга и поддержки соединений Frame Relay.
- Глава 16 “Введение в сетевое администрирование”. В этой главе приведен краткий обзор методов, используемых при проектировании распределенных сетей WAN. В ней приведено описание соединений WAN-сетей, а также описаны процесс проектирования таких сетей и задачи, которые при этом ставятся. В ней также описан процесс сбора требований пользователя, которые необходимо учесть при проектировании сети WAN и преимущества использования при проектировании иерархической модели. В этой главе обсуждаются базовые компоненты различных типов рабочих станций, включая системы Microsoft, UNIX и Apple. Дополнительно в главе вводятся в рассмотрение средства управления сетями, модель OSI и модель управления сетью, а также способы сбора информации о работе сети и регистрация возникающих проблем с помощью соответствующего программного обеспечения.
- Глава 17 “Основы оптических сетей”. В этой главе описано как оптические технологии обеспечивают высокоскоростную передачу данных, высокую пропускную способность и масштабируемость сетей. В этой главе также обсуждаются функции оптических сетей, повышенная масштабируемость, которая достигается путем использования мультиплексирования с уплотнением по длине волны (dense wavelength division multiplexing — DWDM), и решения, предоставляемые оптическими сетями.
- Глава 18 “Управление сетями”. В этой главе обсуждаются основы теории управления сетями. В ней описываются сетевая документация, поддержка работы сети, восстановление данных, управление серверами и их поддержка, а также устранение ошибок и сбоев.
- Глава 19 “Обзор тем и программа экзамена Network+”. В этой главе представлен обзор тем, которые необходимо изучить для того, чтобы успешно сдать сертификационный экзамен Network+.

- Глава 20 “Программа экзамена на сертификат CCNA”. В этой главе представлен обзор тем, которые входят в программу сертификационного экзамена CCNA. Этот обзор будет полезен при подготовке к экзамену.
- Глава 21 “Начальные сведения о конвергированных сетях”. В этой главе описана реализация технологии передачи голосовых, видео и обычных цифровых данных по традиционным сетям и рассматриваются различные технологии передачи голосовых данных по обычным сетям. В этой главе также объясняется необходимость в сетях передачи интегрированных данных. Кроме того, в ней дано определение Архитектуры Cisco для передачи голоса, видео и интегрированных данных (Architecture for Voice, Video and Integrated Data — AVVID) и описаны новые приложения для интегрированных сетей.
- Глава 22 “Разработка стратегии обеспечения безопасности и управления сетью”. Материалы этой главы помогут читателю плодотворно работать с пользователем сетевого проекта при разработке эффективной стратегии сетевой безопасности. Они также будут полезны при выборе соответствующих средств и продуктов, необходимых для реализации этой стратегии.
- Глава 23 “Виртуальные частные сети”. В этой главе рассматриваются виртуальные частные сети как средство обеспечения сетевой безопасности. В ней описан базовый механизм использования общедоступных сетей для передачи частной конфиденциальной информации.
- Приложение А “Глоссарий”. Этот глоссарий содержит определения всех ключевых терминов, использованных в книге.
- Приложение Б “Ответы на контрольные вопросы”. В этом приложении приведены ответы на “Контрольные вопросы”, которые находятся в конце каждой главы.

Прилагаемый компакт-диск

К книге прилагается компакт-диск, предназначенный для дальнейшего углубления полученных знаний и приобретения практических навыков работы с сетями. Этот компакт-диск содержит тесты с практическими вопросами экзамена на сертификат CCNA, интерактивные лабораторные работы (e-Lab Activities), фотографии (PhotoZoom) сетевых устройств и другого аппаратного обеспечения, а также обучающие видеоклипы, помогающие усвоению понятий, которые могут представлять трудности для читателя. Эти материалы предназначены для самостоятельного изучения и позволяют читателю приобрести практические навыки работы с сетями в условиях, когда нет возможности непосредственной работы с физической сетью.

Материалы компакт-диска предоставляют:

- Удобный графический интерфейс пользователя;
- Лабораторные работы и материалы по отдельным главам;
- Информацию и лабораторные работы, которые отсутствуют в онлайн-курсе;
- Краткую и точную проверку ответов на практические вопросы сертификационного экзамена;
- Ориентированную на обучающегося практическую подготовку и соответствующие материалы;
- Гибкость для обучающихся всех уровней.

Кроме того, эти средства обучения показывают важность не только усвоения теоретического материала, но и навыков его практического использования.

Этот компакт-диск помогает понять сетевые технологии и связать теоретические знания с практическими навыками.

От издательского дома “Вильямс”

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

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

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

E-mail: info@williamspublishing.com

WWW: <http://www.williamspublishing.com>

Информация для писем из

России: 115419, Москва, а/я 783

Украины: 03150, Киев, а/я 152



В этой главе...

- Описана Эталонная модель OSI, ее общие функции и проблемы, которые она решает
- Описаны функции физического уровня Эталонной модели OSI
- Описаны функции канального уровня Эталонной модели OSI
- Описаны функции сетевого уровня Эталонной модели OSI
- Описаны функции транспортного уровня Эталонной модели OSI
- Рассмотрены функции маршрутизации
- Рассмотрены различные типы протоколов маршрутизации

Эталонная модель OSI и маршрутизация

Компьютерная сеть представляет собой сложную систему, включающую в себя многочисленные среды передачи информации, протоколы передачи и двусторонние связи с сетями, расположенными вне центрального узла связи. Правильно спроектированная и аккуратно установленная сеть позволяет значительно облегчить проблемы, возникающие при дальнейшем ее расширении. Проектирование, установка и обеспечение работы компьютерной **сети** может оказаться непростой задачей. Даже в небольшой сети, содержащей всего 50 машин, могут возникнуть серьезные проблемы, ведущие к непредсказуемым последствиям. Большие сети, состоящие из тысяч узлов, могут создать еще более сложные проблемы. Несмотря на значительный прогресс в увеличении мощности сетевого оборудования и оптимизации процессов обмена данными, проектирование и установка сети по-прежнему остаются достаточно серьезными задачами.

В настоящей главе рассматривается эталонная модель взаимодействия открытых систем OSI (Open System Interconnection, OSI), а также дается общее описание процесса проектирования сети и методов маршрутизации. Использование упомянутой выше модели в качестве общего эталона облегчает решение вопросов, связанных с внесением изменений в сеть, а ее иерархическая структура позволяет подразделить проектирование сети на проектирование отдельных ее уровней. Эталонная модель OSI является основой проектирования и установки сетей, а ее уровни выполняют свои частные задачи при осуществлении обмена данными. Уровни 1–4 являются важнейшими для обеспечения работы сети. Эти четыре уровня выполняют следующие функции:

- определяют тип и скорость используемой передающей среды;
- определяют способ передачи данных;
- определяют используемые схемы адресации;
- обеспечивают надежность передачи данных по сети и определяют способ управления потоком данных;
- задают тип используемого протокола маршрутизации.

Многоуровневая модель сети: эталонная модель OSI

Для упрощения описания сетевых операций модели сетей используют несколько уровней. Разделение операций на различные уровни называется "расслоением" (*layering*). Для того чтобы понять важность такого расслоения, рассмотрим эталонную модель OSI, уровни которой используются для описания обмена данными между компьютерами и которая помогает понять процесс расслоения. Использование уровней упрощает решение задач, возникающих при обмене данными между двумя компьютерами. При этом каждый уровень сосредоточен на выполнении своих специфических функций, что позволяет разработчику сети выбрать для каждого уровня оптимальный тип устройств и выполняемых функций. В эталонной модели OSI имеется семь уровней, имеющих фиксированные номера и выполняющих присущие именно им функции.

Среди причин подразделения различных сетевых функций на уровни отметим следующие.

- Использование уровней позволяет подразделить сетевые операции на блоки, имеющие более простую структуру.
- Использование уровней позволяет использовать стандартный интерфейс для обеспечения совместимости в рамках концепции "plug and play".
- Использование уровней позволяет проектировщику сосредоточить свое внимание на создании отдельных модулей, каждый из которых исполняет некоторый комплекс операций.
- Использование различных уровней позволяет обеспечить структурную симметрию функций, выполняемых отдельными модулями, в результате чего эти модули могут работать совместно.
- Использование уровней позволяет вносить изменения в отдельные модули, не затрагивая при этом другие модули, что ускоряет модернизацию отдельных частей сети.
- Использование уровней позволяет подразделить задачи проектирования сети на отдельные, более простые операции.

Как показано на рис. 1.1, каждый уровень эталонной модели OSI выполняет особые, присущие именно ему функции, которые перечислены ниже.

- *Уровень приложений (7-й уровень)*. Этот уровень используется для обеспечения работы приложений пользователя. Например, для текстового редактора на этом уровне осуществляется передача файлов.
- *Уровень представления данных (6-й уровень)*. Этот уровень обеспечивает представление данных и их форматирование, а также определяет синтаксис передачи данных. В случае, когда этот синтаксис соответствует требованиям сети, данные, используемые приложением могут быть получены из сети и переданы в нее.
- *Сеансовый уровень (5-й уровень)*. Этот уровень обеспечивает сеанс обмена данными между приложениями, а также управляет этим процессом.
- *Транспортный уровень (4-й уровень)*. На этом уровне происходит формирование сегментов данных и преобразование их в поток данных. Этот уровень способен гарантировать установление связи и надежную передачу данных.

- **Сетевой уровень (3-й уровень).** На этом уровне выбирается оптимальный способ передачи данных из одной точки сети в другую. На этом уровне работают маршрутизаторы. При этом используются схемы логической адресации, которыми может управлять сетевой администратор. Этот уровень использует схему адресации протокола IP, а также схемы адресации AppleTalk, DECnet, Vines и IPX.
- **Уровень канала связи или канальный уровень (2-й уровень).** На этом уровне происходит физическая передача данных. При этом посылаются уведомления об ошибках, анализируется топология сети и осуществляется управление потоком данных. На этом уровне используются MAC-адреса, которые также называются адресами управления доступом к среде (Media Access Control) или аппаратными адресами.
- **Физический уровень (1-й уровень).** На этом уровне используются электрические, механические, процедурные и функциональные средства для установки и поддержки физической связи между различными устройствами сети. При этом используются такие физические передающие среды, как витые пары, коаксиальные и оптоволоконные кабели.



Лабораторная работа: эталонная модель OSI и протокол TCP/IP

В этой лабораторной работе требуется описать и сравнить уровни эталонной модели OSI и протокола TCP/IP. Требуется также назвать протоколы стека TCP/IP и утилиты, функционирующие на каждом уровне.



Лабораторная работа: инкапсуляция и устройства эталонной модели OSI и протокола TCP/IP

В этой лабораторной работе требуется описать и дать характеристику уровней эталонной модели OSI

7	Уровень приложений	→	Связь процессов приложений с сетевыми процессами
6	Уровень представления данных	→	Представление данных
5	Сеансовый уровень	→	Связь между узлами
4	Транспортный уровень	→	Сквозные соединения
3	Сетевой уровень	→	Адреса и выбор оптимального пути
2	Канальный уровень	→	Доступ к среде
1	Физический уровень	→	Передача битов

Рис. 1.1. Семь уровней Эталонной модели OSI

Обмен информацией между устройствами одного ранга

Эталонная модель OSI описывает процесс прохождения информации от прикладной программы (такой, например, как электронные таблицы) через передающую среду к другой прикладной программе, работающей на другом компьютере. По мере того как информация проходит через различные уровни сети, ее вид все менее напоминает привычный для пользователя и все более превращается в последовательность нулей и единиц, которая является первичным языком компьютера.

Каждый уровень для осуществления обмена данными с соответствующим уровнем другой системы использует собственный протокол. При этом информация передается в виде *модулей данных протокола* (*protocol data units — PDU*).

На рис. 1.2 приведен пример связи OSI-типа. На узле (host) А находится информация, которую нужно передать на узел В. Приложение на узле А выполняет обмен информацией с уровнем приложения узла В, который, в свою очередь, обменивается информацией с уровнем представления данных того же узла и так далее, вплоть до достижения физического уровня узла А. Этот физический уровень отправляет и получает информацию через физическую передающую среду. После того как данные прошли по физическим устройствам и получены узлом В, они проходят по уровням узла В в обратном порядке (сначала физический уровень, затем уровень канала связи и т.д.), пока, в конечном итоге, не поступят на уровень приложения узла В.



Рис. 1.2. Обмен информацией между уровнями

Хотя каждый уровень узла А обменивается данными с прилегающими уровнями, он также выполняет некоторые первичные, присущие именно ему функции. Они состоят в обмене данными с соответствующим уровнем узла В, т.е. 1-й уровень узла В выполняет обмен данными с 1-м уровнем узла А, 2-й уровень узла В выполняет обмен данными со 2-м уровнем узла А и т.д.

Расслоение в эталонной модели OSI не допускает непосредственной коммуникации между соответствующими уровнями разных узлов. Поэтому для обмена данными с соответствующим уровнем узла В каждый уровень узла А должен пользоваться услугами прилегающих к нему уровней своего узла. Предположим, что 4-й уровень узла А должен осуществить обмен данными с 4-м уровнем узла В. Для этого 4-й уровень узла А должен воспользоваться услугами 3-го уровня своего узла. При таком взаимодействии 4-й уровень называют пользователем службы (*service user*), а 3-й уровень — провайдером этой службы (*service provider*). Службы 3-го уровня предоставляются 4-му уровню в точке доступа к службе (*service access point, SAP*), которая является тем местом, в котором 4-й уровень может запросить службы 3-го уровня. Таким образом, как показано на рис. 1.2, ТСП-сегменты становятся частью *пакетов* (*packet*) сетевого уровня (называемых также *дейтаграммами* (*datagram*)), которыми обмениваются между собой соответствующие уровни сети. В свою очередь IP-пакеты становятся частью фреймов канала связи, которыми обмениваются непосредственно соединенные между собой устройства. В конечном итоге эти фреймы преобразуются в последовательности битов при окончательной передаче данных между устройствами по протоколу физического уровня.

Инкапсуляция данных

Каким образом 4-й уровень узла В узнает о намерениях 4-го уровня узла А? Персональные запросы 4-го уровня хранятся в виде управляющей информации, которая передается между соответствующими уровнями в виде *заголовка (header)*, который присоединяется к передаваемой прикладной информации. Работа каждого уровня эталонной модели OSI зависит от выполнения своих функций нижним по отношению к нему уровнем. Для выполнения этих функций нижний уровень использует инкапсуляцию, при которой PDU верхнего уровня размещается в поле данных, после чего добавляются заголовки и *трейлеры (trailer)*, которые требуются этому уровню для выполнения его функций.

Понятия данных и заголовка являются относительными и зависят от того, на каком уровне происходит анализ блока информации. Например, для 3-го уровня информационный блок состоит из заголовка 3-го уровня и последующих данных. Однако сами данные 3-го уровня могут включать в себя заголовки 4-го, 5-го, 6-го и 7-го уровней. Аналогичным образом заголовок 3-го уровня представляет собой обычные данные для 2-го уровня. Эта структура показана на рис. 1.3. В заключение отметим, что добавление каждым уровнем заголовка не является обязательным. Некоторые уровни просто преобразуют получаемые данные для того, чтобы они стали доступными прилегающим уровням.

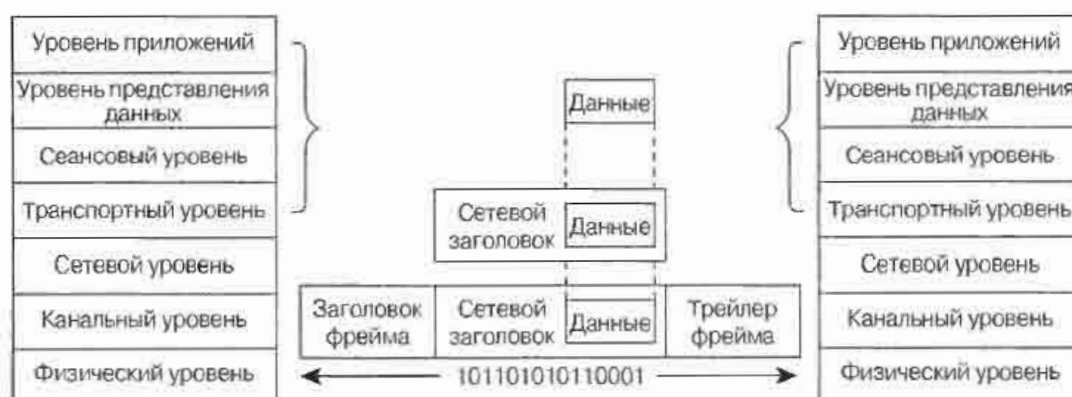


Рис. 1.3. Сетевой уровень

Например, сетевой уровень предоставляет службу транспортному уровню, а транспортный уровень преобразует данные для сетевого уровня, добавляя к ним заголовок. Этот заголовок содержит, необходимую для завершения передачи информацию, такую как логические адреса источника и получателя. Уровень канала связи, в свою очередь, предоставляет службу сетевому уровню, инкапсулируя информацию сетевого уровня во фрейм. Заголовок фрейма содержит информацию, требуемую для выполнения каналом связи своих функций. Например, заголовок фрейма содержит физические адреса. Физический уровень также предоставляет службу уровню канала связи, преобразуя фрейм этого канала в набор нулей и единиц для последующей передачи через физическую среду (обычно по проводу).

Предположим, что узел А желает отправить узлу В по электронной почте следующее сообщение:

The small gray cat ran up the wall to try to catch the red bird
(Серая кошечка подбежала к стене чтобы поймать красную птичку)

В процессе инкапсуляции данных, позволяющей передать это сообщение по электронной почте, выполняются пять этапов преобразования.

- Этап 1.** Когда пользователь посылает электронное сообщение, буквенно-цифровые символы последовательно преобразуются в данные для передачи на 7, 6 и 5-м уровнях и после этого передаются в сеть.
- Этап 2.** Используя сегменты своего формата, транспортный уровень упаковывает данные для транспортировки их по сети и обеспечивает надежную связь между двумя узлами, участвующими в передаче и приеме электронного сообщения.
- Этап 3.** На 3-м уровне данные упаковываются в пакет (дейтаграмму), содержащий сетевой заголовок и логические адреса отправителя и получателя. После этого сетевые устройства пересылают пакеты по сети, используя выбранный маршрутизатором путь.
- Этап 4.** На 2-м уровне каждое сетевое устройство должно вставить пакет во фрейм. Фрейм позволяет осуществить соединение со следующим сетевым устройством. Каждое устройство на выбранном сетевом пути требует создания фрейма для соединения со следующим устройством.
- Этап 5.** На 1-м уровне фрейм должен быть преобразован в последовательность нулей и единиц для прохождения по передающей среде (обычно по проводу). Механизм синхронизации позволяет различать между собой эти биты по мере того как они проходят через передающую среду. На различных участках сетевого пути тип передающей среды может меняться. Например, электронное сообщение может начать свое движение в локальной сети, пересечь магистраль, выйти в распределенную сеть и достичь пункта назначения в другой удаленной локальной сети.

Физический уровень

В настоящее время в сети Ethernet и сети стандарта IEEE 802.3 может использоваться любой протокол локальной сети (Local Access Network — LAN). При этом термин Ethernet часто используется для обозначения любых локальных сетей использующих множественный доступ с контролем несущей и обнаружением коллизий (carrier sense multiple access collision detect — CSMA/CD), которые в целом удовлетворяют спецификациям Ethernet, включая стандарт IEEE 802.3.

При разработке Ethernet ставилась задача заполнения среднего диапазона между низкоскоростными сетями большого размера и специализированными, обычно работающими в одном помещении малыми высокоскоростными сетями. Использование Ethernet эффективно в тех случаях, когда по каналу локальной связи необходимо обеспечить высокоскоростную нерегулярную передачу данных, объем которых иногда достигает большой величины.

Термин Ethernet относится к семейству конкретных реализаций локальных сетей, которое включает в себя три основные категории.

- **Сети Ethernet и сети стандарта IEEE 802.3.** LAN-спецификации, работающие со скоростью 10 Мбит/с по коаксиальному кабелю.

- **Сети Ethernet 100 Мбит/с.** Отдельная спецификация локальной сети, также известная как **быстрый Ethernet (Fast Ethernet)**, которая работает на витой паре со скоростью 100 Мбит/с.
- **Сети Ethernet 1000 Мбит/с.** Отдельная LAN-спецификация, также известная как **гигабитовый Ethernet (Gigabit-Ethernet)**, работающая на оптоволоконном кабеле и на витой паре со скоростью 1000 Мбит/с.

Ethernet-технология сохранилась до настоящего времени и занимает важное место среди других благодаря ее огромной гибкости, а также простоте и легкости реализации. Несмотря на то, что в качестве замены предлагались и другие технологии, сетевые менеджеры и ныне часто выбирают Ethernet или его производные в качестве эффективного средства решения проблем, отвечающего современным требованиям. Для преодоления ограничений Ethernet изобретательные пользователи (и организации, участвующие в разработке стандартов) постоянно создают все новые и новые “надстройки” над стандартным Ethernet. Критики, возможно, скажут, что Ethernet — технология, не способная к росту, однако лежащая в ее основе схема продолжает оставаться одним из основных средств передачи информации в современных приложениях.

Физические соединения сетей Ethernet 802.3

Спецификации Ethernet и стандарты на кабели IEEE 802.3 определяют шинную топологию локальных сетей, работающих со скоростями до 10 Мбит/с.

На рис. 1.4 проиллюстрировано применение трех существующих кабельных стандартов.

- **Стандарт 10Base2**, известный как *тонкий (thin) Ethernet*. Этот стандарт позволяет создавать сегменты длиной до 185 метров с передачей по коаксиальному кабелю.
- **Стандарт 10Base5**, известный как *толстый (thick) Ethernet*. Этот стандарт позволяет создавать сегменты длиной до 500 метров с передачей по коаксиальному кабелю.
- **Стандарт 10BaseT**. Используется для передачи Ethernet-фреймов по недорогой витой паре.

Ethernet и стандарты на кабели IEEE 802.3 определяют сеть с шинной топологией и соединительным кабелем между конечными станциями и передающей средой. Для Ethernet этот кабель называется кабелем трансивера (transceiver cable). Он соединяет с трансивером устройство, подключенное к физической передающей среде. В случае конфигурации IEEE 802.3 ситуация примерно такая же, за исключением того, что соединяющий кабель называют *интерфейсом подключаемого модуля (attachment unit interface — AUI)*, а сам трансивер называют *модулем подключения к передающей среде (media attachment unit — MAU)*. В обоих случаях кабель подсоединяется к плате интерфейса (или к цепи интерфейса) внутри конечной рабочей станции.

Станции соединяются с сегментом сети кабелем, проходящим от AUI на рабочей станции к MAU, который непосредственно подсоединен к коаксиальному кабелю Ethernet. Поскольку стандарт 10BaseT предоставляет доступ только к одной станции, станции, подсоединенные к Ethernet посредством 10BaseT, почти всегда подключены к концентратору или коммутатору LAN.

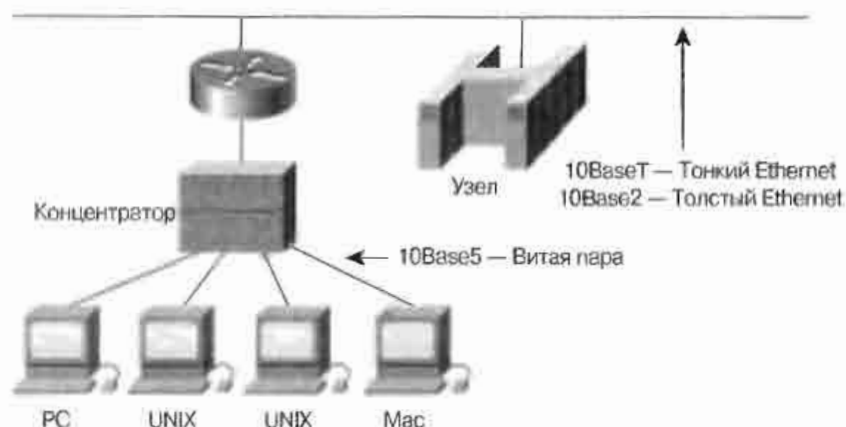


Рис. 1.4. Стандарты 10Base2, 10Base5 и 10BaseT

Канальный уровень

В эталонной модели OSI доступ к передающей среде осуществляется на уровне канала связи. Уровень канала связи или 2-й уровень, где используется MAC-адрес, прилегает к физическому уровню. Никакие два MAC-адреса не могут быть одинаковыми. Таким образом, *сетевой адаптер (network interface card — NIC)* является тем местом, где устройство подсоединяется к физической среде и каждый NIC имеет свой уникальный MAC-адрес.

Перед выпуском с завода каждого NIC производителем ему назначается уникальный номер. Этот адрес запрограммирован в микросхеме, расположенной на NIC. Поскольку MAC-адрес имеется на каждом сетевом адаптере, то при его замене физический адрес этого компьютера (рабочей станции) меняется на MAC-адрес сетевого адаптера.

Для записи MAC-адреса используется шестнадцатеричная система счисления. Существуют два формата MAC-адресов: 0000.0c12.3456 и 00-00-0c-12-34-56.

Поясним это на примере мотеля. Предположим, что в номере 207 установлен замок; назовем его замок А. Ключом А можно открыть дверь номера 207. Аналогично, в номере 410 установлен замок F и его ключом F можно открыть дверь номера 410.

Предположим, что замки А и F меняются местами. После этого ключ А открывает дверь номера 410, а ключ F открывает дверь номера 207.

Если следовать этой аналогии, то сетевые адаптеры являются замками. Если меняются местами сетевые адаптеры, то соответствующие ключи тоже необходимо поменять местами. В этой ситуации ключи являются MAC-адресами.

В случае, если одно устройство сети Ethernet желает переслать данные на другое устройство, то сетевой путь к этому другому устройству может быть проложен с использованием MAC-адреса последнего. Передаваемые по сети данные содержат в себе MAC-адрес адресата. В процессе прохождения их по сети сетевой адаптер каждого устройства проверяет соответствие своего MAC-адреса физическому адресу получателя, который содержится в каждом пакете данных. Если такого соответствия нет, то NIC не реагирует на этот пакет данных и он продолжает двигаться к другой станции.

Однако если эти номера совпадают, то сетевой адаптер делает копию этого пакета данных и направляет ее в компьютер, где она помещается на уровне канала связи. Даже если такая копия была сделана, сам пакет продолжает двигаться по сети, где остальные сетевые адаптеры также могут просмотреть его и проверить наличие описанного выше соответствия.

Интерфейс сети Ethernet/802.3

Ethernet и канал связи 802.3 обеспечивают транспортировку данных по физическому каналу, соединяющему два устройства. Например, как показано на рис. 1.5, в локальной сети Ethernet три устройства могут быть непосредственно подсоединены одно к другому. На компьютере Macintosh слева и на компьютере Intel в середине рисунка указаны MAC-адреса, используемые канальным уровнем. Маршрутизатор, расположенный справа, также использует MAC-адреса для каждого своего LAN-интерфейса.

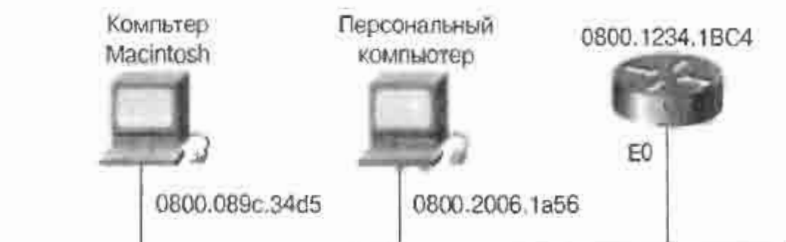


Рис. 1.5. Интерфейс Ethernet 802.3

ПРИМЕЧАНИЕ

Интерфейсы Fast Ethernet в модульных маршрутизаторах серии 2600 и др. обозначены как Fa0/0. Аббревиатура Fa означает Fast Ethernet, а обозначение 0/0 соответствует номеру слота 0 и порту интерфейса 0.

Сетевой уровень

На сетевом уровне эталонной модели OSI используются несколько протоколов.

- Протокол IP обеспечивает маршрутизацию дейтаграмм с *негарантированной доставкой (best-effort delivery)* без установки логического соединения (*connectionless*). Этот протокол не интересуется содержанием дейтаграмм; он лишь ищет наилучший способ направить дейтаграмму к месту ее назначения.
- Протокол управляющих сообщений в сети Internet (*Internet Control Message Protocol — ICMP*) обеспечивает возможность управления и отправки сообщений.
- Протокол преобразования адресов (*Address Resolution Protocol — ARP*) определяет адрес уровня канала связи по известному IP-адресу.
- Обратный ARP (*reverse ARP — RARP*) определяет сетевой адрес устройства в ситуациях, когда известен адрес канального уровня.

IP-адресация и подсети

В среде TCP/IP конечные станции имеют возможность осуществлять связь с серверами, узлами или другими конечными станциями. Это происходит потому, что каждый узел, использующий протокол TCP/IP, имеет уникальный 32-битовый логический адрес, который часто называют *IP-адресом (IP address)*. Кроме того, в среде TCP/IP каждая сеть имеет отдельный уникальный адрес. Перед получением доступа к какому-либо узлу этой сети необходимо выйти на этот адрес. Таким образом, каждая сеть имеет адрес и адреса узлов, входящих в эту сеть, включают в себя этот адрес сети, однако при этом каждый узел имеет также и свой индивидуальный адрес (рис. 1.6).

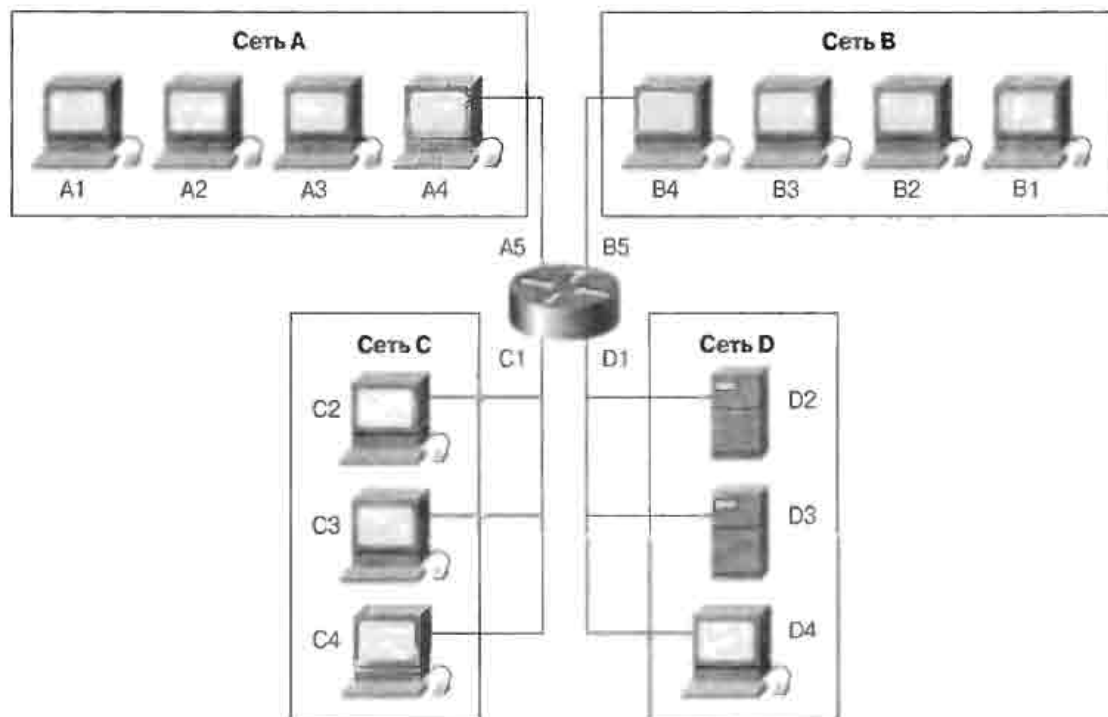


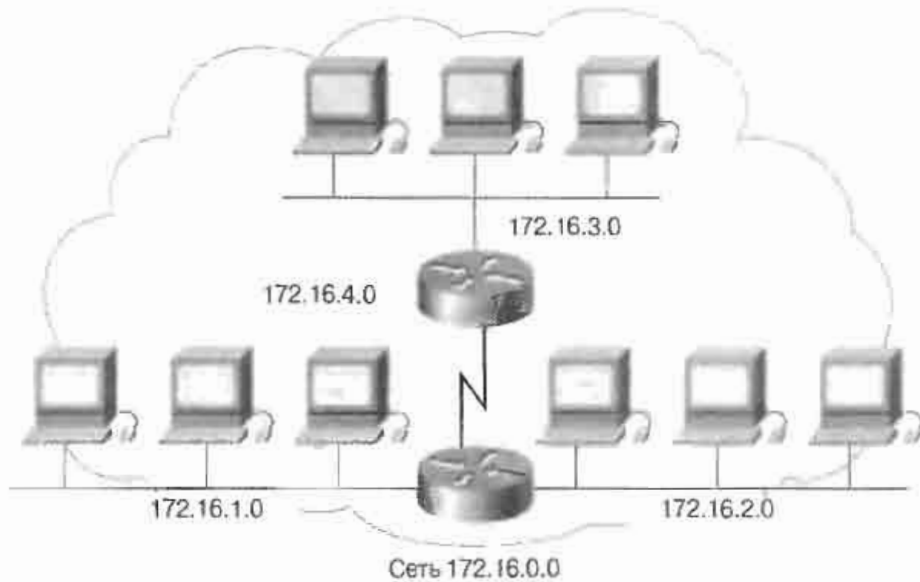
Рис. 1.6. Разделение сети на подсети

Сети могут быть разделены на сегменты — сети меньшего размера, которые называют *подсетями* (*subnetwork*). Таким образом, IP-адрес состоит из трех частей: адрес сети, адрес подсети и адрес узла. Подсети используют уникальные адреса, состоящие из битов поля узла. Адреса устройств какой-либо подсети видны всем другим устройствам этой же сети, но не видны внешним сетям. Это достигается путем использования *маски подсети* (*subnet mask*).

При создании подсетей использование сетевых адресов становится более эффективным. Для мира, внешнего по отношению к данной сети, изменений не происходит, однако сеть приобретает дополнительную структуру. На рис. 1.7, сеть 172.16.0.0 подразделена на четыре подсети: 172.16.1.0, 172.16.2.0, 172.16.3.0 и 172.16.4.0.

Определение пути

Определение пути (*path determination*) представляет собой процесс, в котором определяется оптимальное направление, которое поток данных должен избрать в сетевой среде. Как показано на рис. 1.8, этот наилучший путь выбирают маршрутизаторы. Определение пути происходит на 3-м (сетевом) уровне. При оценке качества путей по сети службы маршрутизации используют сетевую топологическую информацию. Эта информация может быть задана сетевым администратором или получена путем изучения динамических процессов, происходящих в сети.

*Рис. 1.7. Разделение сети на подсети*

Сетевой уровень обеспечивает подключение к сети и предоставляет службу негарантированной доставки пакета из одного конца в другой, т.е. до своего пользователя, транспортного уровня. Сетевой уровень При пересылке пакета от сети-источника к сети-получателю маршрутизатор использует данные, содержащиеся в таблице маршрутизации. После того как маршрутизатор выбрал путь, он направляет пакет, полученный на одном интерфейсе, на другой интерфейс в соответствии с выбранным оптимальным путем.

*Рис. 1.8. Определение маршрута*

Обмен информацией о путях

Для того, чтобы найденный путь действительно оказался самым эффективным, в сети должна постоянно присутствовать информация о доступных путях между маршрутизаторами. Как показано на рис. 1.9, каждая линия между маршрутизаторами имеет свой номер, который маршрутизаторы могут использовать в качестве сетевого адреса. Этот адрес должен содержать информацию, которую можно было бы использовать в процессе маршрутизации.

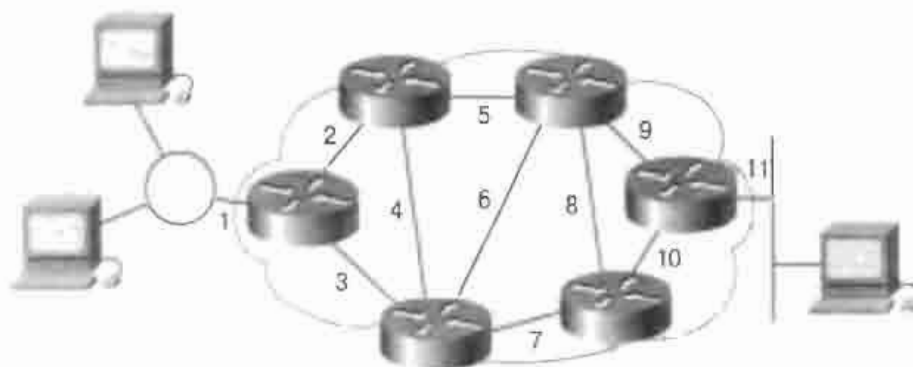


Рис. 1.9. Маршруты передачи данных

Сетевой адрес устройства содержит две части: информацию о пути и информацию об узле. Относящаяся к пути информация описывает путь, избранный маршрутизатором в сетевой среде: часть, относящаяся к узлу, указывает на конкретный порт или устройство в сети. Маршрутизатор использует сетевой адрес для определения номера сети отправителя или получателя. На рис. 1.10 показаны три сети, исходящих из маршрутизатора и три узла, имеющих общий адрес сети, равный 1. В некоторых протоколах сетевого уровня эта связь устанавливается сетевым администратором согласно заранее составленному плану сетевой адресации. В других протоколах такого типа назначение адресов является частично или полностью динамическим.

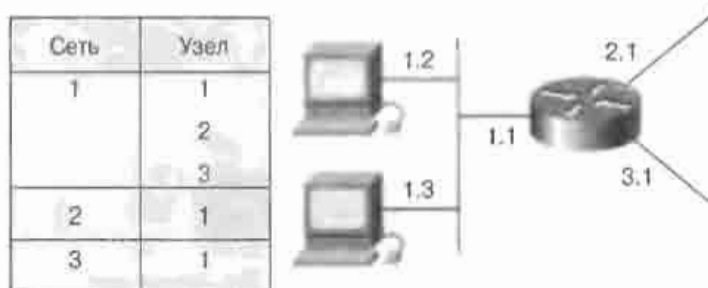


Рис. 1.10. Схемы адресации

Согласованность адресов 3-го уровня в пределах всей сети увеличивает эффективность использования полосы пропускания, предотвращая ненужные широковещательные сообщения. Широковещание вызывает значительное увеличение потока и потерю производительности всеми устройствами, которым не требуется получать такие сообщения. Использование согласованной адресации “из конца в конец” для представления пути между точками среды позволяет сетевому уровню найти путь к месту назначения без непроизводительного использования устройств и связей сети.

Протокол ICMP

ICMP-сообщения передаются в IP-дейтаграммах и используются для передачи управляющих сообщений и сообщений об ошибках. ICMP использует следующие стандартные сообщения (приведена лишь часть таких сообщений):

- destination unreachable (пункт назначения недостижим);
- time exceeded (превышено время ожидания);

- parameter problem (проблема с параметром);
- source quench (подавление источника);
- redirect (перенаправить);
- echo (эхо-запрос);
- echo reply (эхо-ответ);
- timestamp (запрос времени);
- timestamp reply (ответ на запрос о времени);
- information request (информационный запрос);
- information reply (ответ на информационный запрос);
- address request (запрос об адресе);
- address reply (ответ на запрос об адресе).

Например, на рис. 1.11 изображен маршрутизатор, получивший пакет, который он не может доставить до пункта назначения. В таком случае маршрутизатор посылает отправителю сообщение ICMP “Host unreachable”. Невозможность доставить сообщение может объясняться тем, что маршрут до пункта назначения неизвестен. На рис. 1.12 изображена иная ситуация, когда получен положительный эхо-ответ на команду ping.

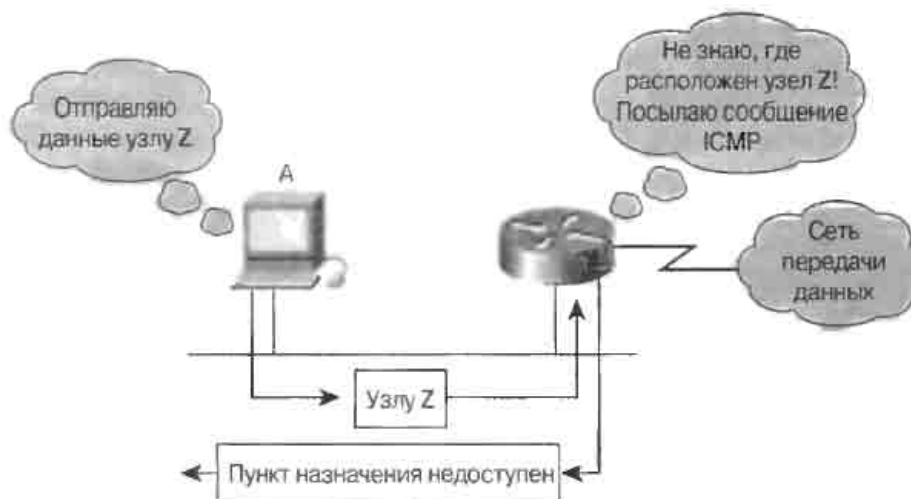


Рис. 1.11. Ситуация, когда доставка пакета невозможна

Протокол ARP

Для осуществления коммуникации в сети Ethernet станция-источник должна знать IP- и MAC-адреса станции-получателя. После того как станция-отправитель определила IP-адрес станции-получателя, Internet-протокол источника использует таблицу ARP для нахождения соответствующего MAC-адреса получателя. Если Internet-протокол находит в своей таблице IP-адрес получателя, соответствующий его MAC-адресу, то он связывает их и использует для инкапсуляции данных, после чего пакет пересылается через сетевую среду и получается станцией-адресатом.

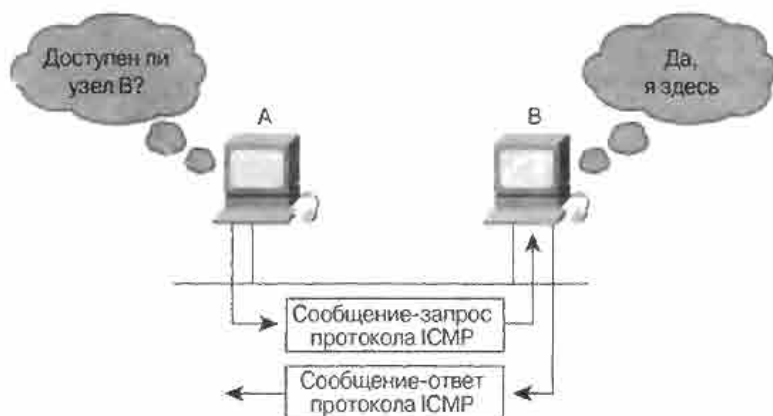


Рис. 1.12. Результат выполнения команды ping

Если MAC-адрес неизвестен, то станция-отправитель должна отправить ARP-запрос. Для того, чтобы определить адрес пункта назначения дейтаграммы, анализируется ARP-таблица маршрутизатора. Если адрес в таблице отсутствует, то посылается широковещательный запрос о поиске станции назначения, который получает каждая станция в сети.

Термин *локальный ARP (local ARP)* используется в том случае, когда узел запроса и узел пункта назначения находятся в одной и той же подсети или подсоединены к общей передающей среде. В примере на рис. 1.13 перед отправкой сообщения протокола ARP запрашивается маска подсети. Анализ маски показывает, что узлы находятся в одной и той же подсети.

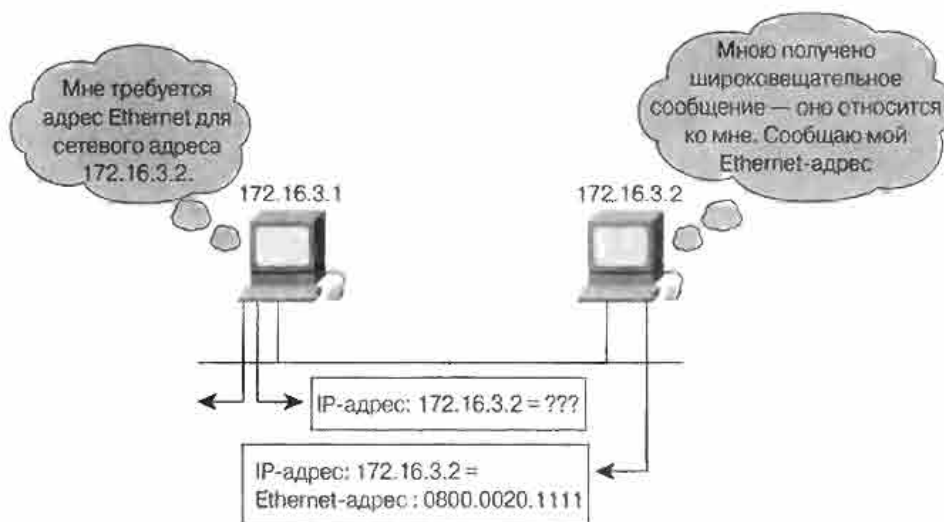


Рис. 1.13. Локальный протокол ARP

Маршрутизация

Сетевой уровень должен вступать во взаимные отношения с различными нижними уровнями. Маршрутизатор должен уметь обрабатывать пакеты, инкапсулированные во фреймы нижних уровней, не меняя адресации третьего уровня для данного пакета. На рис. 1.14 изображен пример такой маршрутизации от одной LAN к другой. В данном случае потоку данных от узла 4 Ethernet-сети 1 требуется найти путь к узлу 5 сети 2.

Анализируя свои таблицы маршрутизации, маршрутизатор обнаруживает, что наилучшим путем к сети 2 является выходной порт To0, который является интерфейсом локальной сети Token Ring. Хотя при переключении маршрутизатором потока с Ethernet-протокола в сети 1 на Token Ring в сети 2 организация фреймов нижних уровней меняется, адресация 3-го уровня для отправителя и получателя остается неизменной. На рис. 1.14 адресом получателя остается сеть 2, несмотря на изменение инкапсуляции нижних уровней.

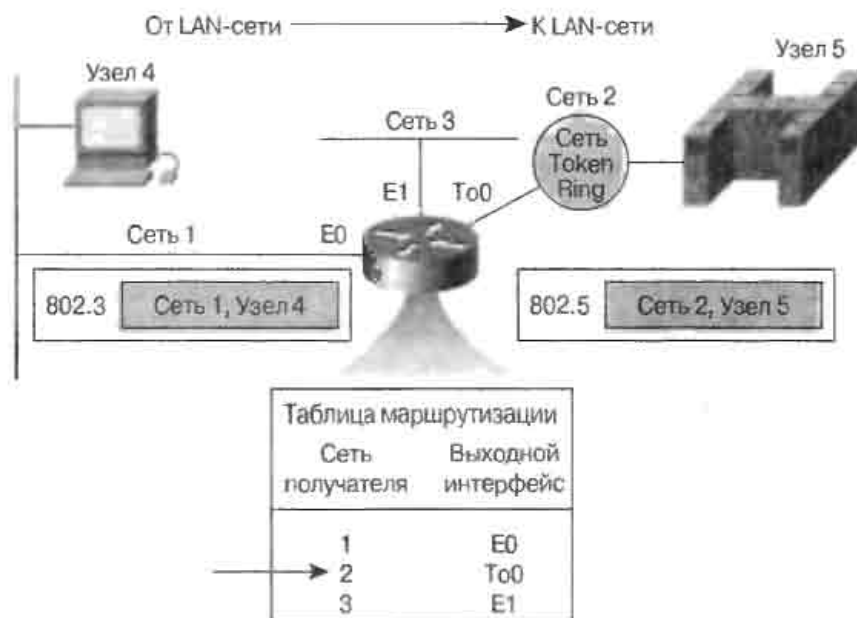


Рис. 1.14. Маршрутизация

Операции маршрутизатора

Маршрутизатор обычно передает пакет от одного канала связи к другому. При такой передаче перед маршрутизатором стоят две задачи: определение пути и коммутация. На рис. 1.15 показано, как маршрутизатор использует адресацию для выполнения функций определения пути и коммутации.

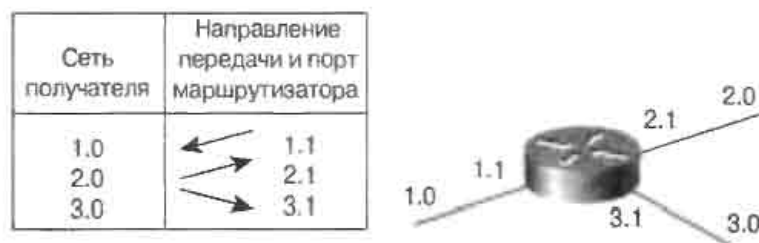


Рис. 1.15. Операции, выполняемые маршрутизатором

Выполняя функцию коммутации маршрутизатор принимает пакет на одном интерфейсе и направляет его на другой. При определении наилучшего пути маршрутизатор выбирает наиболее подходящий интерфейс для отправки пакета. Узловая часть адреса относится к конкретному порту на маршрутизаторе, который ведет к следующему в данном направлении маршрутизатору.

Когда приложению некоторого узла требуется послать пакет в пункт назначения в другой сети, фрейм канального уровня принимается на одном из интерфейсов маршрутизатора. На сетевом уровне исследуется заголовок фрейма для определения сети пункта назначения, а затем маршрутизатор обращается к таблице маршрутизации, которая связывает сети с выходными интерфейсами. После чтения адреса заголовка и трейлера пакета отбрасываются, а сам пакет снова инкапсулируется в канальный фрейм для выбранного интерфейса и ставится в очередь (*queue*) для доставки к следующему переходу (*hop*).

Этот процесс повторяется при каждой коммутации с одного маршрутизатора на другой. На маршрутизаторе подсоединенном к сети, в которой находится узел назначения, пакет инкапсулируется в канальный фрейм типа LAN-получателя и передается на узел пункта назначения.

Сравнение динамической и статической маршрутизации

Статическая маршрутизация (static routing) выполняется вручную. Ее осуществляет сетевой администратор, внося изменения в конфигурацию маршрутизатора. Администратор должен изменять эту информацию о маршрутах каждый раз, когда изменяется сетевая топология. Статическая маршрутизация уменьшает количество передаваемой служебной информации, поскольку в этом случае не посылается информация об изменениях в маршрутном расписании (в случае использования протокола RIP это требуется делать каждые 30 секунд).

Динамическая маршрутизация (dynamic routing) выполняется по-другому. После того, как сетевой администратор введет конфигурационные команды для начала динамической маршрутизации, маршрутная обстановка изменяется автоматически при каждом получении из сети информации об изменениях в ее топологии. При этом обмен информацией между маршрутизаторами об изменениях в топологии сети является частью процессов изменения сети.

Статическая маршрутизация имеет несколько преимуществ. Она позволяет сетевому администратору указать, какая служебная информация будет передаваться по сети. По соображениям безопасности администратор может спрятать некоторые части сети. Динамическая маршрутизация имеет тенденцию к полной открытости всей информации о сети.

Кроме того, в случаях, когда к сети ведет только один путь, статический маршрут может оказаться вполне достаточным. Такой тип сети называется *тупиковой сетью (stub network)*. Задание статической маршрутизации в тупиковой сети позволяет исключить пересылку служебной информации, которая производится при динамической маршрутизации.

Пример стандартного маршрута по умолчанию

На рис. 1.16 показан пример *стандартного маршрута по умолчанию (default route)*, т.е. маршрута, который используется для того, чтобы направить дальше фреймы, для которых в маршрутной таблице нет явного адреса следующего перехода. В этом примере маршрутизаторы компании X знают топологию сети своей компании, но не имеют таких знаний о других сетях. Поддержка информации обо всех сетях, доступных с помощью Internet-среды не нужно и неразумно, а чаще всего и просто невозможно.

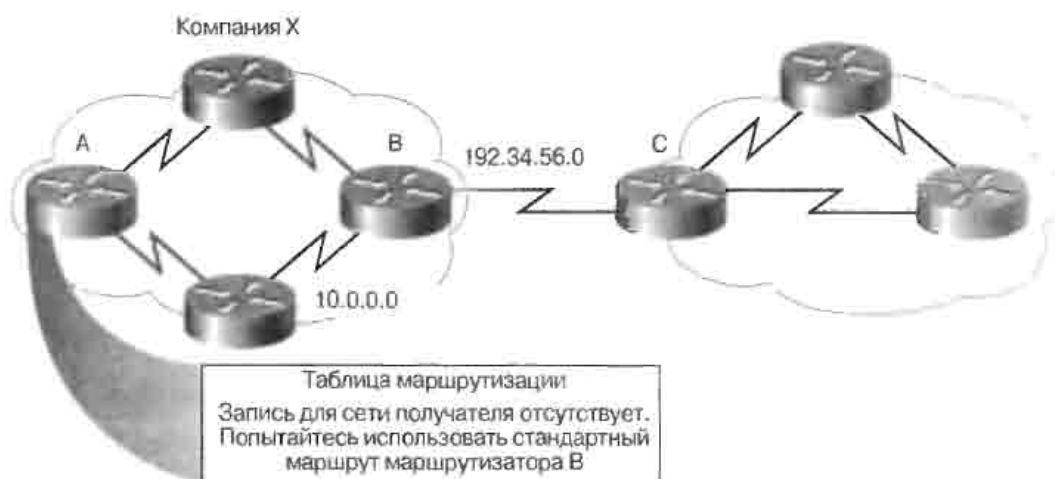


Рис. 1.16. Стандартный маршрут

Маршрутизируемые протоколы и протоколы маршрутизации

Часто смешиваются понятия *маршрутизируемого (routed protocol) протокола* и *протокола маршрутизации (routing protocol)*.

- **Маршрутизируемый протокол** — это любой сетевой протокол, который в своем адресе сетевого уровня содержит достаточно информации для того, чтобы направить пакет от узла к узлу, опираясь на схему адресации. Маршрутизируемый протокол определяет формат и характер использования полей внутри пакета. При этом пакет обычно направляется от одной конечной системы к другой. Примером маршрутного протокола является IP.
- **Протокол маршрутизации** — это протокол, который поддерживает маршрутизируемый протокол, предоставляя ему механизмы совместного использования информации по маршрутизации. Сообщения маршрутизирующих протоколов перемещаются между маршрутизаторами. Маршрутизирующий протокол позволяет маршрутизаторам обмениваться информацией друг с другом с целью поддержки таблиц маршрутизации и внесения в них изменений. Примерами протоколов маршрутизации типа TCP/IP являются протоколы: *Routing Information Protocol (RIP)*, *Interior Gateway Protocol (IGRP)*, *Enhanced Interior Gateway Routing Protocol (Enhanced IGRP)* и *Open Shortest Path First (OSPF)*.

Протоколы маршрутизации

Эффективность динамической маршрутизации зависит от выполнения маршрутизатором двух своих основных функций.

- Поддержка таблицы маршрутизации.
- Своевременное распределение информации о состоянии (топологии) сети между другими пользователями в форме сообщений об изменении маршрутизации.

В процессе обмена информацией о топологии сети динамическая маршрутизация опирается на протокол маршрутизации, который, представляет собой набор правил, используемых маршрутизатором при обмене информацией с соседними маршрутизаторами. Например, протокол маршрутизации описывает:

- как рассылаются сообщения об изменениях в сети;
- какая информация о топологии сети содержится в этих изменениях;
- как часто рассыляется информация о состоянии сети;
- как определить месторасположение получателей сообщений об изменениях в сети.

Внешние протоколы маршрутизации используются для обмена информацией между автономными системами. Внутренние протоколы маршрутизации используются внутри отдельных автономных систем.

IP-протоколы маршрутизации

На сетевом уровне (3-й уровень) эталонной модели OSI маршрутизатор может использовать протоколы маршрутизации для выполнения маршрутизации с использованием специального маршрутизирующего протокола. В качестве примеров IP-протоколов маршрутизации можно привести:

- **RIP** — дистанционно-векторный протокол маршрутизации;
- **IGRP** — дистанционно-векторный протокол маршрутизации, разработанный корпорацией Cisco;
- **OSPF** — протокол маршрутизации состояния канала;
- **EIGRP** — сбалансированный гибридный протокол маршрутизации.

Типы протоколов маршрутизации

Большинство протоколов маршрутизации могут быть отнесены к одному из двух основных типов: дистанционно-векторные или протоколы канала связи. *Дистанционно-векторный протокол маршрутизации (distance-vector routing protocol)* определяет направление (вектор) и расстояние для всех связей в сети. Второй подход, связанный с использованием *протокола маршрутизации канала связи (link-state routing protocol)*, также называемого протоколом поиска *первого кратчайшего пути (the shortest path first — SPF)*, каждый раз воссоздает точную топологию всей сети (или, по крайней мере, того сегмента, в котором расположен маршрутизатор). Третий тип протокола — *сбалансированный гибридный (balanced-hybrid protocol)*, соединяет в себе различные аспекты протокола состояния связи и дистанционно-векторного.

Конвергенция

При динамической маршрутизации выбор протокола, используемого при определении наилучшего пути для потока данных от конкретного источника к конкретному получателю, имеет принципиальное значение. Каждое изменение топологии сети, связанное с ее ростом, изменением конфигурации или сбоем, должно быть отражено в соответствующих таблицах маршрутизации.

В каждый момент времени имеющаяся в таблицах маршрутизации информация должна точно и последовательно отражать новую топологию сети. Такое точное и последовательное соответствие называется *конвергенцией (convergence)*.

В случае, когда все маршрутизаторы сети работают с одной и той же информацией о топологии сети, говорят, что сети конвергированы. Быстрая конвергенция является весьма желательной, потому что она уменьшает период времени, за который информация о состоянии сети могла бы устареть и стать причиной неправильных или неэффективных решений.

Дистанционно-векторная маршрутизация

Дистанционно-векторные протоколы периодически рассылают копии таблицы маршрутизации от одного маршрутизатора к другому. Каждый маршрутизатор получает таблицу маршрутизации от своего непосредственного соседа (рис. 1.17). Например, маршрутизатор В получает информацию от маршрутизатора А. Маршрутизатор В добавляет дистанционно-векторный номер (например, число переходов), увеличивает дистанционный вектор и передает таблицу маршрутизации другому своему соседу, маршрутизатору С. Такой же пошаговый процесс происходит во всех направлениях между маршрутизаторами-соседями.

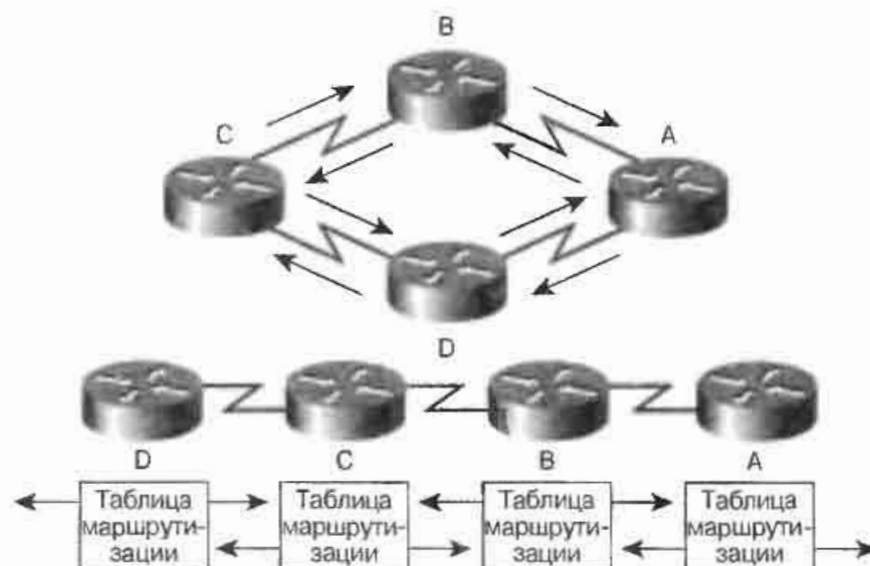


Рис. 1.17. Дистанционно-векторная маршрутизация

В результате этого процесса протокол накапливает данные о расстояниях в сети, что позволяет ему поддерживать базу данных описывающих текущую топологию сети. Однако дистанционно-векторные протоколы не позволяют маршрутизатору знать точную топологию сети.

Маршрутизация состояния канала связи

Вторым основным типом протоколов, используемых для маршрутизации, является протокол состояния канала связи. Протоколы состояния канала связи поддерживают комплексную базу данных, в которой содержится информация о топологии сети. В то время как дистанционно-векторный протокол не содержит конкретной информации об удаленных сетях и об удаленных маршрутизаторах, протокол состояния канала связи поддерживает полную информационную картину топологии сети, включая информацию об удаленных маршрутизаторах и их взаимосвязях.

Маршрутизация состояния канала связи использует *объявления состояния канала связи (link-state advertisement — LSA)*, топологические базы данных, SPF-протокол, результирующее SPF-дерево, а также таблицу маршрутизации портов для каждой сети. На основе концепции состояния канала связи разработчиками была создана OSPF-маршрутизация.

Сравнение дистанционно-векторной маршрутизации и маршрутизации состояния канала связи

Дистанционно-векторную маршрутизацию и маршрутизацию состояния канала связи можно сравнить в нескольких ключевых аспектах.

- Дистанционно-векторная маршрутизация получает все топологические данные из таблиц маршрутизации своих соседей. Маршрутизация состояния канала связи получает информацию о топологии всей сети путем накопления всех необходимых LSA.
- При дистанционно-векторной маршрутизации наилучший путь определяется путем увеличения некоторого числового значения по мере перемещения таблиц от одного маршрутизатора к другому. При маршрутизации состояния канала связи каждый маршрутизатор сам отдельно рассчитывает кратчайший путь к месту назначения.
- В большинстве протоколов дистанционно-векторной маршрутизации отображение изменений топологии происходит периодически по мере поступления таблиц изменений. Эти таблицы перемещаются от одного маршрутизатора к другому, что часто приводит к медленной конвергенции. В протоколах маршрутизации состояния канала связи внесение изменений вызывается изменениями в топологии. Относительно небольшие LSA, передаваемые всем остальным маршрутизаторам, обычно приводят к уменьшению времени конвергенции.

Конфигурирование IP-маршрутизации

Выбор IP в качестве протокола маршрутизации включает в себя установку глобальных параметров. Эти глобальные параметры включают в себя протокол маршрутизации, например, RIP или IGRP и назначение сетевых IP-номеров без указания значений для подсетей.

Конфигурирование IP-адресов

Для установки логического сетевого адреса интерфейса используется команда `ip address`. Для указания формата масок сети текущего сеанса используется команда `term ip netmask-format`. Формат маски можно задать в виде количества битов, занимаемого префиксом подсети, в виде точечной десятичной форме записи, либо в виде шестнадцатеричного числа.

Конфигурирование динамической маршрутизации

Динамической называется такой тип маршрутизации, при котором маршрутизаторы периодически посылают друг другу сообщения об изменениях в маршрутизации. При каждом получении такого сообщения, содержащего новую информацию, маршрутизатор заново вычисляет наилучший путь и рассылает эту новую информацию остальным маршрутизаторам. Используя команды маршрутизации маршрутизаторы могут приспособиться к меняющимся условиям в сети.

С перечисленных ниже команд маршрутизатора начинается процесс настройки системы маршрутизации.

Таблица 1.1. Команды `router` и `network`

Команда маршрутизатора	Описание
<code>router protocol</code>	Определяет IP-протокол маршрутизатора (это может быть RIP, IGRP, OSPF или EIGRP)
<code>network</code>	Дополнительная команда <code>network</code> является обязательной при любом типе маршрутизации

Приведенная ниже команда `network` необходима потому, что она позволяет определить какие интерфейсы будут принимать участие в отправке и получении изменений в маршрутизации.

Таблица 1.2. Команды `network`

Команда <code>network</code>	Описание
<code>network номер сети</code>	Указывает непосредственно подсоединенную сеть

Протокол RIP

Основными характеристиками протокола RIP являются следующие.

- RIP является протоколом дистанционно-векторной маршрутизации.
- В качестве величины для выбора пути используется количество переходов.
- Максимально допустимое количество переходов равно 15.
- По умолчанию изменения передаются в широковещательном режиме каждые 30 секунд.

Для выбора RIP в качестве протокола маршрутизации используется команда `router rip`. Команда `network` назначает IP-адрес сети, к которой этот маршрутизатор непосредственно подсоединен. Процесс маршрутизации связывает интерфейс с соответствующим адресом и начинает обработку пакетов указанных сетей (рис. 1.18).

- `router rip` — выбирает RIP в качестве протокола маршрутизации.
- `network 1.0.0.0` — задает непосредственно подсоединенную сеть.
- `network 2.0.0.0` — задает непосредственно подсоединенную сеть.

После выполнения этих команд интерфейсы, подсоединенные к сетям 1.0.0.0 и 2.0.0.0 будут получать и принимать сообщения об изменениях протокола RIP.

Транспортный уровень

При посылке сегментов данных транспортный уровень может обеспечить их целостность. Одним из методов добиться этого является *контроль потока (flow control)*. Контроль потока позволяет избежать ситуации, когда узел на одной из сторон соединения переполняет буферы узла на другой стороне.

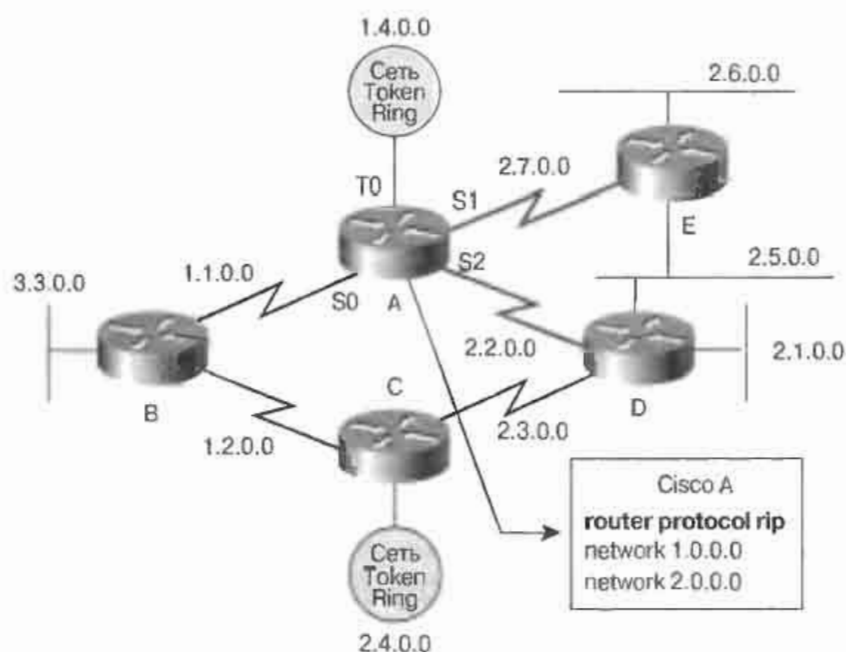


Рис. 1.18. Сообщения об изменениях маршрутизации

Такое переполнение вызывает серьезные проблемы, поскольку оно может привести к потере данных.

Услуги транспортного уровня также позволяют пользователям запросить надежную транспортировку данных между узлом и пунктом назначения. Для обеспечения надежной транспортировки используется ориентированная на соединение связь между системами, которые обмениваются информацией. Применение надежной транспортировки позволяет следующее.

- Выполнить сегментацию приложений верхнего уровня.
- Установить соединение.
- Передать данные.
- Обеспечить надежность транспортировки путем применения окон.
- Использовать механизмы подтверждения.

Сегментирование приложений верхнего уровня

Одной из причин разделения на уровни сетевой модели является возникающая при этом возможность совместно использовать одно и то же транспортное соединение, что выражается в пересылке одного сегмента вслед за другим. Это означает, что различные приложения могут посылать сегменты данных по принципу: "первым пришел — первым обслужили" (first come, first-served). Такие сегменты могут посылаться как в один пункт назначения, так и в несколько.

Установка соединения

Для установки соединения одно устройство делает заказ, который должен быть принят другими. Модули программного обеспечения в двух операционных системах обмениваются информацией между собой, посылая сообщения по сети с целью проверки разрешения передачи и готовности обеих сторон.

После того, как синхронизация будет полностью выполнена, устанавливается соединение и начинается передача данных. В процессе передачи оба устройства продолжают обмен информацией, используя программное обеспечение протокола с целью проверки правильности получения данных.

На рис. 1.19 описано типичное соединение между передающим и принимающим устройством. При первой встрече с человеком мы обычно приветствуем его, пожимая руку. Факт рукопожатия понимается обеими сторонами как признак дружеского расположения. Примерно так же происходит при установке соединения двух систем. Первое рукопожатие или приветствие требует синхронизации. Второе и третье рукопожатия подтверждают запрос первоначальной синхронизации, а также синхронизируют параметры соединения в противоположном направлении. Последним аспектом рукопожатия является подтверждение, используемое для того, чтобы сообщить пункту назначения о том, что обе стороны согласны в том, что связь установлена. После установки связи начинается процесс передачи.



Рис. 1.19. Установка связи между сетями

Передача данных

В процессе передачи данных перегрузка может возникнуть по двум различным причинам. Первая причина: высокоскоростной компьютер может генерировать большее количество данных, чем способна передавать сеть. Вторая причина: если несколько компьютеров одновременно начинают передавать данные в один и тот же пункт назначения. При этом в пункте назначения возникает переполнение, хотя ни один из передающих источников в отдельности вызвать такую перегрузку не в состоянии.

Когда дейтаграммы поступают на обработку на узел или шлюз, они временно хранятся в памяти. Если поток данных продолжается, то память узла или шлюза постепенно переполняется и поступающие дополнительные дейтаграммы приходится отбрасывать. В таких ситуациях, как показано на рис. 1.20, сигнал действует подобно светофору и обращается к отправителю с предложением прекратить отправку данных. Когда получатель вновь сможет принимать дополнительные данные, он посылает транспортный сигнал готовности, который можно интерпретировать как команду: "Посылайте!" После получения такого сигнала отправитель может возобновить передачу сегментов данных.

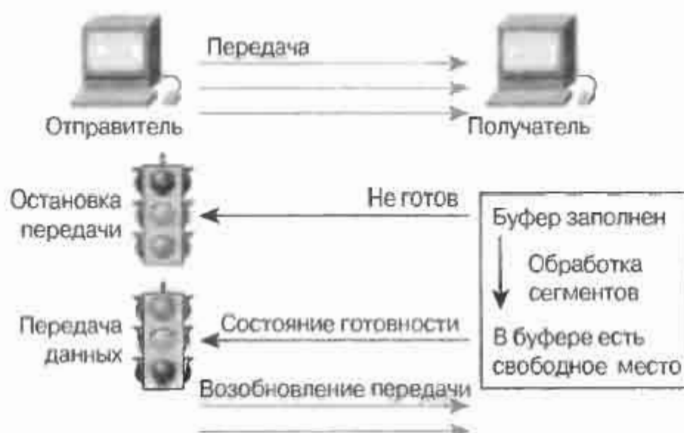


Рис. 1.20. Передача данных

Повышение надежности передачи путем создания окон

В основной своей форме ориентированная на надежность передача требует, чтобы пакеты данных поставлялись принимающей стороне в том же самом порядке, в каком они были переданы. Сбой в работе протокола происходит в тех случаях, когда пакеты данных теряются, повреждаются, дублируются или получаются в измененном порядке. Основным решением в таких ситуациях является организация подтверждения получения каждого сегмента.

Однако если отправителю приходится ожидать подтверждения получения предыдущего сегмента перед отправкой следующего, то пропускная способность оказывается весьма низкой. Поскольку между отправкой сегмента и подтверждением его получения имеется некоторый период времени, его используют для передачи новой порции данных. Количество пакетов, которое отправитель может отправить за этот период называется *окном (window)*.

Механизм создания окон представляет собой способ управлять количеством информации передаваемой от одного узла к другому. Некоторые протоколы измеряют эту информацию в количестве пакетов; протокол TCP/IP измеряет ее в байтах.

Способы подтверждения

Надежная доставка гарантирует, что поток данных, отправленный от одного устройства к другому, проходит по каналу без дублирования или потери данных. Позитивное подтверждение с повторной передачей является одним из методов, гарантирующих надежную доставку данных. Позитивное подтверждение требует обмена информацией между источником и получателем, который заключается в подтверждении адресатом получения данных. Отправитель сохраняет копию каждого отправленного пакета и ожидает подтверждения о его получении перед тем, как отправить следующий. При отправке пакета включается таймер и если по истечении времени таймера подтверждение не поступило, то выполняется повторная передача.

На рис. 1.21 изображен отправитель, посылающий пакеты 1, 2 и 3. Адресат подтверждает получение пакетов, запрашивая пакет 4. После получения подтверждения отправитель посылает пакеты 4, 5 и 6. Если пакет 5 не поступил в пункт назначения, то получатель посылает сообщение с запросом о повторной передаче пакета 5. Отправитель повторно посылает пакет 5 и должен ждать подтверждения его получения перед тем, как отправить пакет 7.



Рис. 1.21. Использование подтверждений

Резюме

- За счет использования уровней Эталонная модель OSI упрощает обмен информацией между двумя компьютерами.
- Соответствующие протоколы каждого уровня обмениваются информацией, которую называют модулями данных протокола (PDU).
- Каждый уровень зависит от сервисных функций лежащего ниже него уровня Эталонной модели OSI. Нижний уровень использует инкапсуляцию для того, чтобы поместить PDU верхнего уровня в свое поле данных; после этого возможно добавление заголовков и трейлеров, которые данный уровень использует для выполнения своих функций.
- Термин *Ethernet* часто используется по отношению ко всем CSMA/CD локальным сетям, которые работают в соответствии со спецификациями Ethernet, включая сеть IEEE 802.3.
- Каналы Ethernet и 802.3 обеспечивают транспортировку данных по физическому каналу, который соединяет какие-либо два устройства.
- Протокол IP обеспечивает негарантированную маршрутизацию дейтаграмм без установления логической связи. Сеть Ethernet не анализирует содержимое дейтаграмм, а лишь ищет способ передать дейтаграмму к ее месту назначения.
- Сообщения ICMP переносятся в IP-дейтаграммах и используются для передачи управляющих сообщений и сообщений об ошибках.
- Протокол ARP используется для преобразования известного IP-адреса в MAC-адрес с целью обеспечения возможности коммуникации в среде множественного доступа, например, такой как Ethernet.
- При осуществлении коммутации маршрутизатор принимает пакет на одном интерфейсе и направляет его на другой.
- Протоколы маршрутизации обеспечивают наличие в адресе сетевого уровня достаточной информации для отправки пакета от одного узла к другому, опираясь на схему адресации.

- Протокол маршрутизации поддерживает маршрутизируемый протокол, создавая при этом механизм совместного использования данных маршрутизации. Сообщения протоколов маршрутизации перемещаются между маршрутизаторами.
- Большинство протоколов маршрутизации относятся к одному из двух типов: дистанционно-векторные или протоколы состояния каналов связи.
- Маршрутизаторы должны быть способны обрабатывать пакеты, инкапсулированные в различные фреймы низкого уровня без изменения адресации 3-го уровня.
- Примерами IP-протоколов маршрутизации могут служить RIP, IGRP, OSPF и EIGRP.
- Службы транспортного уровня дают возможность пользователям запросить надежную транспортировку данных между источником и пунктом назначения.

Основные термины

Cisco IOS (Internetwork Operating System software — Cisco IOS software). Программное обеспечение межсетевой операционной системы корпорации Cisco, которое обеспечивает функциональность, расширяемость и обеспечение безопасности всех программных продуктов архитектуры CiscoFusion. Программное обеспечение операционной системы Cisco предоставляет возможность централизованной, интегрированной и автоматизированной установки и управления сетями, обеспечивая поддержку целого ряда протоколов, передающих сред, служб и платформ.

IP-адрес (IP-address). 32-разрядный адрес, назначаемый узлу в протоколе TCP/IP. IP-адрес принадлежит к одному из пяти классов (A, B, C, D или E) и представляется в десятичном формате в виде четырех октетов, разделенных точками. Каждый адрес состоит из номера сети, необязательного номера подсети и номера компьютера. Номера сети и подсети используются для маршрутизации, а номер компьютера — для адресации уникального узла в сети или подсети. Маска подсети используется для выделения информации о сети и подсети из IP адреса. IP-адрес также называется Internet-адресом (Internet address).

Дейтаграмма (datagram). Блок информации, посланный как пакет сетевого уровня, через передающую среду, без предварительного установления виртуального канала. IP-дейтаграммы — основные информационные блоки в Internet. Термины ячейка, фрейм, сообщение, пакет и сегмент (*cell, frame, message, packet* и *segment*) также используются для описания логически сгруппированных блоков информации на разных уровнях эталонной модели OSI и в различных технологических циклах.

Динамическая маршрутизация (dynamic routing). Маршрутизация, которая автоматически подстраивается под топологию сети или под изменения в потоке данных. Также называется адаптивной маршрутизацией (*adaptive routing*).

Дистанционно-векторный протокол маршрутизации (distance-vector routing protocol). Изучает все переходы в маршруте для построения дерева кратчайшего пути. Протокол заставляет все маршрутизаторы при каждом обновлении рассылать внутренние таблицы только своим соседям. Дистанционно-векторный протокол маршрутизации сводится к циклам маршрутизации, однако в вычислительном отношении он проще, чем протокол состояния канала связи. Также называется алгоритмом маршрутизации Беллмана-Форда (*Bellman-Ford routing algorithm*).

Заголовок (header). Контрольная информация, помещаемая перед данными в процессе их инкапсуляции для передачи по сети.

Интерфейс подключаемых сетевых устройств (attachment unit interface — AUI). В стандарте IEEE802.3 интерфейс (кабель) между MAU и сетевой платой. Термин AUI также обозначает разъем на задней панели, к которому может подсоединяться AUI-кабель. Такие порты можно встретить на плате Cisco LightStream Ethernet. Также называется приемопередающим кабелем (transceiver cable).

Канальный уровень (data link layer). Второй уровень эталонной модели OSI. Обеспечивает точную передачу данных по физическому каналу. Занимается физической адресацией, сетевой топологией, контролем линий связи, сообщениями об ошибках, порядком доставки фреймов и управлением потоками данных. Разделен IEEE на два подуровня: MAC и LLC. Уровень канала связи примерно соответствует уровню управления каналом (data link control layer) в модели SNA.

Конвергенция (convergence). Способность и скорость согласования действий группы взаимодействующих сетевых устройств, использующих специфический маршрутизирующий протокол. Такое согласование необходимо после изменений в топологии сети.

Маршрутизируемый протокол (routed protocol). Протокол, который может управляться маршрутизатором. Маршрутизатор должен осуществлять логическое взаимодействие в сетевом комплексе, как это определено протоколом. Примеры маршрутизируемых протоколов: AppleTalk, DECNet, и IP.

Маска подсети (subnet mask). Маска подсети используется для выделения информации о сети и подсети из IP-адреса.

Модуль данных протокола (protocol data unit — PDU). Термин, обозначающий пакет в эталонной модели OSI.

Негарантированная доставка или “доставка в лучшем случае” (best-effort delivery). Такая доставка осуществляется в том случае, когда сетевая система не использует механизм подтверждения для гарантированной доставки информации.

Окно (window). Число октетов, которое может послать отправитель в ожидании сигнала подтверждения.

Определение пути (path determination). Решение, по какому пути следует направить поток данных. Определение пути происходит на сетевом уровне эталонной модели OSI.

Открытый протокол OSPF (Open Shortest Path First protocol — OSPF). Иерархический маршрутизирующий протокол состояния канала связи, предложенный в качестве замены RIP в среде Internet. Протокол OSPF обеспечивает уменьшение затрат, маршрутизацию с несколькими путями и балансировку нагрузки.

Очередь (queue). 1. Вообще: упорядоченный список элементов, ожидающих обработки. 2. Применительно к маршрутизации: число не переданных пакетов, ожидающих отправки через интерфейс маршрутизатора.

Пакет (packet). Логически сгруппированный блок информации, который включает заголовок, содержащий контрольную информацию, и (обычно) пользовательские данные. Термин “пакет” чаще всего употребляется в контексте блоков данных сетевого уровня. Термины “дейтаграмма”, “фрейм”, “сообщение” и “сегмент” (datagram, frame, message, segment) также используются для описания логически сгруппированных блоков информации на разных уровнях эталонной модели OSI и в различных технологических циклах.

Переход (hop). Переход пакета данных между двумя узлами сети (например, между двумя маршрутизаторами).

Подсеть (subnet). Часть базовой сети передачи данных.

Протокол маршрутизации (routing protocol). Протокол, который осуществляет выбор маршрута путем реализации конкретного протокола. Примерами протоколов маршрутизации могут служить IGRP, OSPF и RIP.

Протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP). Разработан корпорацией Cisco для определения проблем связанных с маршрутизацией, в больших гетерогенных сетях.

Протокол маршрутизации с выбором первого кратчайшего пути (shortest path first protocol — SPF). Обычно используется в протоколах состояния канала связи. Иногда называется алгоритмом Дейкстры (*Dijkstra's algorithm*).

Протокол маршрутной информации (Routing Information Protocol — RIP). Протокол, поставляемый с UNIX BSD. Наиболее часто используемый протокол внутреннего шлюза Internet. В качестве маршрутизирующей метрики (показателя) использует индекс перехода.

Протокол обратного преобразования адресов (Reverse Address Resolution Protocol — RARP). Протокол семейства TCP/IP, представляющий собой метод определения IP-адресов по MAC-адресам.

Протокол преобразования адресов (Address Resolution Protocol — ARP). Internet-протокол семейства TCP/IP, используемый для преобразования IP-адреса в MAC-адрес. Описан в RFC 826.

Протокол маршрутизации по состоянию канала связи (link-state routing protocol). Протокол маршрутизации, в котором каждый маршрутизатор передает широкоэвещательно (всем узлам в сети) или определенной группе адресов (групповая адресация) информацию относительно достижимости каждого из своих соседей. Этот протокол создает согласованное представление о сети и не имеет тенденции к созданию петель, однако это дается ценой больших вычислительных трудностей и большего объема передаваемых данных (по сравнению с дистанционно-векторным протоколом).

Протокол управляющих сообщений Internet (Internet Control Message Protocol — ICMP). Протокол сетевого уровня, который сообщает об ошибках и предоставляет другую информацию относительно обработки IP-пакета. Описан в RFC 792.

Разделение на уровни (layering). Разделение сетевых функций, используемое в эталонной модели OSI. Упрощает разрешение проблем, возникающих при взаимодействии компьютеров в сети.

Расширенный протокол маршрутизации внутреннего шлюза (Enhanced Interior Gateway Routing Protocol — EIGRP). Усовершенствованная версия IGRP, разработанная компанией Cisco. Обеспечивает улучшенные свойства сходимости и производительности и объединяет преимущества дистанционно-векторного протокола и протокола состояния канала связи. Также называется EIGRP.

Сбалансированный гибридный протокол (balanced-hybrid protocol). Сочетает в себе свойства дистанционно-векторного протокола и протокола состояния канала связи.

Сеансовый уровень (session layer). Пятый уровень эталонной модели OSI. Устанавливает, поддерживает и управляет сеансами связи между приложениями.

Сетевая карта (network interface card — NIC). Плата, обеспечивающая коммуникационные возможности компьютерных систем. Называется также сетевым адаптером (*adapter*).

Сетевой уровень (network layer). Третий уровень эталонной модели OSI. Уровень, на котором происходит маршрутизация. Обеспечивает соединение и выбор пути ме-

жду двумя конечными системами. Примерно соответствует уровню контроля пути в модели SNA.

Сеть (network). Группа компьютеров, принтеров, маршрутизаторов, коммутаторов и других устройств, которые обмениваются друг с другом информацией посредством какой-либо передающей среды.

Стандартный маршрут (default route). Запись в таблице маршрутизации, которая используется для отправки фреймов, у которых нет явно указанного адреса следующей точки перехода.

Статическая маршрутизация (static routing). Явно указанные и введенные в таблицу маршруты. Статические маршруты имеют преимущество перед маршрутами, выбранными в соответствии с динамическими протоколами маршрутизации.

Транспортный уровень (transport layer). Четвертый уровень эталонной модели OSI. Сегментирует и преобразует данные в один поток. Транспортный уровень может гарантировать соединение и обеспечивает надежную транспортировку.

Тупиковая сеть (stub network). Сеть, имеющая единственное соединение с маршрутизатором.

Уведомление о состоянии канала связи (link-state advertisement — LSA). Широковещательный пакет, используемый протоколом состояния канала связи. Содержит информацию о соседях и об их достижимости. LSA используется принимающими маршрутизаторами для обновления своих таблиц маршрутизации. Иногда называется пакетом состояния канала связи (*link-state packets*).

Управление доступом к передающей среде (Media Access Control — MAC). Часть канального уровня, включающая 6-байтный (48-битов) адрес источника и пункта назначения, а также метод получения разрешения на передачу.

Управление потоком данных (flow control). Операции, выполняемые для предотвращения переполнения буферов данных в принимающих устройствах. Когда приемный буфер переполнен, посылающему устройству отправляется сообщение о приостановлении передачи до тех пор, пока данные в буфере не будут обработаны. В IBM-сетях эта методика называется определяющей (*pacing*).

Уровень представления данных (presentation layer). Шестой уровень эталонной модели OSI. Обеспечивает представление данных и форматирование кода, а также согласование синтаксиса передачи данных. Этот уровень гарантирует, что данные, которые прибывают из сети, могут быть использованы приложением, а также то, что информация, посланная приложением, может быть передана в сеть.

Уровень приложений (application layer). Седьмой уровень Эталонной модели взаимодействия открытых систем (OSI). Предоставляет сетевые службы для пользовательских приложений. Например, текстовый процессор обслуживается службами передачи файлов этого уровня.

Устройство подсоединения к передающей среде (media attachment unit — MAU). Используется в сетях Ethernet IEEE 802.3. Предоставляет интерфейс между AUI-портом станции и общей передающей средой Ethernet. MAU может быть отдельным или встроенным в станцию устройством и выполняет функции физического уровня, включая преобразование цифровых данных от интерфейса Ethernet, определение конфликтов (коллизий) и направление битов в сеть. Иногда называется устройством доступа к передающей среде (*media access unit*) или приемопередатчиком (*transceiver*).

Физический уровень (*physical layer*). Первый уровень эталонной модели OSI. Этот уровень определяет электрические, механические, процедурные и функциональные спецификации для активизации, поддержания и отключения физического соединения между конечными системами. Соответствует уровню физического управления в модели SNA.

Контрольные вопросы

Для проверки понимания тем и понятий, описанных в настоящей главе, рекомендуется ответить на предлагаемые ниже контрольные вопросы. Ответы на них приведены в приложении А.

1. Какой уровень эталонной модели OSI наилучшим образом описывает стандарты 10BaseT?
 - А. Канальный.
 - В. Сетевой.
 - С. Физический.
 - Д. Транспортный.
2. Какое из приведенных ниже утверждений наилучшим образом описывает функции транспортного уровня эталонной модели OSI?
 - А. Он посылает данные, используя управление потоком.
 - В. Он обеспечивает наилучший путь для доставки.
 - С. Он определяет сетевые адреса.
 - Д. Он делает возможной сетевую сегментацию.
3. Какая из следующих функций используется маршрутизатором для пересылки пакетов данных между сетями?
 - А. Приложение и передающая среда.
 - В. Определение пути и коммутация.
 - С. Широковещание и обнаружение коллизий.
 - Д. Никакая из упомянутых выше.
4. Какие из перечисленных ниже являются основными типами динамической маршрутизации?
 - А. Статический и по умолчанию.
 - В. TCP- и UDP-обмен.
 - С. Дистанционно-векторный и канальный.
 - Д. Никакие из вышеперечисленных.
5. В случае, когда все маршрутизаторы в сети работают с одной и той же информацией о топологии сети, то о сети говорят как о...
 - А. конвергированной.
 - В. формализованной.
 - С. реконфигурированной.
 - Д. ничто из вышеперечисленного.

6. Опишите цель инкапсуляции данных
7. Опишите главную функцию транспортного уровня эталонной модели OSI.
8. Опишите цель использования протокола ICMP.
9. Опишите процедуру создания окон в протоколе TCP/IP.
10. Опишите главную функцию сетевого уровня эталонной модели OSI.

Часть II

CCNA 3: Основы коммутации и промежуточной маршрутизации

- Глава 2 Начальные сведения о маршрутизации по адресам без классов
- Глава 3 Протокол OSPF для отдельной зоны
- Глава 4 Усовершенствованный протокол маршрутизации внутреннего шлюза
- Глава 5 Коммутация в локальных сетях и проектирование локальных сетей
- Глава 6 Коммутаторы
- Глава 7 Конфигурирование коммутаторов
- Глава 8 Протокол связующего дерева STP
- Глава 9 Виртуальные локальные сети
- Глава 10 Магистральный протокол VLAN



В этой главе...

- Описана междоменная маршрутизация с адресами без классов
- Рассмотрено определение номера узла и подсети с помощью маски переменной длины (variable-length subnet masking — VLSM)
- Описано обобщение маршрутов с помощью маски VLSM
- Рассмотрен протокол информации о маршрутах версии 2 (Routing Information Protocol version 2 — RIPv2)
- Описано конфигурирование протокола RIPv2
- Описано тестирование протокола RIPv2 и устранение ошибок в конфигурации

Начальные сведения о маршрутизации по адресам без классов

В настоящей главе приводятся начальные сведения о маршрутизации, не использующей классы адресов и междоменной маршрутизации без классов. Также описаны маски переменной длины для подсетей и рассмотрен протокол RIP версий 1 и 2.

Рекомендуется также выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Обзор маршрутизации по адресам без классов

При использовании маршрутизации CIDR (Classless Interdomain Routing) запись IP-адресов несколько отличается от обычной. CIDR-адрес включает в себя IP-адрес в обычном виде и информацию о том, сколько битов используются для сетевого префикса. Например, в CIDR-адресе 206.13.01.48/25 префикс /25 указывает на то, что первые 25 битов задают уникальную сеть, а оставшиеся биты указывают конкретный узел. Адрес 206.13.01.48/25 может быть также записан как 206.13.01.48 255.255.255.128.

Для чего используется адресация CIDR?

В современных маршрутизаторах применяется особый тип IP-адресов, называемых адресами бесклассовой междоменной маршрутизации (classless interdomain routing — CIDR). В этих адресах не используется понятие класса сети. В системе, использующей классы адресов, маршрутизатор сначала определяет класс адреса, а затем выделяет октеты сети и узла, исходя из установленного класса сети. Оставшиеся биты являются адресом узла.

Префикс адреса записывается за символом косой черты (/) в конце адреса, например, 10.10.10.10/30. В этой записи комбинация символов /30 является префиксом. При таком способе задания адресов части адреса, относящиеся к сети и к узлу не обязательно должны занимать целое число октетов.

Описанная в 1993г. в RFC 1517, 1518, 1519, 1520 и впервые реализованная в 1994г., адресация CIDR существенно повышает масштабируемость протокола IPv4 и его эффективность. Это достигается за счет:

- замены адресации на основе классов более гибкой и требующей меньше ресурсов бесклассовой схемой;
- обобщения маршрутов, также называемого *созданием суперсетей (supernetting)*.
- В последующих разделах обобщение маршрутов в *суперсетях* и выделение адресов описаны более подробно.

Обобщение маршрутов и создание суперсетей

Используя битовую маску вместо класса адреса для определения относящейся к сети части адреса, адресация CIDR позволяет маршрутизаторам обобщать информацию о маршрутах. Это значительно уменьшает размер таблицы маршрутизации. Иными словами, лишь один адрес и комбинация масок могут задавать маршруты к большому количеству сетей.

Как показано в табл. 2.1, без использования адресации CIDR и обобщения маршрутов маршрутизатор должен поддерживать индивидуальные позиции для каждой подсети класса В.

Затененные столбцы в табл. 2.1 указывают 16 битов, которые, согласно определению классов, представляют собой номер сети. Маршрутизаторы, использующие адресацию, основанную на классах, вынуждены при работе с сетями класса В использовать все эти 16 битов. Поскольку первые 16 битов каждого из этих восьми номеров сети уникальны, маршрутизатор считает эти восемь сетей уникальными и создает для каждой из них отдельную запись в таблице маршрутизации.

Однако в действительности эти восемь сетей имеют общие одинаковые биты, как показывает затененная часть табл. 2.2. Если последний общий бит, выделенный полужирным шрифтом в табл. 2.1, задан префиксом, то можно использовать лишь один общий номер, представляющий много подсетей. Такой подход называется обобщением маршрутов; оно позволяет сэкономить место в таблице маршрутизации и, соответственно, сократить ее размер.

Таблица 2.1 Обобщение маршрутов и создание суперсети с использованием общих 16 битов

Номер сети	Первый октет	Второй октет	Третий октет	Четвертый октет
172.24.0.0/16	10101100	00011000	00000000	00000000
172.25.0.0/16	10101100	00011001	00000000	00000000
172.26.0.0/16	10101100	00011010	00000000	00000000
172.27.0.0/16	10101100	00011011	00000000	00000000
172.28.0.0/16	10101100	00011100	00000000	00000000
172.29.0.0/16	10101100	00011101	00000000	00000000
172.30.0.0/16	10101100	00011110	00000000	00000000
172.31.0.0/16	10101100	00011111	00000000	00000000

Из табл. 2.2 видно, что у рассматриваемых в данном примере восьми адресов сетей первые 13 битов одинаковы.

Таблица 2.2 Обобщение маршрутов и использование суперсети с общими 13 битами

Номер сети	Первый октет	Второй октет	Третий октет	Четвертый октет
172.24.0.0/16	10101100	00011000	00000000	00000000
172.25.0.0/16	10101100	00011001	00000000	00000000
172.26.0.0/16	10101100	00011010	00000000	00000000
172.27.0.0/16	10101100	00011011	00000000	00000000
172.28.0.0/16	10101100	00011100	00000000	00000000
172.29.0.0/16	10101100	00011101	00000000	00000000
172.30.0.0/16	10101100	00011110	00000000	00000000
172.31.0.0/16	10101100	00011111	00000000	00000000

Используя CIDR-адресацию маршрутизатор может обобщить маршруты к этим 8 сетям с помощью 13-битового префикса 10101100 00011, который совместно используют эти восемь сетей (и только они).

Для представления этого префикса в десятичном виде оставшаяся часть адреса заполняется нулями, а затем на нее накладывается 13-битовая маска подсети:

10101100 00011000 00000000 00000000 = 172.24.0.0

11111111 11111000 00000000 00000000 = 255.248.0.0

Адрес и маска определяют не связанный с классами префикс, который обобщает маршруты к восьми сетям: 172.24.0.0/13.

При использовании адреса с префиксом для обобщения маршрутов уменьшается размер таблицы маршрутизации, благодаря чему:

- более эффективно осуществляется маршрутизация;
- уменьшается количество циклов центрального процессора CPU, которые требуются для пересчета таблицы маршрутизации и для сортировки записей таблицы маршрутизации при поиске требуемого адреса;
- уменьшаются требования к памяти маршрутизатора.

Под созданием суперсети понимается использование битовой маски для группирования нескольких сетей с адресами, основанными на классах, в сеть с одним адресом. Понятия суперсети и обобщения маршрутов используются для обозначения одного и того же процесса, хотя термин “суперсеть” чаще используется в тех случаях, когда обобщенные сети находятся под общим административным контролем.

Следует отметить, что пространство адресов классов А и В фактически исчерпано, поэтому у крупных организаций практически не остается иного выбора, кроме запроса у своих провайдеров нескольких адресов класса С. Если компании удастся приобрести непрерывный блок сетевых адресов класса С, то использование суперсетей позволяет представить эти адреса в виде одной крупной сети.

Суперсети и выделение адресов

Предположим, что компании XYZ требуются адреса для 400 рабочих станций. При использовании основанной на классах системы адресации компания XYZ могла бы обратиться к центральному агентству по выделению адресов с просьбой выделить адрес класса В. Если бы компания получила адрес класса В, а затем использовала его для адресации одной логической группы из 400 рабочих станций, то десятки тысяч адресов оказались бы неиспользуемыми. Вторым возможным решением для компании XYZ был бы запрос двух адресов класса С, которые вместе давали бы 508 ($2 * 254$) адресов. Недостатком такого решения было бы то, что компании XYZ пришлось бы осуществлять маршрутизацию между своими собственными логическими сетями, а Internet-маршрутизаторам, не имеющим установок по умолчанию (стандартных), пришлось бы поддерживать две таблицы маршрутизации для сети XYZ вместо одной.

При использовании системы адресации без классов применение суперсетей позволяет компании XYZ получить требуемое ей адресное пространство без неэффективной затраты адресов или увеличения без необходимости размеров таблиц маршрутизации. Используя адресацию CIDR компания XYZ запрашивает адресный блок у своего провайдера службы Internet, а не у центрального агентства, такого как InterNIC. Internet-провайдер оценивает потребности компании и выделяет ей адресное пространство из своего собственного крупного блока CIDR-адресов. При этом провайдер принимает на себя решение задачи управления адресным пространством в системе адресации без классов.

При использовании такой системы маршрутизаторы Internet хранят только один обобщенный маршрут к сети провайдера (маршрут к суперсети), а провайдер хранит маршруты, которые относятся к сетям своих пользователей. Такой подход радикально уменьшает размер таблиц Internet-маршрутизации.

В следующем примере компания XYZ получает от провайдера два смежных блока адресов класса С — 207.21.54.0 и 207.21.55.0. Из затененного блока в табл. 2.3 видно, что эти сетевые адреса имеют общий 23-битовый префикс 11001111 00010101 0011011.

Таблица 2.3 Суперсети и выделение адресов

Номер сети	Первый октет	Второй октет	Третий октет	Четвертый октет
207.21.54.0	11001111	00010101	00110110	00000000
207.21.55.0	11001111	00010101	00110111	00000000

При использовании суперсети с 23-битовой маской (207.21.54.0 /23) адресное пространство обеспечивает для рабочих станций значительно более 400 адресов (2^9 или 512) без напрасной затраты адресов класса В. В условиях, когда в качестве управляющей инстанции блока-CIDR адресов выступает Internet-провайдер, сети его пользователей, среди которых находится и сеть компании XYZ, могут быть анонсированы среди маршрутизаторов Internet как одна суперсеть. На рис. 2.1 Internet-провайдер управляет блоком из 256 адресов класса С и анонсирует их используя 16-битовый префикс 207.21.0.0/16.

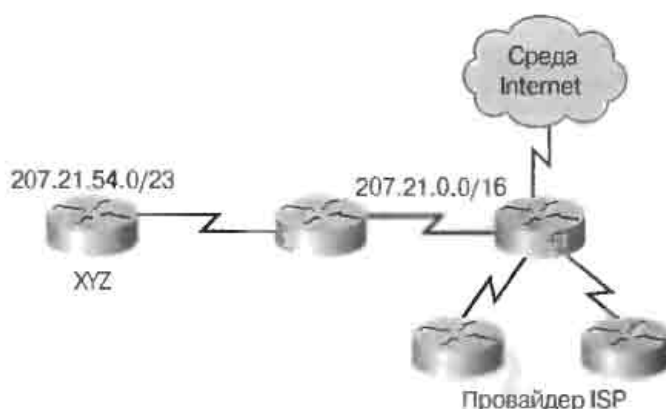


Рис. 2.1. Адресация CIDR

Адресация CIDR позволяет Internet-провайдерам иерархически распределять смежные блоки адресов и управлять ими, а адресное пространство протокола IPv4 обладает следующими преимуществами:

- эффективное выделение адресов;
- уменьшение количества записей в таблицах маршрутизации.

Использование масок подсети переменной длины

Маски подсетей переменной длины (Variable-length subnet masks — VLSM) были разработаны для того, чтобы стало возможным использование нескольких уровней IP-адресов для подсетей в одной сети. Эта стратегия может быть использована только в том случае, когда она поддерживается используемым протоколом маршрутизации, таким, например, как протокол выбора кратчайшего пути (Open Shortest Path First — OSPF) или усовершенствованный протокол внутреннего шлюза (Enhanced Interior Gateway Routing Protocol — EIGRP). Протокол RIP версии 1 был разработан ранее масок VLSM и поэтому их не поддерживает, однако протокол RIP версии 2 (RIPv2) поддерживает VLSM. Маски VLSM позволяют организации использовать более одной маски подсети в одном и том же адресном пространстве сети. Реализация масок VLSM позволяет администратору создавать “подсети в подсети” и максимально эффективно использовать адресное пространство.

Функции масок VLSM

В том случае, когда в IP-сети используется более одной маски подсети, она рассматривается как сеть с масками переменной длины, что позволяет преодолеть ограничение на конечное число подсетей фиксированного размера, налагаемое одной маской подсети. В настоящем разделе описаны функции масок подсетей переменной длины.

На рис. 2.2 сеть 172.16.14.0/24 подразделена на подсети меньшего размера.

- Подсети с одной маской — /27;
- Одна из неиспользуемых сетей с маской /27 далее подразделена на три подсети с маской /30.

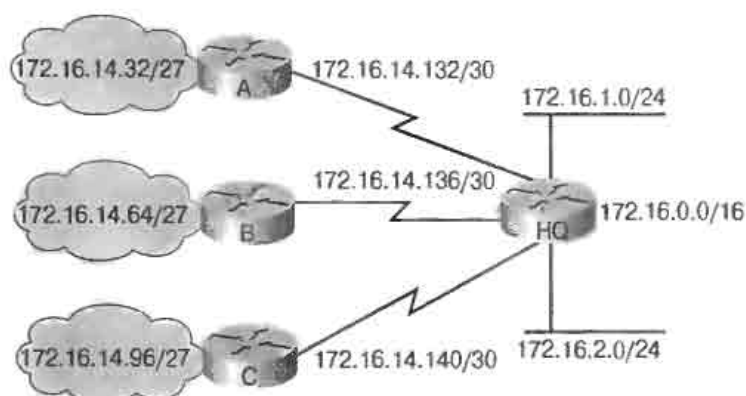


Рис. 2.2. Использование масок переменной длины

Использование масок VLSM предоставляет возможность использовать в сети более одной маски подсети и возможность создавать подсети в уже существующих подсетях. Ниже описываются преимущества использования масок VLSM.

- **Более эффективное использование IP-адресов**— Если в сети не используются маски VLSM, то компании могут использовать в сети с номером классов A, B или C лишь одну маску подсети.

Например, предположим, что сетевой адрес 172.16.0.0/16 (рис. 2.2) подразделен на подсети с использованием маски /24 и одна из подсетей этого диапазона, 172.16.14.0/24, подразделена далее на подсети с помощью маски /27. Эти малые подсети имеют адреса из диапазона от 172.16.14.0/27 до 172.16.14.224/27. На рис. 2.2 одна из этих малых подсетей разделена далее с помощью префикса /30, в результате чего созданы подсети, в которых имеется только две рабочих станции для использования в каналах распределенной сети WAN. Их адреса находятся в диапазоне от 172.16.14.128/30 до 172.16.14.156/30. На рис. 2.2 каналы сети WAN используют подсети 172.16.14.132/30, 172.16.14.136/30 и 172.16.14.140/30 из этого диапазона.

- **Большие возможности использовать обобщенные маршруты**— Маски VLSM позволяют использовать более глубокую иерархию уровней в адресном пространстве, что дает возможность более эффективно осуществлять маршрутизацию с использованием обобщенных маршрутов в таблицах маршрутизации. Например, как показано на рис. 2.2, подсеть 172.16.14.0/24 обобщает все адреса, которые относятся к подсетям деления адреса 172.16.14.0, включая адреса подсетей 172.16.14.0/27 и 172.16.14.128/30.

Рассмотрим подсети, образованные путем заимствования 3 битов из позиции узла адреса 207.21.24.0 класса C, показанные в табл. 2.4.

Таблица 2.4 Создание подсетей с помощью одной маски

Номер подсети	Адрес подсети
Подсеть 0	207.21.24.0/27
Подсеть 1	207.21.24.32/27
Подсеть 2	207.21.24.64/27

Окончание табл. 2.4

Номер подсети	Адрес подсети
Подсеть 3	207.21.24.96/27
Подсеть 4	207.21.24.128/27
Подсеть 5	207.21.24.160/27
Подсеть 6	207.21.24.192/27
Подсеть 7	207.21.24.224/27

При использовании команды **ip subnet-zero** такая маска создает семь готовых к использованию подсетей, каждая из которых может включать в себя до 30 рабочих станций. Четыре из этих подсетей могут быть использованы для удаленных офисов (филиалов) А, В, С и D данной организации.

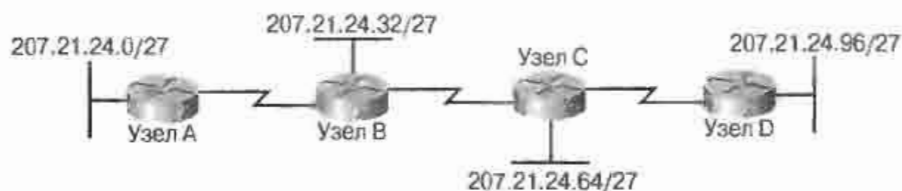


Рис. 2.3. Использование подсетей для адресации в распределенной сети WAN

К сожалению для будущего расширения остаются только три подсети; кроме того необходимо еще дать адреса (в буквальном смысле этого слова) трем каналам типа "точка-точка" между этими четырьмя узлами. Если назначить этим каналам сети WAN три оставшиеся адреса для подсетей, то этим будет исчерпано имеющееся количество IP-адресов. Более того, расточительное использование оставшихся адресов подсетей с 30 узлами для адресации этих двух сетей из двух узлов приведет к напрасной затрате более трети оставшегося адресного пространства. Как, вероятно, догадывается читатель, имеются способы избежать столь нерационального использования адресов. За последние 20 лет сетевые инженеры разработали три стратегии адресации каналов типа "точка-точка" распределенных сетей WAN.

- использование масок VLSM;
- использование частных адресов (RFC 1918);
- использование нумерованных IP-адресов

Частные адреса и нумерованные IP-адреса обсуждаются далее в разделе "Обобщение маршрутов" настоящей главы. В настоящем разделе основное внимание уделяется маскам VLSM. Если пользователь применяет маску VLSM, то его адрес класса C может быть подразделен на группы (подсети) различных размеров. Для адресации локальных сетей LAN создаются крупные подсети, а для каналов сетей WAN и в других особых случаях создаются подсети весьма малых размеров.

30-битовая маска может быть использована для создания подсетей, в которых имеется только два адреса для рабочих станций, т.е. столько, сколько требуется для соединений типа "точка-точка". На рис. 2.4 показано, как, расширяя префикс до 30, из одной подсети можно создать восемь подсетей. На нем также показано, что происходит, если одну из трех оставшихся подсетей (подсеть 6 или 207.21.24.192/27) вновь подразделить на подсети с использованием 30-битовой маски.

Подсеть 0	207.21.24.0/27		Субподсеть 0	207.21.24.192/30
Подсеть 1	207.21.24.32/27		Субподсеть 1	207.21.24.196/30
Подсеть 2	207.21.24.64/27		Субподсеть 2	207.21.24.200/30
Подсеть 3	207.21.24.96/27		Субподсеть 3	207.21.24.204/30
Подсеть 4	207.21.24.128/27		Субподсеть 4	207.21.24.208/30
Подсеть 5	207.21.24.160/27		Субподсеть 5	207.21.24.212/30
Подсеть 6	207.21.24.192/27		Субподсеть 6	207.21.24.216/30
Подсеть 7	207.21.24.224/27		Субподсеть 7	207.21.24.220/30

Рис. 2.4. Подразделение на подсети с помощью маски переменной длины

Подразделение таким способом на подсети уже существующей подсети 207.21.24.192/27 предоставляет пользователю восемь диапазонов адресов, которые могут быть использованы для сетей типа “точка-точка”. Например, сеть 207.21.24.192/30 может быть использована для последовательного канала типа “точка-точка” между маршрутизатором узла А и маршрутизатором узла В, как показано на рис. 2.5. IP-адрес сети 207.21.24.193 может быть назначен WAN-интерфейсу узла А, а адрес 207.21.24.194 — интерфейсу сети WAN узла В.



Рис. 2.5. Использование маски VLSM для адресации соединения типа “точка-точка”

Вычисление масок VLSM

Как уже говорилось выше, использование масок VLSM позволяет подразделить на подсети уже разделенный таким образом адрес. Предположим, например, что имеется сетевой адрес 172.16.32.0/20 и необходимо назначить адреса сети, в которой есть 10 рабочих станций. Для этого выделяются 20 битов для адреса сети и остающиеся 12 битов для адреса узла. Однако при таком определении адреса подсетей создается 4000 ($2^{12} - 2 = 4094$) адресов для рабочих станций, большая часть которых не будет использоваться. При использовании маски VLSM можно далее подразделить адрес 172.16.32.0/20, что предоставляет больше адресов для сетей с меньшим количеством рабочих станций в каждой сети. Если, например, подразделить сеть 172.16.32.0/20 на подсети 172.16.32.0/26, то образуется 64 (2^6) подсети, каждая из которых может поддерживать до 62 ($2^6 - 2 = 62$) рабочих станций. Такое подразделение проиллюстрировано на рис. 2.6.

Адрес подсети:	172.16.32.0/20			
В бинарной форме	10101100.00010000.00101000.00000000			
VLSM-адрес:	172.16.32.0/26			
В бинарной форме	10101100.00010000.00100000.00000000			
1-я подсеть:	172.16.32.0	0010	000.00	000000=172.16.32.0/26
2-я подсеть:	172.16.32.64	0010	000.01	000000=172.16.32.64/26
3-я подсеть:	172.16.32.128	0010	000.10	000000=172.16.32.128/26
4-я подсеть:	172.16.32.192	0010	000.11	000000=172.16.32.192/26
5-я подсеть:	172.16.33.0	0010	001.00	000000=172.16.33.0/26
		Адрес сети	Адрес Подсети VLSM	Адрес узла

Рис. 2.6. Вычисление масок VLSM

Эта же процедура используется и для дальнейшего подразделения подсети 172.16.32.0/20 на подсети 172.16.32.0/26:

- Этап 1.** Записать адрес 172.16.32.0 в двоичной форме.
- Этап 2.** Провести вертикальную черту между 20-м и 21-м битом, как показано на рис. 2.6. (/20 было первоначальной границей подсети).
- Этап 3.** Провести вертикальную черту между 26-м и 27-м битами, как показано на рис. 2.6 (первоначальная граница подсети /20 расширяется на 6 битов вправо и принимает вид /26.)
- Этап 4.** Вычислить 64 адреса подсетей, используя биты, расположенные между двумя вертикальными линиями, от младшего к старшему. На рис. 2.6 показаны первые пять полученных подсетей.

Как правило, маски VLSM используются для максимизации количества доступных сети IP-адресов. Например, поскольку последовательные каналы типа “точка-точка” требуют только двух адресов для рабочих станций, использование для них маски подсети /30 позволит избежать нерационального расходования ограниченного количества IP-адресов.

На рис. 2.7 адреса подсетей, используемые в сегментах Ethernet, получены в результате подразделения подсети с адресом 172.16.32.0/20 на несколько подсетей меньшего размера с помощью маски /26. На рис. 2.7 проиллюстрировано применение адресов подсетей в зависимости от требований к количеству адресов для рабочих станций. Например, каналы сетей WAN используют адреса подсетей с префиксом /30

Этот префикс позволяет использовать только две рабочих станции, однако этого количества достаточно для соединения типа “точка-точка” между двумя маршрутизаторами.

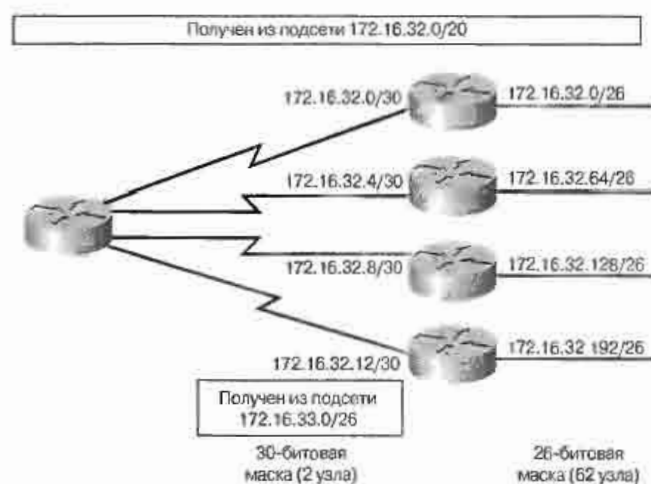


Рис. 2.7. Пример использования масок VLSM

Для вычисления адресов подсетей, используемых на каналах сетей WAN, можно создать новые подсети из одной из неиспользуемых подсетей /26. В данном примере подсеть 172.16.32.0/26 делится на подсети меньшего размера с помощью префикса /30. Это позволяет получить еще четыре новых бита для подсетей и, следовательно, 16 (2^4) новых подсетей для каналов сетей WAN. Следует помнить о том, что дальнейшее под-

разделение на подсети возможно только для неиспользуемых подсетей. Иными словами, если какие-либо из адресов подсети уже используются, то дальнейшее деление на подсети становится невозможным.



Лабораторная работа: вычисление масок VLSM

В этой лабораторной работе следует потребоваться применить маску VLSM для более эффективного использования назначенного IP-адреса и уменьшения объема информации маршрутизации на верхнем уровне.

Конфигурирование маски VLSM

В настоящем разделе рассматривается конфигурирование маски VLSM на маршрутизаторе Cisco. В примере 2.1 показаны команды, требуемые для конфигурирования маршрутизатора узла A (RTA) с 27-битовой маской на порте Ethernet (e0) и 30-битовой маски на последовательном порте (s0).

Пример 2.1 Конфигурирование маски VLSM

```
RTA(config)# interface e0
RTA(config-if)# ip add 207.21.24.33 255.255.255.224
RTA(config-if)# interface s0
RTA(config-if)# ip add 207.21.24.193 255.255.255.252

RTA# show ip route
Codes: C-connected, S-static, I-IGRP, R-RIP, M-mobile, B-BGP
D-EIGRP, EX-EIGRP external, O-OSPF, IA-OSPF inter area
E1-OSPF external type1, E2-OSPF external type 2, E-EGP
i-IS-IS, L1-IS-IS level-1, L2-IS-IS level-2,
*-candidate default

Gateway of last resort is not set
207.21.24.0 is variably subnetted, 2 subnets, 2 masks
C 207.21.24.32 255.255.255.224 is directly connected, Ethernet0
C 207.21.24.192 255.255.255.252 is directly connected, Serial0
```

Для того, чтобы в сети с масками переменной длины маршрутизаторы могли обмениваться информацией маршрутизации, они должны посылать маски в своих обновлениях маршрутизации. Если в сообщениях обновления маршрутов не будет маски подсети, то для своей работы маршрутизаторы будут иметь только класс адреса и свою собственную маску подсети.

Правильно работать с масками VLSM будут только протоколы маршрутизации, которые игнорируют правила классов для IP-адресов и используют бесклассовые префиксы (см. табл. 2.5)

Таблица 2.5. Основанные на классах и бесклассовые протоколы маршрутизации

Протоколы маршрутизации на основе классов	Протоколы маршрутизации, не использующие классов
RIP версии 1	RIP версии 2
IGRP	EIGRP

Окончание табл. 2.5

Протоколы маршрутизации на основе классов	Протоколы маршрутизации, не использующие классов
EGP	OSPF
BGP 3	IS-IS
	BGP 4

Использование масок VLSM протоколами RIP и IGRP

Протоколы RIP версии 1 и IGRP, типичные протоколы внутреннего шлюза, не поддерживают масок VLSM, поскольку они не пересылают информацию о подсетях в своих сообщениях обновлений маршрутизации. Для определения префикса подсети с заданным адресом после получения сообщения обновления эти основанные на классах протоколы маршрутизации используют один из описанных ниже методов.

- Если маршрутизатор получает информацию о сети и принимающий интерфейс принадлежит к той же сети (но к другой подсети), то маршрутизатор применяет маску подсети, сконфигурированную на принимающем интерфейсе.
- Если маршрутизатор получает информацию о сети, адрес которой отличается от адреса, сконфигурированного на принимающем интерфейсе, то он применяет маску подсети по умолчанию (основанную на классах).

Несмотря на имеющиеся у него ограничения протокол RIP является весьма популярным протоколом маршрутизации, который поддерживается практически всеми IP-маршрутизаторами. Популярность протокола RIP объясняется его простотой и универсальной совместимостью. Однако первая версия этого протокола (RIPv1) страдает серьезными недостатками.

- Протокол RIPv1 не посылает в своих сообщениях обновлений маршрутизации маски подсети. Без информации о подсетях маски VLSM и адресация CIDR использоваться не могут.
- Сообщения обновления этого протокола рассылаются широковещательно, что увеличивает объем передаваемой служебной информации.
- Этот протокол не поддерживает аутентификации.

В 1988г. в RFC 1058 предлагалось в новой версии 2 протокола RIP устранить эти недостатки.

- В протоколе RIPv2 рассылается информации о подсетях и поддерживаются как маски VLSM, так и адресация CIDR.
- Обновления маршрутизации рассылаются методом многоадресной рассылки с использованием адреса класса D 224.0.0.9, что обеспечивает более эффективную работу сети.
- В обновлениях маршрутизации поддерживается аутентификация.

Благодаря наличию этих двух важных функций протокол RIPv2 всегда предпочтительнее, чем RIPv1, кроме случая, когда унаследованные в сети устройства не могут его поддерживать.

При первой установке протокола RIP на маршрутизаторе Cisco этот маршрутизатор прослушивает сообщения обновления маршрутизации как 1-й, так и 2-й версий, однако отправляет только сообщения 1-й версии. Для того, чтобы воспользоваться преимуществами функций 2-й версии следует отключить поддержку 1-й версии и включить рассылку обновлений 2-й версии с помощью команды, показанной в примере 2.2.

Пример 2.2 Конфигурирование протокола RIP версии 2

```
Router(config)#router rip
Router(router-config)#version 2
```

Простота и эффективность протокола RIP гарантируют, что он продолжит существовать и применяться. Уже разработана новая версия, которая будет поддерживать сети протокола IPv6.

**Лабораторная работа: базовое конфигурирование протокола RIP**

В этой лабораторной работе требуется сконфигурировать рабочие станции и маршрутизаторы. Также нужно установить схему IP-адресации, используемой в сети класса B, и сконфигурировать протокол RIP на маршрутизаторах.

Обобщение маршрутов

Использование адресации CIDR и масок VLSM не только предотвращает нерациональное расходование адресов, но также способствует агрегированию или обобщению маршрутов. Если бы не эта функция обобщения маршрутов, то магистральная маршрутизация в Internet стала бы невозможной еще до 1997г.

На рис. 2.8 показано, как обобщение маршрутов уменьшает нагрузку на маршрутизаторы восходящего направления.

Сложная иерархия сетей разного размера и взаимодействия подсетей обобщается в различных точках с использованием префикса адреса до тех пор, пока вся сеть не будет анонсирована как один обобщенный маршрут.

Следует обратить внимание на то, что такое обобщение маршрутов или использование суперсетей возможно только в том случае, если все маршрутизаторы сети используют бесклассовый протокол маршрутизации, такой как OSPF или EIGRP. Протоколы маршрутизации, не использующие классов, передают префикс длины (маску подсети) с 32-битовым адресом в сообщениях об обновлении маршрутизации. На рис. 2.8 обобщенный маршрут, который в конечном итоге поступает к провайдеру, содержит 20-битовый префикс, общий для всех адресов данной организации: 200.199.48.0/20 или, в двоичной форме, 11001000 11000111 0001. Для того, чтобы обобщение маршрутов функционировало должным образом, необходимо аккуратно назначать адреса иерархическим способом, так, чтобы обобщенные адреса имели одинаковые обобщающие биты.

Например, как показано на рис. 2.9, маршрутизатор A может либо послать три обновления маршрутов, либо обобщить их в одном номере сети. На рис. 2.9 показано, как маршруты 172.16.25.0/24, 172.16.26.0/24 и 172.16.27.0/24 могут быть обобщены в одном адресе 172.16.0.0/16

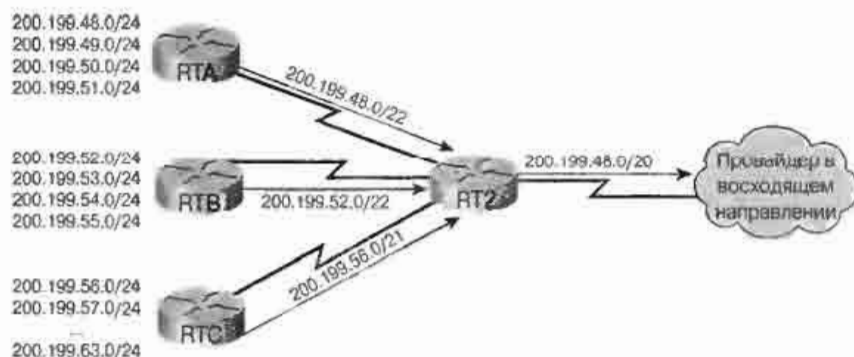


Рис. 2.8. Обобщение маршрутов

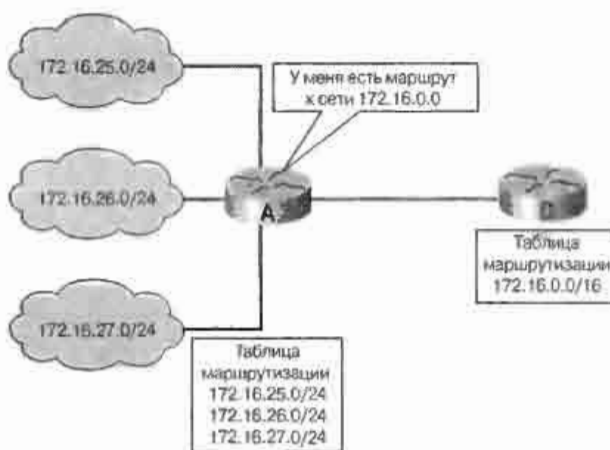


Рис. 2.9. Дополнительное обобщение маршрутов

Маршрутизатор на рис. 2.9 может обобщить маршруты к сети 172.16.0.0/16, включая все подсети этой сети. Однако если бы где-либо в сети существовали другие подсети сети 172.16.0.0 (например, если бы сеть 172.16.0.0 не была непрерывной), то выполненное таким образом обобщение маршрутов было бы недействительным. Сети, которые не являются непрерывными, и обобщение маршрутов в них обсуждаются далее в настоящей главе. Другим преимуществом обобщения маршрутов в крупной сложной сети является то, что изменение топологии можно изолировать от других маршрутизаторов. Т.е. если в домене 172.16.27.0/24 какой-либо канал находится в состоянии флэппинга (flapping) (т.е. то работает, то не работает), то обобщенный маршрут не изменяется. Соответственно, ни одному внешнему по отношению к данному домену не требуется изменять свою таблицу маршрутизации в связи с этим флэппингом.

Обобщение маршрутов наиболее эффективно в среде с подсетями, когда сетевые адреса в непрерывных блоках являются степенями числа 2. Например, 4, 16 или 512 адресов могут быть представлены в таблице маршрутизации одной записью, поскольку обобщающие маски являются двоичными — так же как и маски подсетей, поэтому обобщение будет происходить на двоичных границах (квадраты числа 2).

Протоколы маршрутизации обобщают маршруты на основе совместно используемых номеров подсетей всей сети. Бесклассовые протоколы маршрутизации, такие как RIPv2, OSPF, Intermediate System-to-Intermediate System (IS-IS) и EIGRP, поддерживают обобщение маршрутов на основе адресов подсетей, включая адресацию с помощью масок

VLSM. Основанные на классах протоколы маршрутизации, такие как RIPv1 и IGRP, автоматически обобщают маршруты на границе сети с классами и не поддерживают обобщение маршрутов на всех других границах. Обобщение маршрутов описано в RFC 1518, "An Architecture for IP Address Allocation with CIDR."

Обобщение маршрутов в октете

Предположим, что маршрутизатор получает обновления маршрутизации для следующих маршрутов (рис. 2.10):

172.16.168.0/24
172.16.169.0/24
172.16.170.0/24
172.16.171.0/24
172.16.172.0/24
172.16.173.0/24
172.16.174.0/24
172.16.175.0/24

172.16.168.0/24 =	10101100	00010000	10101	000	00000000
172.16.169.0/24 =	172	16	10101	001	0
172.16.170.0/24 =	172	16	10101	010	0
172.16.171.0/24 =	172	16	10101	011	0
172.16.172.0/24 =	172	16	10101	100	0
172.16.173.0/24 =	172	16	10101	101	0
172.16.174.0/24 =	172	16	10101	110	0
172.16.175.0/24 =	172	16	10101	111	0

Число общих битов = 21

Полный адрес: 172.16.168.0/21

Число

отличающихся битов = 11

Рис. 2.10. Обобщение маршрутов в октете

Для определения обобщенного маршрута маршрутизатор определяет количество старших битов, которые совпадают во всех адресах. После записи всех IP-адресов в бинарном формате легко определить количество старших битов, которые совместно используются всеми IP-адресами. На рис. 2.10 общими для всех адресов являются 21 бит. Следовательно наилучшим обобщенным маршрутом является 172.16.168.0/21. Обобщение адресов возможно в том случае, когда количество адресов является какой-либо степенью числа 2. Если количество адресов не является степенью 2, то следует разделить эти адреса на группы и обобщить маршруты этих групп отдельно.

Для того, чтобы маршрутизатор мог обобщить наибольшее количество маршрутов в одном, план адресов должен быть организован иерархическим образом. Такой подход особенно важен при использовании масок VLSM.

Обобщение маршрутов во фрагментарной сети

Основанные на классах протоколы маршрутизации автоматически выполняют обобщение маршрутов на границах сети. Такое поведение, которое не может быть изменено протоколами RIPv1 или IGRP, имеет приведенные ниже важные следствия.

- В крупных сетях различного типа подсети не анонсируются.
- Сети, не являющиеся непрерывными, невидимы друг для друга.

На рис. 2.11 протокол RIPv1 не анонсирует подсети 172.16.5.0/25 и 172.16.6.0/25, поскольку этот протокол не может анонсировать подсети: оба маршрутизатора, маршрутизатор А и маршрутизатор В анонсируют этот маршрут 172.16.0.0. Однако это приводит к путанице при маршрутизации через сеть 192.168.14.0. В этом примере маршрутизатор С получает маршруты, относящиеся к сети 172.16.0.0, с двух различных направлений, вследствие чего не может принять правильного решения о маршрутизации.

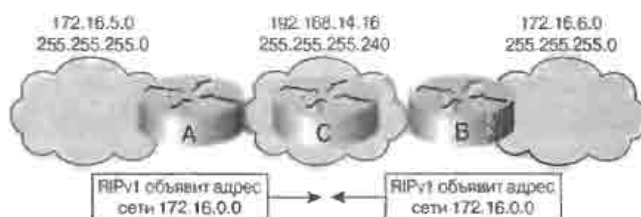


Рис. 2.11. Обобщение маршрутов во фрагментированных сетях

Возникшую проблему можно разрешить путем использования какого-либо из протоколов: RIPv2, OSPF, IS-IS или EIGRP, однако не следует использовать обобщение маршрутов, поскольку маршруты подсетей будут анонсированы вместе с их нынешними масками подсетей.

Программное обеспечение IOS Cisco также предоставляет функцию нумерованных IP-(адресов), которая позволяет разделять фрагментированные сети нумерованным каналом. Нумерованным называется канал, который может еще не иметь назначенного номера IP-адреса, однако его видят другие подсети, что позволяет предотвратить разрывы в каналах. Наличие нумерованного канала без использования IP-функции нумерованного канала может привести к разрывам в каналах.

Флэппинг маршрутов

Флэппинг маршрутов происходит в том случае, когда интерфейс маршрутизатора быстро переходит из состояния “включен” в состояние “выключен” (“up” and “down” states). Это явление может вызываться рядом причин, в том числе неисправностью интерфейса или плохо терминированной средой передачи.

Обобщение маршрутов эффективно изолирует находящиеся в восходящем направлении маршрутизаторы от проблем флэппинга. Если интерфейс маршрутизатора RTC, подсоединенный к сети 200.199.56.0 выходит из строя, то RTC удалит этот маршрут из своей таблицы маршрутизации. Если бы эти маршрутизаторы не были сконфигурированы для то обобщения маршрутов, то RTC отправил бы срочное (unplanned) сообщение маршрутизатору RTZ об удалении сети 200.199.56.0. В свою очередь маршрутизатор RTZ отправил бы сообщение обновления маршрутизатору в восходящем направлении и т.д. Каждый раз, когда на эти маршрутизаторы поступает новая информация, их процессоры приступают к работе. Эта работа может потребовать довольно больших вычислительных затрат и повлиять на производительность работы сети (особенно в случае OSPF-маршрутизации).

Рассмотрим какое влияние на производительность сети оказывает восстановление через несколько секунд работоспособности интерфейса маршрутизатора RTC, связанного с сетью 200.199.56.0. Маршрутизаторы посылают друг другу сообщения обновления и заново пересчитывают маршруты. Кроме того, что произойдет если через несколько секунд канал RTC вновь выйдет из строя? А затем вновь вернется в работоспособное состояние? Такая ситуация называется флэппингом и она делает маршрутизатор практически неработоспособным, поскольку он “завален” сообщениями обновлений и пересчетами маршрутов.

Однако конфигурирование обобщения маршрутов предотвращает воздействие флэппинга маршрута RTC на другие маршрутизаторы. Маршрутизатор RTC посылает RTZ сообщение обновления о суперсети (200.199.56.0 /21), которая включает в себя восемь сетей (от 200.199.56.0 до 200.199.63.0). при этом потеря одной сети не делает недействительным маршрут к суперсети. Хотя маршрутизатор RTC может оказаться постоянно занятым своим собственным флэппингом на маршруте, маршрутизатор RTZ и все находящиеся в восходящем направлении маршрутизаторы ничего не заметят. Таким образом, обобщение маршрутов эффективно изолирует другие маршрутизаторы от проблемы флэппинга маршрута.

Протокол RIP версии 2

Сети должны быть масштабируемы. Иными словами, они должны быть способными к росту. Выбранный протокол маршрутизации может оказать большое влияние на масштабируемость сети, поэтому выбор протокола маршрутизации весьма важен. В целом межсетевой протокол маршрутизации (Routing Internet Protocol — RIP) рассматривается как подходящий для всех небольших сетей, однако в крупных сетях он не обеспечивает масштабируемости. Протокол RIPv1 основан на использовании классов адресов, в то время как RIPv2 является бесклассовым протоколом маршрутизации. Ограничение, налагаемое использованием классов состоит в том, что на границах крупных сетей требуется автоматическое обобщение маршрутов к границе сети, в которой используются классы. Это означает, что протокол RIPv1 не поддерживает маски VLSM, в то время как RIPv2 их поддерживает.

Краткая история протокола RIP

В международных сетях, таких как Internet, маловероятно использование лишь одного протокола маршрутизации. Более вероятно, что сеть организована как множество автономных систем (autonomous system — AS). Каждая из них обычно администрируется как отдельная сетевая структура.

Каждая автономная система AS имеет свою технологию маршрутизации, которая отличается от используемых в других автономных системах. Протоколы маршрутизации, используемые в одной автономной системе AS, в целом называются протоколами внутреннего шлюза (Interior Gateway Protocol — IGP). Для передачи информации маршрутизации между автономными системами используются отдельные протоколы, имеющие общее название протоколов внешнего шлюза (Exterior Gateway Protocol — EGP). Протокол RIP был предназначен для выполнения функций протокола внутреннего шлюза IGP в автономных системах среднего размера. Он не предназначался для использования в более сложных сетевых средах.

Протокол RIPv1 считается бесклассовым протоколом внутреннего шлюза IGP. Он является дистанционно-векторным протоколом, в котором происходит широко-

вещательная рассылка всей таблицы маршрутизации каждому соседнему маршрутизатору с заранее заданным интервалом (например, 30 секунд). В качестве метрики протокол RIP использует количество переходов, максимальное значение которого равно 15. Как уже говорилось ранее, при получении пакета обновления маршрутизации для выработки префикса сетевого адреса происходит выбор одной из приведенных ниже двух альтернатив.

- Если маршрутизатор получает информацию о сети и принимающий интерфейс принадлежит к той же самой сети, но к другой подсети, то маршрутизатор применяет маску подсети, сконфигурированную. На принимающем интерфейсе.
- Если же маршрутизатор получает информацию о сетевом адресе, НЕ СОВПАДАЮЩЕМ со сконфигурированным на входном интерфейсе, то принимается значение интерфейса по умолчанию (основанное на классах).

Для адресов класса А стандартная маска с учетом класса имеет вид 255.0.0.0.

Для адресов класса В стандартная маска с учетом класса имеет вид 255.255.0.0.

Для адресов класса С стандартная маска с учетом класса имеет вид 255.255.255.0.

Протокол RIPv1 получил широкое распространение и приобрел популярность поскольку он поддерживается практически всеми IP- маршрутизаторами. Его популярность основана на его простоте и универсальной совместимости. Протокол RIPv1 поддерживает распределение нагрузки на шести маршрутах с равной оценкой, количество которых может достигать шести (по умолчанию принимается количество возможных маршрутов равно четырем).

Следует помнить об ограничениях протокола RIPv1:

- Он не пересылает информацию о масках подсети в своих обновлениях маршрутов;
- Обновления маршрутизации рассылаются широковещательно, т.е. с адресом 255.255.255.255;
- Аутентификация не поддерживается;
- Этот протокол не поддерживает масок подсети переменной длины (variable-length subnet masking — VLSM) и бесклассовой междоменной маршрутизации (classless interdomain routing — CIDR).

В примере 2.3 показано конфигурирование протокола RIPv1.

Пример 2.3. Конфигурирование протокола RIP v1

```
Sydney(config)# router rip
Sydney(config-router)# network 172.16.0.0
Sydney(config-router)# network 192.168.100.0
```

Функции протокола RIP версии 2

Протокол RIPv2 представляет собой усовершенствованную версию RIPv1. Он имеет ряд общих с RIPv1 функций:

- Используется метрика количества переходов с максимальным значением 15;
- Он также является дистанционно-векторным протоколом;

- Для предотвращения петель маршрутизации используются таймеры удержания со значением по умолчанию равным 180 секундам;
- Для предотвращения петель маршрутизации используется расщепление горизонта;
- Значение метрики, равное 16 переходам рассматривается как бесконечное;
- Вместе с маршрутом передается маска подсети;
- Поддерживаются маски VLSM путем передачи такой маски вместе с каждым маршрутом, что полностью определяет подсеть;
- Поддерживается аутентификация;
- Используется как передача открытым текстом так и использование шифрования MD5;
- В сообщении обновлений маршрутизации включается IP-адрес маршрутизатора следующего перехода;
- Используются тэги внешних маршрутов;
- Поддерживаются обновления многоадресной маршрутизации.

Протокол RIPv2 поддерживает префиксную маршрутизацию, что позволяет ему рассылать информацию о маске подсети вместе с обновлением маршрута. Он также поддерживает бесклассовую маршрутизацию, в которой различные подсети одной сети могут использовать различные маски подсети (маски подсетей переменной длины).

Протокол RIPv2 поддерживает аутентификацию в своих обновлениях маршрутизации. В качестве проверки аутентификации на интерфейсе может быть использован набор ключей. RIPv2 позволяет использовать в своих пакетах различные типы аутентификации. При этом возможен выбор открытого текста или MD5. По умолчанию принимается открытый текст (Для аутентификации источника обновления маршрутизации может быть использована MD5). MD5 обычно используется для шифрования и включения секретных паролей и не имеет известного обращения. RIPv2 рассылает многоадресные обновления маршрутизации, используя адрес класса D, что обеспечивает повышенную эффективность.

Сравнение протоколов RIPv1 и RIPv2

Для определения направления и расстояния до любого канала в объединенной сети протокол RIP использует дистанционно-векторные алгоритмы. Если к пункту назначения существует несколько маршрутов, то RIP выбирает маршрут с наименьшим количеством переходов. Однако, поскольку количество переходов является единственной метрикой, используемой протоколом RIP, выбранный таким образом маршрут к пункту назначения не обязательно является наилучшим. При этом учитывается только количество переходов и не принимаются во внимание другие параметры маршрута.

Протокол RIPv1 позволяет маршрутизаторам обновлять свои таблицы маршрутизации с заранее заданным интервалом. По умолчанию такой интервал равен 30 секундам. Постоянная рассылка обновлений маршрутизации очень быстро повышает объем передачи данных по сети. Для предотвращения петель маршрутизации протокол RIP имеет ограничение на максимальное количество переходов равное 15. Если сеть-получатель находится на расстоянии более 15 переходов, то она рассматривается как недостижимая и пакет отбрасывается. Такой подход создает проблемы масштабируе-

мости если маршрутизация происходит в крупных неоднородных сетях. Протокол RIPv1 для предотвращения петель использует также расщепление горизонта. Это означает, что на интерфейсе маршрут анонсируется только в том случае, если обновление маршрутизации поступило не на этот интерфейс. Для предотвращения петель используется также таймер удержания. Его действие выражается в том, что после получения обновления маршрутизатор игнорирует любую новую информацию маршрутизации в течение промежутка времени заданного для таймера удержания. Ниже приводится общее описание работы протокола RIPv1 при его использовании на маршрутизаторе.

- Непосредственно подсоединенные подсети изначально известны маршрутизатору и эти маршруты анонсируются соседним маршрутизаторам;
- Обновления маршрутов рассылаются широковещательно все соседние маршрутизаторы оповещаются одним сообщением;
- Для получения информации о новых маршрутах маршрутизаторы просматривают обновления маршрутов;
- Для каждого маршрута в обновлении приводится значение метрики, которые характеризует его качество;
- Если существует несколько маршрутов, то выбирается маршрут с наименьшей метрикой;
- Топологическая информация находится в таблицах маршрутизации, которые как минимум содержат информацию о подсетях и метрике;
- От соседних маршрутизаторов ожидаются периодические сообщения об обновлении маршрутов.
- В случае отсутствия требуемого заданным интервалом регулярного сообщения соответствующий ранее полученный маршрут удаляется из таблицы маршрутизации;
- Предполагается, что полученное от соседнего маршрутизатора сообщение было им и отправлено.

В табл. 2.6 приведено сравнение протоколов RIPv1 и RIPv2.

Таблица 2.6. Сравнение протоколов RIPv2 и RIPv1

RIPv2	RIPv1
Поддерживает аутентификацию	Не поддерживает аутентификации
Поддерживает бесклассовые маски подсетей VLSM	Поддерживаются только маски, использующие классы
Следующий узел	Следующий шлюз
Многоадресная рассылка по адресу 224.0.0.9	Широковещательная рассылка—255.255.255.255
Интерфейс использует теги маршрутов	Не использует тегов маршрутов
Поддерживает также все функции RIPv1	

Конфигурирование протокола RIP версии 2

Протокол RIPv2 является протоколом динамической маршрутизации, который конфигурируется путем указания имени протокола маршрутизации (RIP версия 2) с последующим назначением IP-адресов сетей без указания значений для подсетей. В настоя-

в этом разделе описываются основные команды, используемые для конфигурирования протокола RIPv2 на маршрутизаторе Cisco.

Для включения протокола динамической маршрутизации необходимо выполнить описанные ниже действия.

- Выбрать протокол маршрутизации, такой, например, как RIPv2.
- Назначить IP-адреса сетей без указания значений для подсетей.
- Назначить на интерфейсах адреса сетей и подсетей, а также соответствующие маски.

Для обмена информацией с другими маршрутизаторами в протоколе RIPv2 используется многоадресная рассылка. Значения метрики для маршрутов помогают маршрутизатору находить наилучшие маршруты к сетям или подсетям.

Процесс маршрутизации начинается выполнением команды **router**. Команда **network** вызывает выполнение маршрутизатором следующих трех функций:

- с интерфейса рассылаются многоадресные сообщения об обновлении маршрутов;
- сообщения обновлений обрабатываются, если они поступают на этот же интерфейс;
- анонсируется подсеть, непосредственно подсоединенная к данному интерфейсу.

Выполнение команды **network** требуется для того, чтобы процесс маршрутизации определил, какие интерфейсы будут участвовать в отправке и получении обновлений маршрутизации. Команда **network** запускает протокол маршрутизации на всех интерфейсах, которые имеет данный маршрутизатор в конкретной сети. Команда **network** также позволяет маршрутизатору анонсировать эту сеть.

Совместное выполнение команд **router rip** и **version 2** задает протокол RIPv2 в качестве протокола маршрутизации, а команда **network** задает подсоединенную сеть, участвующую в процессе маршрутизации.

Конфигурация для маршрутизатора А, показанного на рис. 2.12, включает в себя следующие команды:

- **router rip** — задает RIP в качестве протокола маршрутизации;
- **version 2** — задает использование версии 2 протокола RIP;
- **network 172.16.0.0** — задает непосредственно подсоединенную сеть;
- **network 10.0.0.0** — задает непосредственно подсоединенную сеть.

Интерфейсы маршрутизатора А, подсоединенные к сетям 172.16.0.0 и 10.0.0.0 или к их подсетям, будут получать и отправлять обновления маршрутизации протокола RIPv2. Эти сообщения позволят маршрутизатору узнать топологию сети. Маршрутизаторы В и С имеют аналогичные RIP-конфигурации, но с другими номерами сетей.

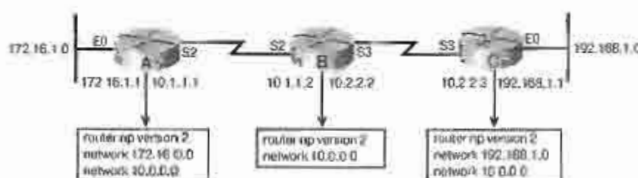


Рис. 2.12. Конфигурирование протокола RIP



Лабораторная работа: переход с протокола RIPv1 на RIPv2

В этой лабораторной работе требуется включить на маршрутизаторе протокол RIPv1, а затем перейти на протокол RIPv2.

Тестирование протокола RIP V2

Команды **show ip protocols** и **show ip route** отображают информацию о протоколах маршрутизации и о таблице маршрутизации. В настоящем разделе описано использование группы команд **show** для тестирования конфигурации протокола RIP.

Команда **show ip protocols** отображает параметры протоколов маршрутизации и информацию о таймере, связанные с данным маршрутизатором. В примере 2.4 приведен вывод по команде **show ip protocols** для маршрутизатора A, показанного на рис. 2.12.

Пример 2.4 Вывод по команде show ip protocols

```
RouterA# show ip protocols

Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 12 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing rip
Default Version Control: send version 1 receive any version
Interface Send Receive Triggard RIP Key-Chain
Ethernet0 1 1 2
Serial2 1 1 2
EIGRP maximum metric variance 1
Routing for Networks:
 10.0.0.0
172.16.0.0
Routing Information Sources:
Gateway Distance Last Update(this router) 120 02:12:15
10.1.1.2 120 01:09:01
Distance: (default is 120)
```

В примере 2.4 на маршрутизаторе сконфигурирован протокол RIP, который рассылает информацию обновленной таблицы маршрутизации каждые 30 секунд (этот интервал задается в конфигурации). Если маршрутизатор, на котором сконфигурирован протокол RIP, не получает от другого маршрутизатора сообщения об обновлении маршрутов в течение 180 секунд или более, то он помечает маршрут, обслуживаемый неответчающим маршрутизатором, как недействительный. В примере 2.4 таймер удержания установлен на 180 секунд, поэтому обновление для маршрута, который был недействительным, а в данный момент вновь стал работоспособным, будет оставаться в состоянии удержания "возможно, неработоспособен" до тех пор, пока не пройдет 180 секунд.

Если не поступило нового сообщения обновления после 240 секунд "flush timer set", то маршрутизатор удаляет записи в таблице маршрутизации для данного маршрутизатора. В примере 2.4 прошло 18 секунд с того момента, как маршрутизатор A получил обновление маршрутизации от маршрутизатора B.

Маршрутизатор вводит маршруты для сетей, перечисленных после строки "Routing for Networks" ("Маршрутизация для сетей"). Маршрутизатор получает маршруты от соседних RIP-маршрутизаторов, перечисленных после строки "Routing Information Sources" ("Источники информации маршрутизации").

Расстояние по умолчанию, равное 120, относится к административному расстоянию для RIP-маршрута.

Для вывода обзорной информации об IP-информации интерфейса и его состоянии может быть использована команда **show ip interface brief**.

Команда **show ip route** отображает содержимое таблицы IP-маршрутизации, как показано в примере 2.5.

Пример 2.5 Вывод по команде show ip route

```
RouterA# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
172.16.0.0/16 is subnetted, 1 subnets
C 176.16.1.0/24 is directly connected, Ethernet0
10.0.0.0/24 is subnetted, 2 subnets
R 10.2.2.0/24 [120/1] via 10.1.1.2, 00:00:07, Serial2
C 10.1.1.0/24 is directly connected, Serial2
R 192.168.1.0/24 [120/1] via 10.1.1.2, 00:00:07, Serial2
```

Таблица маршрутизации содержит записи для всех известных сетей и подсетей, а также специальный код, который указывает, каким образом была получена эта информация. Отдельные поля вывода по этой команде и их функции описаны в табл. 7.2.

Таблица 2.7. Описание вывода таблицы маршрутов

Поле вывода	Описание
R или C	Идентифицирует источник маршрута. Например, литерой C обозначаются маршруты к непосредственно подсоединенным сетям. Литерой R обозначаются маршруты, полученные от другого RIP-маршрутизатора
192.168.1.0 10.2.2.0	Обозначает IP-адрес удаленной сети
120/1	Первое число в скобках представляет собой административное расстояние источника; второе число — метрика для данного маршрута (например, 1 переход).
Via 10.1.1.2	Указывает адрес маршрутизатора следующего перехода к удаленной сети
00:00:07	Указывает время, прошедшее со времени последнего обновления маршрута в формате ЧЧ:ММ:СС
Serial 2	Указывает интерфейс, через который можно получить доступ к данной конкретной сети

Администратору следует просмотреть таблицу маршрутизации чтобы выяснить, имеется ли в ней информация о маршрутах. Если обмена информацией маршрутизации не происходит (т.е. в том случае, если вывод по команде **show ip route** не отображает записей о маршрутах, полученных с помощью протокола маршрутизации), то на маршрутизаторе следует использовать команды **show running-config** или **show ip protocols** привилегированного режима EXEC для обнаружения ошибок в конфигурировании протокола маршрутизации.



Лабораторная работа: тестирование конфигурации протокола RIPv2

В этой лабораторной работе требуется включить на маршрутизаторе протокол RIP версий 1 и 2 и протестировать маршрутизацию протокола RIPv2 с помощью различных команд show.

Устранение ошибок конфигурирования протокола RIP

В настоящем разделе описано использование команды **debug ip rip**.

Для отображения обновлений маршрутизации протокола RIP по мере их получения и отправки следует выполнить команду **debug ip rip**. Для отключения этого отладочного режима следует использовать команды **no debug all** или **undebug all**.

В примере 2.6 показано как маршрутизатор, на котором включен режим отладки, получает обновления маршрутизации от маршрутизатора-источника, имеющего адрес 10.1.1.2. Этот маршрутизатор отправил информацию о двух получателях в обновлении таблицы маршрутизации. Маршрутизатор, находящийся в режиме отладки, также отправил сообщения, в обоих случаях по широковещательному адресу 255.255.255.255 в качестве адреса получателя. Число в скобках представляет собой адрес источника, инкапсулированный в IP-заголовке. Поскольку используется протокол RIPv1, сообщения обновлений рассылаются по широковещательному адресу. Протокол RIPv2 рассылал бы эти сообщения по адресу 224.0.0.9 многоадресной рассылки класса D, что было бы более эффективно.

Пример 2.6 Вывод по команде **debug ip rip**

```
RouterA# debug ip rip
RIP protocol debugging is on
RouterA#
00:06:24: RIP: received v1 update from 10.1.1.2 on Serial2
00:06:24: 10.2.2.0 in 1 hops
00:06:24: 192.168.1.0 in 2 hops
00:06:33: RIP: sending v1 update to 255.255.255.255 via Ethernet0
(172.16.1.1)
00:06:34: network 10.0.0.0, metric 1
00:06:34: network 192.168.1.0, metric 3
00:06:34: RIP: sending v1 update to 255.255.255.255 via Serial2
(10.1.1.2)
00:06:34: network 176.168.0.0, metric 1
```

Иногда по команде **debug ip rip** выводятся и другие строки, подобные приведенным ниже, которые появляются в начале работы или при возникновении в сети какого-либо события, такого, например, как переход интерфейса или очистка пользователем таблицы маршрутизации вручную.

```
RIP: broadcasting general request on Ethernet0
RIP: broadcasting general request on Ethernet1
```

Строка, подобная приведенной ниже, может быть вызвана неправильно сформированным пакетом от передатчика.

```
RIP: bad version 128 from 160.89.80.43
```

Выводимая по команде **debug ip rip** информация и значение отдельных полей описаны в табл. 2.8.

Таблица 2.8. Объяснение вывода по команде debug ip rip

Выводимая информация	Описание
RIP:broadcasting general request on Ethernet0 as startup	Изменение типа интерфейса или ручная очистка интерфейса пользователем
RIP:bad version 128 from 160.89.80.43	Неправильно сформированный пакет с адреса 160.89.80.43
RIP:received v2 update from 150.100.2.3 on Serial0	Отображает версию RIP по которой производит отправку сообщений 150.100.2.3
RIP:sending v1 update to 255.255.255.255 via Serial0 (150.100.2.2)	Указывает на то, что на интерфейсе Serial0 сконфигурирован протокол RIPv1
RIP:ignored v1 packet from 150.100.2.2 (illegal version)	Указывает на то, что протокол RIPv1 на маршрутизаторе не сконфигурирован
RIP:sending v2 update to 224.0.0.9 via FastEthernet0 (150.100.3.1)	Указывает на то, что протокол RIPv2 сконфигурирован и рассылает сообщения обновления маршрутизации
RIP:build update entries 150.100.2.0/24 via 0.0.0.0, metric 1, tag0	Указывает на использование стандартных маршрутов и тегов маршрутов



Лабораторная работа: устранение ошибок в конфигурировании протокола RIPv2 с помощью команды Debug

В этой лабораторной работе следует сконфигурировать протокол RIPv2 на обоих маршрутизаторах. После этого с помощью команды **debug** следует проверить правильность работы протокола RIP и проанализировать данные, передаваемые между этими маршрутизаторами.

Стандартные маршруты

Как правило, маршрутизаторы узнают о маршрутах к получателям тремя различными способами, описанными ниже.

- *Статические маршруты* устанавливаются вручную системным администратором в виде явного адреса следующего перехода к пункту назначения. Они полезны из соображений безопасности и для уменьшения объема передачи данных, поскольку другие маршруты неизвестны.
- *Стандартные маршруты* также устанавливаются вручную системным администратором в качестве маршрута передачи данных в том случае, когда иные маршруты к получателю отсутствуют. Стандартные маршруты уменьшают размеры таблиц

маршрутизации. Если в таблице маршрутизации отсутствует запись, соответствующая данной сети-получателю, то пакет направляется в эту стандартную сеть.

- *Динамическая маршрутизация* означает, что маршрутизатор узнает о маршрутах к получателям за счет получения регулярных сообщений об обновлении маршрутов от других маршрутизаторов при посредстве протоколов маршрутизации, таких как, например, протокол RIP.

Простой статический маршрут может быть задан с использованием команды **ip route**, как показано в примере 2.7.

Пример 2.7 Статический маршрут

```
Router(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1
```

Команда **ip default-network** устанавливает стандартный маршрут в сети, использующей протокол динамической маршрутизации, как показано в примере 2.8.

Пример 2.8. Стандартный динамический маршрут

```
Router(config)#ip default-network 192.168.20.0
```

После того, как в таблице маршрутизации были заданы все сети, для которых требовалось выполнить конфигурирование, часто оказывается полезным обеспечить, чтобы все остальные пакеты также направлялись в какой-то определенный пункт назначения, такой, например, как маршрутизатор, подсоединенный к сети Internet. Задаваемый таким образом маршрут называется стандартным маршрутом маршрутизатора. Все пакеты, для которых нет маршрута в таблице маршрутизации, направляются на назначенный стандартный интерфейс маршрутизатора.

На рис. 2.13 показана стандартная сеть (сеть-получатель по умолчанию), в которую будут направляться пакеты, как показано в примере 2.8.

На маршрутизаторах, подсоединенных к маршрутизатору, имеющему стандартный статический маршрут, как правило конфигурируется команда **ip-default network**.

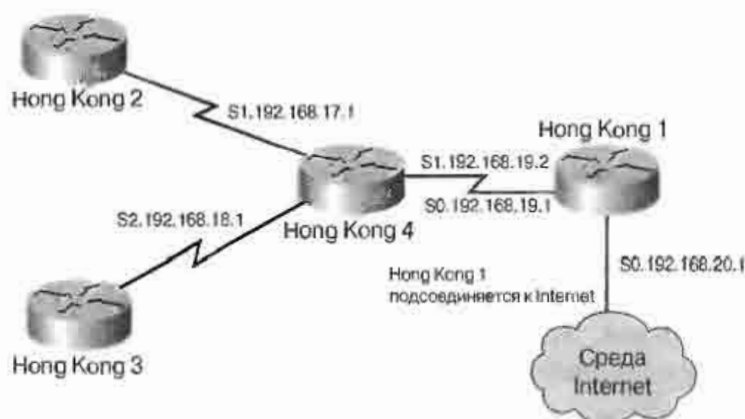


Рис. 2.13. Маршрутизация и использованием стандартных маршрутов w/RIP

В примере 2.9 приведена команда для определения статического стандартного маршрута, который может быть использован при статической или динамической маршрутизации.

На рис. 2.13 маршрутизаторы Hong Kong 2 и Hong Kong 3 используют Hong Kong 4 в качестве стандартного шлюза.

Маршрутизатор Hong Kong 4 использует интерфейс 192.168.19.2 в качестве шлюза по умолчанию. Hong Kong 1 направляет в Internet все пакеты от своих внутренних узлов и рабочих станций. Для того, чтобы маршрутизатор Hong Kong 1 мог выполнять эту операцию, необходимо сконфигурировать стандартный маршрут, как показано в примере 2.9.

Пример 2.9 Установка стандартного маршрута

```
HongKong1(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.1
```

Нули представляют любую сеть-получатель с любой маской. Маршруты по умолчанию называют четырехнулевыми маршрутами. На диаграмме маршрутизатор Hong Kong 1 имеет один выход в Internet через интерфейс 192.168.20.1.

Резюме

В данной главе были изложены рассмотрены следующие основные положения.

- Междоменная маршрутизация без классов (Classless Interdomain Routing — CIDR) заменяет прежние методы назначения IP-адресов, использование классы адресов.
- Маршрутизация CIDR была введена в 1983 году в RFC 1517, 1518, 1519, and 1520 и реализована в 1994г.
- Маршрутизация CIDR вводит понятие суперсети и обобщение маршрутов.
- Использование масок VLSM позволяет сетевому администратору более эффективно выделять и использовать IP-адреса. Использование бесклассовой маршрутизации повышает эффективность использования VLSM, поскольку границы сети с классами перестают быть необходимыми.
- Обобщение маршрутов наиболее эффективно в сети, подразделенной на подсети.
- Протоколы RIPv1 и RIPv2 являются дистанционно-векторными протоколами маршрутизации, которые используют в качестве метрики количество переходов и широковещательно рассылают обновления маршрутизации каждые 30 секунд.
- Протокол RIPv1 не рассылает информацию о подмасках сети в своих обновлениях маршрутизации. При отсутствии информации о подсетях поддержка VLSM и CIDR невозможна. Эти широковещательно рассылаемые сообщения увеличивают объем передачи данных; этот протокол не поддерживает аутентификации.
- Протокол RIPv2 рассылает информацию о подсетях и поддерживает VLSM и CIDR. Он рассылает обновления маршрутизации используя адреса класса D для повышения эффективности. В нем также поддерживается аутентификация в сообщениях обновления.
- Команда **router RIP** задает RIP в качестве протокола маршрутизации.

- Команда **network** задает подсоединенную сеть, участвующую в процессе RIP-маршрутизации. Протокол RIPv2 поддерживает аутентификацию, маски подсетей, информацию о следующем узле, многоадресную рассылку и теги маршрутов.
- В дополнение к изложенному в настоящей главе материалу рекомендуется изучить относящиеся к ней видеоклипы, фотографии и выполнить лабораторные работы, находящиеся на компакт-диске CD-ROM, прилагаемом к книге.

Глоссарий

Маска подсети переменной длины (variable-length subnet mask — VLSM). Способ задания для нескольких различных подсетей одной и той же сети одной маски подсети. Использование VLSM позволяет оптимизировать использование доступного пространства адресов.

Междоменная бесклассовая маршрутизация (classless interdomain routing — CIDR). Протоколы бесклассовой маршрутизации основаны на обобщении маршрутов. Маршрутизация CIDR позволяет маршрутизаторам группировать маршруты для уменьшения объема информации маршрутизации, передаваемой базовыми маршрутизаторами. При использовании CIDR несколько IP-сетей выглядят для внешних по отношению к ним сетей как одна крупная сеть. В формате CIDR IP-адреса и соответствующие маски подсетей записываются в виде четырех октетов, разделенных точками, за которыми следует косая черта и префикс, задающий маску подсети.

Обобщение маршрутов (route summarization). Объединение анонсированных адресов в протоколах OSPF и IS-IS. В протоколе OSPF это приводит к тому, что другим зонам (areas) анонсируется один обобщенный маршрут граничным маршрутизатором данной зоны.

Создание суперсетей (supernetting). Обобщение нескольких IP-адресов сетей, анонсируемое как один бесклассовый адрес сети.

Стандартный маршрут (default route). Маршрут, выбираемый устройством в том случае когда другие варианты отсутствуют.

Статический маршрут (static route). Зафиксированный и не изменяющийся в процессе маршрутизации маршрут.

Контрольные вопросы

1. Какие два из приведенных ниже адресов являются действительными адресами подсетей в том случае, когда сеть 172.17.15.0/24 делится на подсети с помощью дополнительных 4 битов? (Выбрать два.)
 - A. 172.17.15.0
 - B. 172.17.15.8
 - C. 172.17.15.40
 - D. 172.17.15.96
 - E. 172.17.15.248
2. Какая из приведенных ниже масок подсетей является наиболее эффективной при использовании в каналах “точка-точка” распределенной сети WAN?

- A. 255.255.255.0
 - B. 255.255.255.224
 - C. 255.255.255.252
 - D. 255.255.255.248
3. Что из приведенного ниже является функцией маршрутизации CIDR? (Выбрать все правильные)
- A. Адресация без использования классов
 - B. Создание суперсетей
 - C. Увеличение количества записей в таблице маршрутизации
 - D. Обобщение маршрутов
4. Что из нижеперечисленного является обобщенным адресом для сетей 172.21.136.0/24 и 172.21.143.0/24?
- A. 172.21.136.0/21
 - B. 172.21.136.0/20
 - C. 172.21.136.0/22
 - D. 172.21.128.0/2
5. Какой из приведенных ниже протоколов маршрутизации не содержит в своих сообщениях обновления информации о маске подсети?
- A. EIGRP
 - B. OSPF
 - C. RIPv1
 - D. RIPv2
6. Какой метод представляет коллекцию IP-адресов в одном IP-адресе?
- A. Бесклассовая маршрутизация
 - B. Создание суперсетей
 - C. Трансляция адресов
 - D. Обобщение маршрутов



В этой главе...

- Описан протокол OSPF
- Рассмотрен процесс выбора назначенного маршрутизатора
- Перечислены типы сетей OSPF
- Описано конфигурирование протокола OSPF в отдельной зоне
- Описано тестирование работы протокола OSPF и устранение неисправностей

Протокол OSPF для отдельной зоны

Протоколы маршрутизации состояния каналов представляют собой сложные и масштабируемые протоколы маршрутизации. В настоящей главе описывается промышленный стандарт протокола маршрутизации состояния каналов, называемого протоколом выбора кратчайшего пути (Open Shortest Path First — OSPF). В ней описан процесс выбора маршрутизатора OSPF и функционирование протокола OSPF в различных сетях. Приводятся также инструкции по конфигурированию базовой сети протокола OSPF для одной зоны. Описаны также процедуры тестирования конфигурации протокола OSPF и устранения ошибок в ней.

Рекомендуется также выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Основные понятия протокола OSPF для одной зоны

Протоколы маршрутизации по состоянию каналов отличаются от дистанционно-векторных протоколов. Протоколы состояния каналов осуществляют лавинную рассылку информации о состоянии каналов и предоставляют возможность каждому маршрутизатору иметь полную картину топологии сети. При использовании дистанционно-векторных протоколов маршрутизаторам неизвестна полная топологическая картина сети. Протокол OSPF является протоколом состояния каналов.

При использовании протокола OSPF наилучший маршрут определяется с помощью алгоритма выбора кратчайшего пути (созданного компьютерным специалистом Дейкстры [Dijkstra]); этот наилучший маршрут выбирается как маршрут к каналу с наименьшей оценкой (стоимостью). Алгоритм выбора кратчайшего пути (shortest path first — SPF) был создан для сетевых соединений типа “точка-точка”. Для реализации протокола OSPF в разнообразных современных сетях ему необходимо знать тип сети, в которой он функционирует.

Перед тем как начнется обмен информацией о состоянии каналов, протокол OSPF устанавливает связь с соседними маршрутизаторами. Для этой цели используется входящий в OSPF протокол Hello.

OSPF является сложным (комплексным) протоколом и описывается набором требуемых для его функционирования операций.

Обзор протокола OSPF

Протокол OSPF является протоколом маршрутизации состояния каналов, основанным на открытых стандартах. Он описан в нескольких стандартах инженерной группы Internet (Internet Engineering Task Force — IETF), последним из которых является стандарт RFC 2328.

Термин “открытый” в протоколе OSPF означает его доступность для всех пользователей; протокол OSPF не является фирменным протоколом. В настоящее время протоколу OSPF вследствие его масштабируемости все чаще отдается предпочтение перед протоколом информации о маршрутах (Routing Information Protocol — RIP) при выборе для сети протокола внутреннего шлюза (Interior Gateway Protocol — IGP).

Протокол RIP не допускает расширения за предельное значение 15 переходов, медленно сходится и может выбирать медленные маршруты, поскольку не учитывает при выборе маршрута критически важные факторы, такие как ширина полосы пропускания. Протокол OSPF учитывает эти ограничения и, как показывает опыт его использования, является надежным, масштабируемым протоколом маршрутизации, эффективным для современных сетей. Протокол OSPF может быть использован в отдельной зоне в небольших сетях и в нескольких зонах для больших сетей. Протокол OSPF может быть использован в крупномасштабных сетях. Маршрутизация OSPF может быть расширена на крупные сети при условии, что при проектировании сети использовались иерархические принципы построения сетей. При проектировании крупных сетей OSPF используются иерархические принципы. Эти принципы состоят в подсоединении нескольких зон к зоне распределения (нулевой зоне или зоне 0), также называемой *магистралью*. Такой принцип проектирования позволяет осуществлять полный контроль над сообщениями об обновлении маршрутов. Задание зон уменьшает объем служебной нагрузки маршрутизации, ускоряет сходимость, ограничивает возможную нестабильность сети одной зоной и повышает производительность сети. Для эффективного контроля сетевых операций сети протокола OSPF делятся на части, называемые *зонами*. Главная зона называется нулевой зоной (Area 0). Все сети OSPF имеют зону 0 и используют ее как главную зону распределения.

Терминология протокола OSPF

Протокол OSPF является протоколом состояния каналов и функционирует иначе, чем дистанционно-векторные протоколы. Маршрутизаторы канального уровня идентифицируют соседние маршрутизаторы и обмениваются с ними информацией. С протоколом OSPF связан набор новых терминов. Они приведены на рис. 3.1.

Информация, собранная от соседних маршрутизаторов OSPF не является полной таблицей маршрутизации. Каждый OSPF-маршрутизатор сообщает своим соседям о состоянии своих соединений или каналов, как показано на рис. 3.2. Эта информация распространяется методом лавинной рассылки. Под лавинной рассылкой понимается отправка одной и той же информации со всех портов, за исключением того порта, на который она поступила. Маршрутизатор OSPF объявляет о состоянии своих каналов и передает далее полученную им информацию о состоянии каналов другим маршрутизаторам.

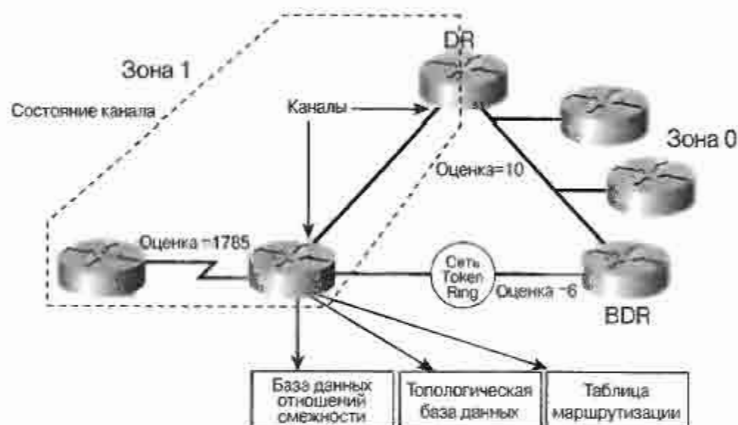


Рис. 3.1. Терминология протокола OSPF

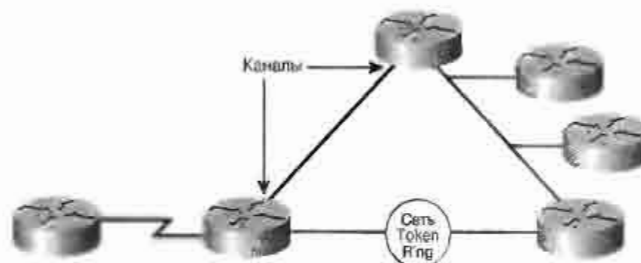


Рис. 3.2. Каналы протокола OSPF

Маршрутизаторы в зоне 1 обрабатывают эту информация и строят свою топологическую базу данных, называемую также базой данных состояния каналов. Эта база данных показана на рис. 3.3. Все маршрутизаторы в одной OSPF-зоне имеют одну и ту же базу данных состояния каналов. Каждый маршрутизатор имеет, таким образом, одну и ту же информацию о состоянии каналов и базу данных о своих соседях. Автономная система (autonomous system — AS) может быть подразделена на ряд зон, представляющих собой группы связанных (непрерывных) сетей и подсоединенных к ним устройств. Маршрутизаторы с несколькими интерфейсами могут быть участниками нескольких зон. Эти маршрутизаторы, называемые граничными маршрутизаторами зон (Area Border Routers) поддерживают отдельные топологические базы данных для каждой зоны.

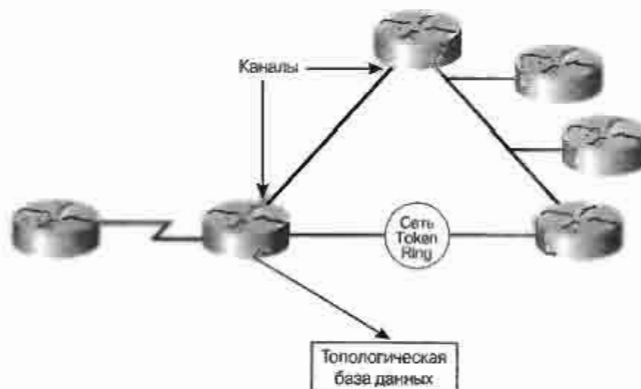


Рис. 3.3. Топологические базы данных (состояния каналов) протокола OSPF

После этого каждый маршрутизатор применяет *алгоритм выбора кратчайшего пути* (*shortest path first — SPF algorithm*), также называемый алгоритмом Дейкстры к своей копии базы данных. Эти вычисления определяют наилучший маршрут к пункту назначения. Алгоритм SPF складывает стоимости (оценки) для отдельных переходов, которые обычно базируются на ширине полосы пропускания, как показано на рис. 3.5. Минимальная оценка маршрута добавляется к таблице маршрутизации, также называемой таблицей пересылки.

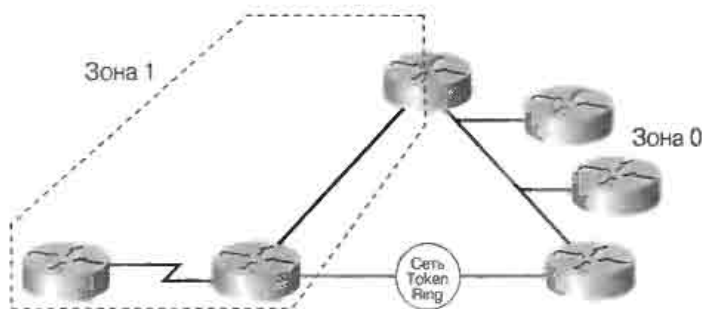


Рис. 3.4. Зона каналов протокола OSPF

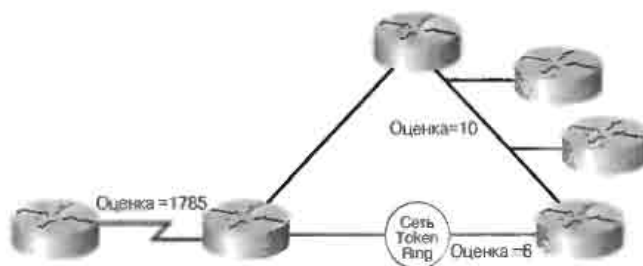


Рис. 3.5. Вычисление оценки согласно протоколу OSPF

OSPF-маршрутизаторы записывают информацию о своих соседях в таблицу смежных устройств. Для уменьшения объема информации, которой обмениваются соседние устройства в одной и той же сети маршрутизаторы OSPF избирают *назначенный маршрутизатор* (*designated router — DR*) и *резервный назначенный маршрутизатор* (*backup designated router — BDR*). Эти маршрутизаторы служат фокусными точками при обмене информацией маршрутизации.

Состояния протокола OSPF

OSPF-маршрутизаторы устанавливают связи или состояния (*states*) со своими соседями для эффективного совместного использования информации канального уровня. Иначе функционируют дистанционно-векторные протоколы маршрутизации, такие как RIP, которые широковещательно рассылают полностью свои таблицы маршрутизации со всех своих интерфейсов в надежде, что эту таблицу получит требуемый маршрутизатор. В стандартном режиме маршрутизаторы протокола RIP каждые 30 секунд рассылают только один тип сообщения — свою полную таблицу маршрутизации. В отличие от них маршрутизаторы OSPF используют пять различных типов пакетов для идентификации своих соседей и обновления информации маршрутизации канального уровня. В табл. 3.1. описаны типы пакетов протокола OSPF.

Эти пять типов пакетов позволяют протоколу OSPF осуществлять разнообразные и сложные типы связей. Более подробно эти типы пакетов обсуждаются далее в настоящей главе. На данном этапе читателю следует познакомиться с различными связями, которые можно установить между маршрутизаторами OSPF, с различными типами сетей OSPF и с протоколом Hello, входящим в состав протокола OSPF.

Таблица 3.1. Типы пакетов протокола OSPF

Тип пакета протокола OSPF	Описание
Тип 1 — Hello	Используется для создания и поддержки таблицы соседних устройств
Тип 2 — Пакет описания базы данных (Database description packet — DBD)	Описывает содержимое базы данных состояния каналов OSPF-маршрутизатора
Тип 3 — Запрос информации о состоянии каналов	Запрашивает отдельные фрагменты базы данных состояния каналов маршрутизатора
Тип 4 — Обновление состояния каналов (Link-state update — LSU)	Передает объявления о состоянии каналов (link-state advertisements — LSA) соседним маршрутизаторам
Тип 5 — Подтверждение получения объявления о состоянии каналов (Link-state acknowledgement — LSACK)	Подтверждает получение от соседнего устройства объявления LSA

Ключевым фактором при проектировании OSPF-сетей и при устранении ошибок в них является понимание связей или состояний, которые возникают между OSPF-маршрутизаторами. Интерфейсы OSPF маршрутизаторов могут находиться в одном из приведенных ниже семи состояний. Связи между соседними OSPF-маршрутизаторами последовательно проходят эти состояния сверху вниз в приведенном ниже списке.

- Состояние отключения (Отключенное) (Down)
- Инициализация (Init)
- Двустороннее соединение (Two-way)
- ExStart
- Обмен (Exchange)
- Загрузка (Loading)
- Состояние установки полной связи между соседними (смежными) устройствами (Full adjacency)

Состояние отключения

Состояние отключения (Down State) имеет место в том случае, когда обмен информацией между соседними устройствами не происходил. Маршрутизаторы ожидают перехода в следующее состояние — состояние инициализации.

Состояние инициализации (Init State)

В состоянии инициализации (Init State) OSPF-маршрутизаторы регулярно (обычно каждые 10 секунд) посылают пакеты 1-го типа (Hello) для установки связи с соседними маршрутизаторами. Когда некоторый интерфейс получает первый Hello-пакет, соответствующий маршрутизатор переходит в состояние инициа-

ции (Init) — это означает, что маршрутизатору известно о наличии у него соседнего устройства и он ожидает перехода связи с ним в следующее состояние.

Существует два типа связи между маршрутизаторами: двусторонняя связь и состояние полной связи соседних устройств, хотя между этими двумя состояниями находятся несколько промежуточных состояний. Перед тем, как станет возможной установка какого-либо типа связи, маршрутизатор должен получить от своего соседа сообщение Hello.

Состояние двусторонней связи

Каждый OSPF-маршрутизатор пытается установить со всеми своими соседями по сети OSPF состояние двусторонней связи или двунаправленное соединение, используя для этого пакеты Hello.

Кроме различной иной информации пакеты Hello содержат список известных отправителю соседних OSPF-маршрутизаторов.

Маршрутизатор переходит в состояние двусторонней связи в тот момент, когда он видит себя в пакете Hello, полученном от соседнего устройства. Например, как показано на рис. 3.6, когда маршрутизатор RTB узнает, что маршрутизатор RTA знает о нем (RTB), маршрутизатор RTB объявляет о наличии состояния двусторонней связи между ним и маршрутизатором RTA.



Рис. 3.6. Состояние двусторонней связи протокола OSPF

Состояние двусторонней связи является базовым состоянием двух соседних устройств протокола OSPF, однако в этом состоянии совместное использование маршрутизаторами информации маршрутизации еще не происходит. Для того, чтобы узнать о состоянии каналов других маршрутизаторов и, в конечном итоге, создать таблицу маршрутизации, каждый OSPF-маршрутизатор должен образовать по крайней мере одно соединение (состояние смежности) с соседним устройством. Состояние смежности представляет собой более тесную связь между OSPF-маршрутизаторами, включающее в себя ряд последовательных состояний, которые базируются не только на Hello-сообщениях, но и на других четырех типах OSPF-пакетах. Маршрутизаторы, которые пытаются стать смежными друг для друга устройствами, обмениваются информацией маршрутизации еще до того, как будет полностью установлено состояние смежности. Первым этапом установки состояния полной смежности является состояние ExStart.

Состояние ExStart

В техническом аспекте в момент когда маршрутизатор и его соседнее устройство входят в состояние ExStart, их связь характеризуется как состояние смежности, однако в действительности эти устройства еще не являются полностью смежными. Состояние ExStart устанавливается с помощью пакетов описания базы данных (database description — DBD)(пакетов 2-го типа). Эти пакеты также обозначаются как пакеты DDP.

Для обсуждения того, какой маршрутизатор в данном соединении будет ведущим ("master"), а какой ведомым ("slave"), маршрутизаторы используют пакеты Hello, а для обмена содержимым баз данных используются пакеты DBD (рис. 3.7).

Маршрутизатор с максимальным значением OSPF-идентификатора (ID) становится ведущим. (OSPF-идентификатор ID маршрутизатора обсуждается далее в настоящей главе). Когда два соседних маршрутизатора определяют свои роли как ведомого и ведущего, они входят в состояние обмена (Exchange) и начинают направлять друг другу информацию маршрутизации.

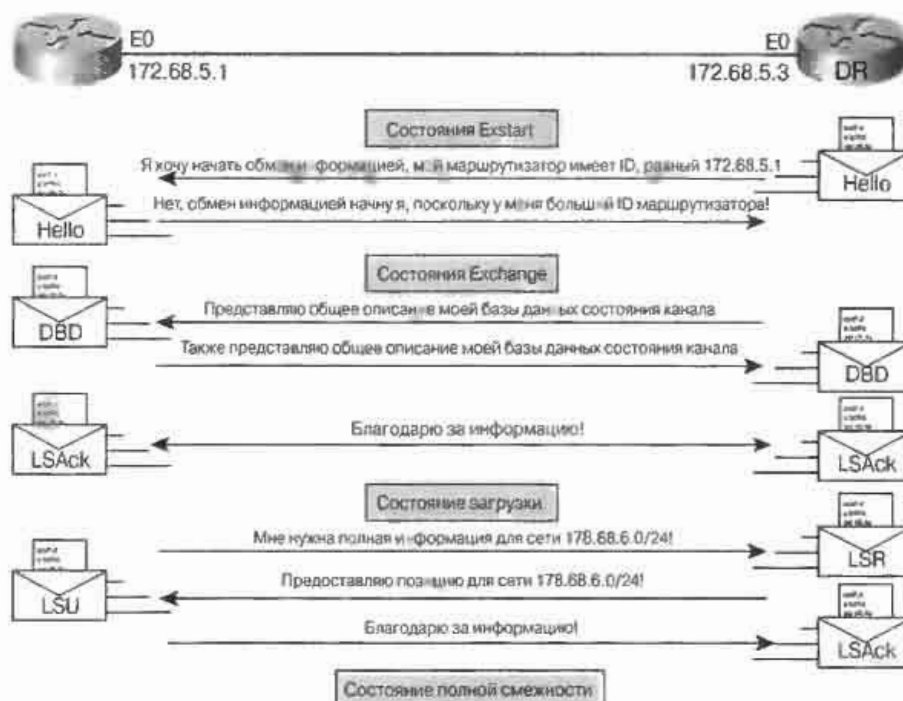


Рис. 3.7. Обнаружение маршрутизатора по протоколу OSPF

Состояние обмена

В состоянии обмена Exchange соседние маршрутизаторы используют пакеты 2-го типа (DBD) для отправки друг другу своей информации о состоянии каналов, как показано на рис. 3.7. Иными словами, маршрутизаторы описывают друг другу свои базы данных состояния каналов. При этом маршрутизаторы сравнивают полученную информацию с информацией, содержащейся в их собственных базах данных состояния каналов. Если какой-либо из маршрутизаторов получает информацию о канале, которая пока отсутствует в его базе данных, то он запрашивает у соседнего маршрутизатора полное обновление. Полный обмен информацией происходит в состоянии загрузки (Loading).

Состояние загрузки (Loading)

После того, как оба маршрутизатора описали друг другу свои базы данных, они могут запросить более полную информацию, используя пакеты 3-го типа — запросы состояния каналов (link-state request — LSR). Когда маршрутизатор получает запрос LSR, он отвечает отправкой обновления маршрутизации, используя пакет 4-го типа — пакет обновления состояния каналов (link-state update — LSU). Эти LSU-пакеты 4-го типа содержат объявления актуального состояния каналов (link-state ad-

vertisement — LSA), которые составляют суть протоколов маршрутизации состояния каналов. Как показано на рис. 3.7, подтверждение получения LSU-пакетов 5-го типа осуществляется с помощью пакетов 5-го типа, называемых подтверждением состояния каналов (link-state acknowledgment — LSAck).

Состояние полной смежности

После того, как полностью реализовано состояние загрузки (Loading), маршрутизаторы являются полностью смежными. Каждый маршрутизатор поддерживает свой список смежных соседних маршрутизаторов, называемый также базой данных смежных устройств. Эту таблицу смежных устройств не следует смешивать с базой данных состояния каналов или с базой данных пересылки. В табл. 3.2 перечислены важные базы данных протокола OSPF.

Таблица 3.2. Базы данных протокола OSPF

База данных	Описание
База данных о смежных устройствах	Список всех соседних устройств, с которыми данный маршрутизатор установил двусторонние соединения.
База данных канального уровня (топологическая база данных)	Информация обо всех маршрутизаторах сети. Эта база данных отражает текущую сетевую топологию. Все маршрутизаторы одной и той же области имеют идентичные базы данных канального уровня
База данных пересылки (таблица маршрутизации)	Список маршрутов, генерируемый при выполнении алгоритма к база данных канального уровня. Таблица маршрутизации каждого маршрутизатора уникальна и содержит информацию о том, каким образом и по каким маршрутам следует отправлять пакеты, предназначенные другим маршрутизаторам

Сравнение протокола OSPF с дистанционно-векторными протоколами маршрутизации

Протокол OSPF использует технологию состояния канала связи, в то время как протокол RIP использует дистанционно-векторную технологию. Маршрутизаторы состояния канала поддерживают общую картину сети и обмениваются информацией о состоянии канала сразу после обнаружения изменений в сетевой топологии. Маршрутизаторы состояния канала не осуществляют периодической широковещательной рассылки своих таблиц маршрутизации, как это делают дистанционно-векторные протоколы, и, таким образом, в меньшей степени используют полосу пропускания для поддержки своих таблиц маршрутизации. Использование протокола RIP целесообразно в небольших сетях.

Протокол OSPF был разработан для удовлетворения потребностей крупных масштабируемых сетей. Протокол RIP выбирает наилучший маршрут на основе количества требуемых переходов. Выбранный таким образом маршрут может оказаться маршрутом с низкой скоростью передачи. Протокол RIP и другие дистанционно-векторные протоколы используют для вычисления наилучших маршрутов простые алгоритмы. Алгоритм SPF довольно сложен. Маршрутизатору, использующему дистанционно-векторную маршрутизацию, как правило, требуется меньший объем памяти и менее мощный процессор, чем маршрутизатору, использующему протокол OSPF.

Протокол OSPF выбирает наилучший маршрут на основе оценки, отражающей ширину полосы пропускания. Чем больше полоса пропускания, тем меньше OSPF-оценка канала. В качестве наилучшего протокол OSPF выбирает самый быстрый свободный от петель маршрут, проходящий по дереву кратчайшего пути. Протокол OSPF гарантирует отсутствие петель в выбранном маршруте, в то время как дистанционно векторные протоколы могут вызвать появление петель маршрутизации.

Если каналы нестабильны, то лавинная рассылка информации о состоянии канала может привести к появлению *несинхронизированных объявлений состояния канала (link-state advertisement — LSA)* и к несогласованным решениям, принимаемыми маршрутизаторами.

В протоколе OSPF затрагиваются следующие вопросы:

- Скорость конвергенции (сходимости);
- Поддержка масок переменной длины для подсетей (variable-length subnet masking — VLSM);
- Размер сети;
- Выбор маршрута;
- Группировка членов.

В крупных сетях конвергенция по протоколу RIP может потребовать нескольких минут, поскольку всем маршрутизаторам требуется скопировать свои таблицы маршрутизации и обменяться ими с другими непосредственно подсоединенными маршрутизаторами. В протоколе OSPF конвергенция происходит быстрее, поскольку лавинная рассылка осуществляется не для всей таблицы маршрутизации, а только для произошедших изменений в сети. В том случае, когда рассылаются только изменения в сети, обновление маршрутизации называется *ступенчатым (incremental update)*.

OSPF представляет собой бесклассовый протокол и поддерживает маски VLSM. Протокол RIP версии 1 (RIPv1) не поддерживает маски VLSM, однако протокол RIP версии 2 (RIPv2) обладает такими функциями. В протоколе RIP количество переходов ограничено 15, а сеть, удаленная более чем на 15 узлов (маршрутизаторов) рассматривается как недостижимая. Это ограничивает использование протокола RIP сетями с простой топологией и незначительным количеством узлов. В пользователе OSPF практически отсутствуют ограничения на количество узлов и переходов и он может использоваться в средних и крупных сетях. Протокол RIP выбирает маршрут путем добавления 1 к значению счетчику переходов к сети, сообщаемому соседним маршрутизатором. Затем сравниваются значения счетчиков для различных маршрутов и выбирается маршрут с наименьшим расстоянием, т. е. с минимальным количеством переходов. Этот алгоритм прост и не требует мощного процессора в маршрутизаторе или большого объема памяти. При определении наилучшего маршрута протокол OSPF не учитывает доступную полосу пропускания каналов. Протокол OSPF выбирает маршрут используя оценку — метрику, основанную на ширине полосы пропускания. Для того, чтобы каждый маршрутизатор мог выбрать наилучший маршрут, все OSPF-маршрутизаторы должны получить полную информацию обо всех сетях.

Этот алгоритм достаточно сложен и использование протокола OSPF требует более мощных маршрутизаторов и большего объема памяти. Протокол RIP использует плоскую топологию и все маршрутизаторы в зоне использования протокола RIP обмениваются друг с другом всей своей информацией. Протокол OSPF использует области,

называемые *зонами*. Сеть может быть подразделена на кластеры маршрутизаторов. Благодаря этому протокол OSPF ограничивает передачу потоков данных в эти зоны, а изменения в одной зоне не оказывают влияния на производительность работы в других зонах. Такой иерархический подход позволяет эффективно масштабировать сеть.

Алгоритм выбора кратчайшего пути

Для определения наилучшего пути к пункту назначения протокол OSPF использует алгоритм выбора кратчайшего пути. В этом алгоритме наилучшим является маршрут с наименьшей оценкой. Этот алгоритм был создан голландским компьютерным специалистом Дейкстры (Dijkstra) и обнародован в 1959 году. В этом алгоритме сеть рассматривается как множество узлов, соединенных каналами типа “точка-точка”. Каждому каналу присваивается некоторое значение оценки. Каждому узлу назначается некоторое имя. Каждый узел имеет полную базу данных всех каналов, поэтому всем узлам известна вся информация о физической топологии сети. После этого алгоритм выбора кратчайшего пути вычисляет свободную от петель топологию, используя узел в качестве начальной точки и последовательно анализируя его информацию о смежных узлах.

Типы сетей протокола OSPF

Для того, чтобы совместно использовать информацию о маршрутизации, OSPF-маршрутизаторы должны установить связь с соседними устройствами; каждый маршрутизатор пытается установить отношения смежности или соседства по крайней мере с одним маршрутизатором каждой IP-сети, к которой подсоединены его порты. Некоторые маршрутизаторы могут попытаться установить отношения смежности со всеми соседними маршрутизаторами, в то время как другие — только с одним или двумя. OSPF-маршрутизаторы определяют, с какими иными маршрутизаторами им следует установить отношения смежности, на основе типа сети, которая их соединяет.

После того, как между соседними устройствами установлены отношения смежности, между ними происходит обмен информацией о состоянии канала. Как показано на рис. 3.8, и перечислено в приводимом ниже списке, интерфейсы OSPF маршрутизаторов распознают три типа сетей.

- Широковещательные сети множественного доступа;
- Нешироковещательные сети множественного доступа (nonbroadcast multiaccess — NBMA);
- Сети с каналами типа “точка-точка”.

Сетевой администратор может сконфигурировать на каком-либо интерфейсе и четвертый тип сетей — сеть типа “точка-несколько точек”. В табл. 3.3 приведены типы OSPF-сетей. В сети *множественного доступа (multiaccess network)* невозможно заранее узнать, сколько маршрутизаторов будут соединены друг с другом. В сетях типа “точка-точка” (*point-to-point*) могут быть соединены только два маршрутизатора. Если все маршрутизаторы установят отношения смежности со всеми остальными и будут обмениваться информацией о состоянии каналов, то объем служебных сообщений станет слишком большим. Например, пяти маршрутизаторам потребуется установить 10 отношений смежности и, соответственно, будут рассылаться 10 сообщений о состоянии каналов. Десяти маршрутизаторам потребуется 45 отношений смежности. В общем случае потребуется установить $(n \cdot n - 1) / 2$ отношений смежности.

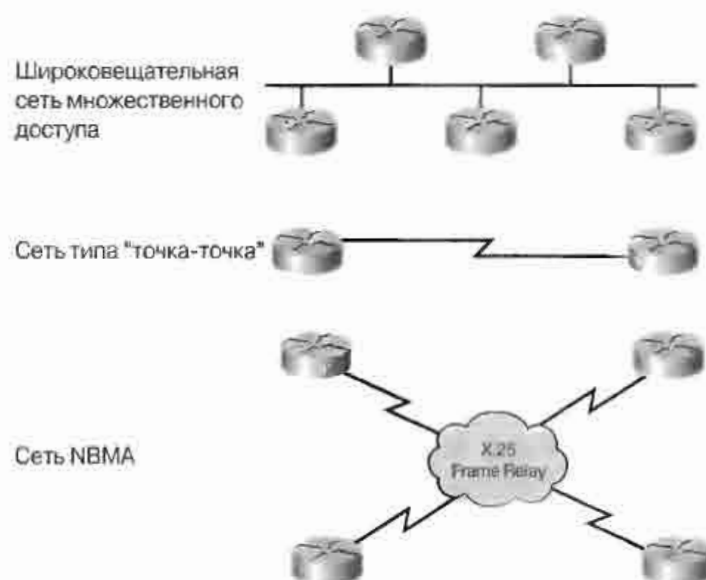


Рис. 3.8. Типы OSPF-сетей

Таблица 3.3. Типы сетей OSPF

Тип сети	Определяемые характеристики	Есть ли выбор DR-маршрутизатора?
Широковещательный множественный доступ	Ethernet, Token Ring, или FDDI	Да
Нешироковещательный множественный доступ	Frame Relay, X.25, SMDS	Да
"Точка-точка"	PPP, HDLC	Нет
"Точка-несколько точек"	Конфигурируется сетевым администратором	Нет

Возникающая проблема большого объема служебных сообщений может быть решена выбором назначенного маршрутизатора (designated router — DR).

Этот назначенный маршрутизатор становится смежным устройством для всех маршрутизаторов широковещательного сегмента. Все остальные маршрутизаторы этого сегмента посылают информацию о состоянии канала назначенному маршрутизатору. В этом случае назначенный маршрутизатор DR становится источником информации для данного сегмента. В рассмотренных выше примерах потребуется рассылка, соответственно, 5 и 10 сообщений о состоянии канала. Назначенный маршрутизатор DR рассылает информацию о состоянии каналов всем другим маршрутизаторам сегмента, используя адрес многоадресной рассылки 224.0.0.5 для всех OSPF-маршрутизаторов. Однако, несмотря на повышение эффективности работы сети, которое обеспечивается использованием назначенного маршрутизатора, в данном подходе присутствует и недостаток — назначенный маршрутизатор представляет собой точку, от которой зависит работа всего сегмента и в случае выхода его из строя весь сегмент становится неработоспособным. Поэтому выбирается также резервный назначенный маршрутизатор (backup designated router — BDR), который принимает на себя выполнение функций назначенного маршрутизатора в случае отказа последнего. На рис. 3.9 показаны маршрутизаторы DR и BDR, получающие сообщения LSA. Для того, чтобы оба маршрутизатора, DR и BDR, получали все сооб-

шения о состоянии канала, посылаемые в сегмент, используется адрес многоадресной рассылки 224.0.0.6.

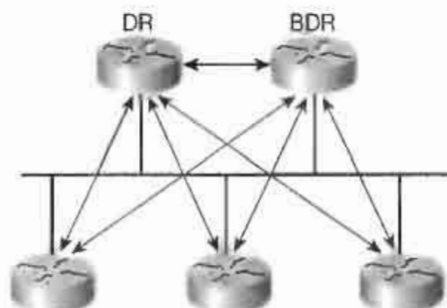


Рис. 3.9. Маршрутизаторы DR и BDR получают сообщения LSA

В сетях типа “точка-точка” существуют только два узла и поэтому маршрутизаторы DR и BDR не выбираются. Оба маршрутизатора соединения типа “точка-точка” являются друг для друга полностью смежными устройствами.

Протокол приветствия (Hello) стека протоколов OSPF

Начиная процесс OSPF-маршрутизации на интерфейсе маршрутизатор посылает пакет приветствия Hello и далее регулярно рассылает такие пакеты.

Правила обмена пакетами OSPF Hello в совокупности называются *протоколом Hello (Hello protocol)*. На 3-м уровне эталонной модели OSI пакеты Hello рассматриваются как пакеты многоадресной рассылки с адресом 224.0.0.5. Этот адрес можно рассматривать как рассылку “всем OSPF-маршрутизаторам”. OSPF-маршрутизаторы используют пакеты Hello для инициирования новых отношений смежности и для того, удостовериться в том что соседние маршрутизаторы по-прежнему функционируют. По умолчанию пакеты Hello рассылаются каждые 10-секунд по широковещательным сетям множественного доступа и по сетям соединений типа “точка-точка”. На интерфейсах, подсоединенных к сетям NBMA, пакеты Hello рассылаются каждые 30 секунд. В сетях множественного доступа согласно протоколу OSPF выбирается назначенный маршрутизатор (DR) и резервный назначенный маршрутизатор (BDR).

Хотя пакет Hello имеет небольшой размер, он содержит заголовок пакета OSPF, как показано на рис. 3.10. В поле типа пакета Hello содержит значение 1.

Версия	Тип	Длина пакета
ID маршрутизатора		
ID зоны		
Контрольная сумма	Тип аутентификации	
Данные аутентификации		

Рис. 3.10. Заголовок пакета OSPF

В пакете Hello содержится информация о том, от каких соседних устройств желательно получить согласие на установку отношений смежности и на обмен информацией о состоянии канала (рис. 3.11).

Маска подсети		
Интервал рассылки пакетов Hello	Стадии	Приоритет маршрутизатора
Интервал молчания		
Назначенный маршрутизатор		
Резервный назначенный маршрутизатор		
ID соседнего маршрутизатора		
ID соседнего маршрутизатора		
(При необходимости в конце заголовка могут быть добавлены дополнительные поля ID соседнего маршрутизатора)		

Рис. 3.11. Заголовок OSPF-пакета Hello

Операции протокола OSPF

В процессе своего функционирования OSPF-маршрутизаторы должны выполнить следующие операции.

1. Установить отношения смежности с другими маршрутизаторами.
2. Выбрать назначенный маршрутизатор (DR) и резервный назначенный маршрутизатор (BDR) (если в этом есть необходимость).
3. Проанализировать возможные маршруты.
4. Выбрать оптимальные маршруты для дальнейшего использования.
5. Поддерживать текущее состояние информации маршрутизации.

Эти операции более подробно описаны в последующих разделах.

Установка отношений смежности

На первом этапе функционирования OSPF-маршрутизатор устанавливает отношения смежности с соседними устройствами в одной IP-сети (рис. 3.12).

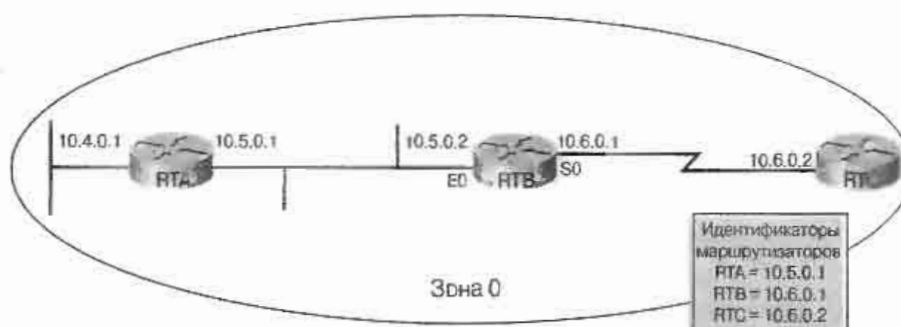


Рис. 3.12. Пример топологии OSPF-сети

Для того, чтобы установить отношения смежности с другим маршрутизатором, маршрутизатор RTB рассылает пакеты Hello, объявляя при этом свой идентификатор маршрутизатора (ID). Предполагая что RTB соответствующим образом сконфигурирован, он выполняет многоадресную рассылку пакетов Hello со своих обоих интерфейсов, S0 и E0. Оба маршрутизатора, RTA и RTC, должны получить эти пакеты Hello. После их получения оба этих маршрутизатора добавляют RTB к полю Neighbor ID своих соответствующих пакетов Hello и переходят в состояние инициализации (Init state) с маршрутизатором RTB.

Маршрутизатор RTB получает пакеты Hello от обоих своих соседних устройств и видит свой идентификатор ID (10.6.0.1) в поле Neighbor ID. Маршрутизатор RTB объявляет о своем состоянии двусторонней связи (Two-Way state) с маршрутизатором RTA и об аналогичном состоянии с маршрутизатором RTC.

На этом этапе маршрутизатор RTB определяет, с какими маршрутизаторами следует установить отношения смежности, на основе типа сетей, с которыми связаны его отдельные интерфейсы. Если сеть относится к типу “точка-точка”, то маршрутизатор становится смежным устройством с единственным партнером по каналу. Если сеть относится к сетям множественного доступа, то маршрутизатор RTB начинает процесс выбора назначенного маршрутизатора (DR) или резервного назначенного маршрутизатора (BDR), кроме того случая, когда обе эти роли уже выполняются другими маршрутизаторами (как это указано в заголовке пакета Hello).

Если необходимо выбрать маршрутизатор DR или BDR, то OSPF-маршрутизаторы выполняют действия, описанные в следующем разделе. Однако если такой выбор не является необходимым, то маршрутизаторы переходят в состояние ExStart, как это описано в разделе “Обнаружение маршрутов”.

Выбор назначенного маршрутизатора и резервного назначенного маршрутизатора

Поскольку в сетях множественного доступа возможна поддержка более чем двух маршрутизаторов, протокол OSPF выбирает маршрутизатор DR в качестве фокуса для всех обновлений состояния канала и для объявлений LSA. Роль DR-маршрутизатора является критически важной для работы сети, поэтому выбирается также резервный назначенный маршрутизатор BDR, который играет роль “теневого правительства”. Если маршрутизатор DR выходит из строя, то его функции плавно переходят к маршрутизатору BDR. На рис. 3.13 показан процесс выбора маршрутизаторов DR и BDR.



Рис. 3.13. Выбор маршрутизаторов DR и BDR в сети протокола OSPF

Как и любой другой процесс выбора, выбор маршрутизаторов DR/BDR может быть “нечестным”. В качестве “избирательных бюллетеней” выступают пакеты приветствия Hello, содержащие поле идентификатора маршрутизатора и поле приоритета. В группе смежных маршрутизаторов выборы “выигрывает” маршрутизатор с максимальным приоритетом, который и становится назначенным маршрутизатором. Маршрутизатор со вторым по величине приоритетом становится резервным назначенным маршрутизатором BDR. После того, как маршрутизаторы DR и BDR выбраны, они сохраняют свой статус до тех пор, пока какой-либо из них не выйдет из строя, даже если в сети появились новые маршрутизаторы с более высоким приоритетом. Новые маршрутизаторы извещаются о том, какие маршрутизаторы в данный момент являются назначенным и резервным назначенным, с помощью пакетов Hello.

По умолчанию все OSPF-маршрутизаторы имеют одинаковое значение приоритета, равное 1. Однако можно явным образом назначить любому OSPF-интерфейсу любое значение приоритета в интервале от 0 до 255. Присвоение маршрутизатору нулевого значения приоритета полностью исключает возможность того, что этот маршрутизатор станет маршрутизатором DR или BDR. Задание маршрутизатору значения приоритета 255 гарантирует, что он, по крайней мере, окажется в списке маршрутизаторов с одинаковым наивысшим приоритетом. В том случае, когда таких маршрутизаторов более одного, выбор маршрутизатора DR/BDR осуществляется по значению поля ID. Если два маршрутизатора имеют одинаковый приоритет, то выбирается маршрутизатор, имеющий большее значение ID. Вместо этого должно быть использовано значение приоритета, поскольку каждый интерфейс может иметь свое собственное, уникальное значение приоритета. Легко создать такую конфигурацию маршрутизатора, при которой он «выиграет» выборы на одном интерфейсе и «проиграет» на другом.

Рассмотрим процесс выбора DR-маршрутизатора на примере конкретной сети. Как показано на рис. 3.13, маршрутизаторы RTB и RTC соединены каналом типа «точка-точка» протокола PPP (Point-to-Point Protocol — PPP). В сети 10.6.0.0/16 выбор назначенного маршрутизатора не является необходимостью, поскольку в этом канале могут существовать только два маршрутизатора.

Поскольку сети 10.4.0.0/16 и 10.5.0.0/16 являются Ethernet-сетями множественного доступа, в них могут присутствовать более двух маршрутизаторов. Даже в том случае, когда к сегменту множественного доступа подсоединен только один маршрутизатор, DR-маршрутизатор должен быть выбран, поскольку потенциально к сети могут быть добавлены новые маршрутизаторы. DR-маршрутизатор должен быть выбран как в сети 10.4.0.0/16, так и в сети 10.5.0.0/16.

ПРИМЕЧАНИЕ

Маршрутизаторы DR и BDR выбираются для каждой отдельной сети. Зона протокола OSPF может включать в себя более одной IP-сети, поэтому в каждой зоне может быть (и, как правило, бывает) несколько маршрутизаторов DR и BDR.

В рассматриваемом примере маршрутизатор RTA играет двойную роль — как назначенного (DR), так и резервного (BDR) маршрутизаторов. Поскольку в сети 10.4.0.0/16 маршрутизатор RTA является единственным маршрутизатором, он сам выбирает себя в качестве DR-маршрутизатора. Сеть 10.4.0.0/16 представляет собой Ethernet-сеть множественного доступа, поэтому в ней выбирается DR-маршрутизатор, поскольку потенциально к этой сети могут быть добавлены новые маршрутизаторы. Маршрутизатор RTA является также претендентом при выборе DR и BDR в сети 10.5.0.0/16, и таким образом, становится BDR-маршрутизатором этой сети. Хотя маршрутизатор RTB имеет одинаковое с маршрутизатором RTA значение приоритета, именно он выбирается в качестве DR-маршрутизатора для сети 10.5.0.0/16; вопрос решается в его пользу, поскольку он имеет более высокое значение ID (10.5.0.2 в сравнении 10.5.0.1).

Когда процесс выбора DR и BDR заканчивается и устанавливается двустороннее соединение, маршрутизаторы оказываются готовыми к совместному использованию информации маршрутизации со смежными маршрутизаторами и строят свои базы данных состояния канала. Этот процесс обсуждается в следующем разделе.

Обнаружение маршрутов

В сети множественного доступа обмен информацией о маршрутизации происходит между одним из маршрутизаторов: DR или BDR и всеми остальными маршрутизаторами сети. В качестве маршрутизаторов DR и BDR сети 10.5.0.0 /16 маршрутизаторы RTA и RTB обмениваются информацией о состоянии канала.

В этом процессе обмена информацией также участвуют канальные партнеры по сети типа “точка-точка” или “точка — несколько точек”. Поэтому, в частности, маршрутизаторы RTB и RTC также совместно используют информацию о состоянии канала. Однако возникает вопрос о том, какой из них первым получает информацию. Ответ на этот вопрос дается на первом этапе процесса обмена информацией. Целью первого этапа ExStart является установка отношения “ведущий/ведомый” между этими двумя маршрутизаторами.

Маршрутизатор, идентификатор ID которого, объявленный в пакете Hello, имеет большее значение, становится ведущим, как показано на рис. 3.7. ведущий маршрутизатор руководит обменом информацией о состоянии канала, а ведомый маршрутизатор отвечает на запросы ведущего. Маршрутизатор RTB участвует в этом процесс вместе с маршрутизаторами RTA и RTC.

После того, как эти маршрутизаторы определили свои роли как ведомого и ведущего, они переходят в состояние Exchange. Как показано на рис. 3.7, ведущий маршрутизатор проводит ведомый через процесс обмена описаниями DBD, описывающими с определенной степенью подробности базы данных состояния канала каждого маршрутизатора. Эти описания включают в себя тип состояния канала, адрес анонсирующего маршрутизатора, оценку канала и номер последовательности. Маршрутизаторы подтверждают получение описания DBD отправляя пакет LSAck (типа 5), в котором дублируется номер последовательности DBD. Каждый маршрутизатор сравнивает информацию, полученную в описании DBD, с уже имеющейся у него информацией. Если в описании DBD анонсируется новая или более поздняя информация о состоянии канала, то маршрутизатор переходит в состояние загрузки (Loading) и посылает пакет LSR (типа 3) относительно этой позиции базы (рис. 3.7). В ответ на LSR-сообщение маршрутизатор, посылающий полную информацию о состоянии канала, отправляет пакет LSU (типа 4). Пересылаемые сообщения LSU содержат подтверждения LSA.

После окончания этапа загрузки (Loading) маршрутизаторы достигают состояния полной смежности (переходят в состояние Full). Как показано на рис. 3.7, маршрутизатор RTB в этом состоянии является смежным для маршрутизаторов RTA и RTC (рис. 3.7).

К моменту создания таблиц маршрутизации и пересылки данных смежные маршрутизаторы должны находиться в состоянии Full. На этом этапе все соседние маршрутизаторы должны иметь идентичные базы данных состояния канала.

Выбор наилучшего маршрута

Когда база данных состояния канала для маршрутизатора сформирована, он становится готовым к созданию таблицы маршрутизации и, соответственно, к пересылке данных. Как уже говорилось в настоящей главе, для определения наилучшего маршрута к пункту назначения в протоколе OSPF используется оценка, представляющая собой значение метрики (рис. 3.14). По умолчанию оценка базируется на ширине полосы пропускания перелающей среды. В целом оценка уменьшается при возрастании скорости

передачи данных по каналу. Например, Ethernet-интерфейс (E0) маршрутизатора RTB с пропускной способностью 10 Мбит/с имеет меньшую оценку чем последовательный T1-интерфейс (S0), поскольку скорость передачи 10 Мбит/с больше, чем 1.544 Мбит/с. Для вычисления маршрута к пункту назначения с наименьшей оценкой маршрутизатор RTB использует алгоритм SPF. Упрощенно говоря, алгоритм SPF складывает оценки отдельных участков маршрута от локального маршрутизатора (называемого корневым) до цели пункта назначения. Если к пункту назначения существует несколько маршрутов, то предпочтение отдается маршруту с наименьшей оценкой. Это процесс показан на рис. 3.14. По умолчанию протокол OSPF хранит в таблице маршрутизации до четырех позиций маршрутов с равными оценками для балансирования нагрузки.



Рис. 3.14. Выбор протоколом OSPF наилучшего маршрута

Иногда каналы, такие как последовательные линии, начинают быстро колебаться между рабочим и нерабочим состоянием (такое явление называется флэппингом).

Если флэппинг канала вызывает генерирование сообщений LSU, то маршрутизаторы, получающие такие обновления маршрутов, должны вновь выполнять алгоритм SPF для вычисления новых маршрутов. Продолжительный флэппинг может серьезно снизить производительность работы сети. Повторные вычисления, выполняемые алгоритмом SPF могут вызвать истощение мощности центрального процессора; более того, постоянные обновления могут препятствовать сходимости баз данных состояния канала. Для борьбы с этим явлением в IOS Cisco используется таймер удержания алгоритма SPF. После получения сообщения LSU таймер удержания определяет, в течение какого времени маршрутизатор будет ожидать перед выполнением алгоритма SPF. Команда **timers spf** позволяет задать время удержания таймера, которое по умолчанию равно 10 секундам.

После того, как маршрутизатор RTB с помощью алгоритма SPF выбрал наилучшие маршруты, он переходит в финальную стадию функционирования протокола OSPF.

Поддержка информации о маршрутах

После того, как OSPF-маршрутизатор создал маршруты в своей таблице маршрутизации, он должен постоянно поддерживать точную информацию о маршрутах. В случае изменения состояния канала OSPF-маршрутизаторы для уведомления других маршрутизаторов сети о произошедшем изменении используют процесс лавинной рассылки. Критические интервалы протокола Hello представляют собой простой механизм для извещения других маршрутизаторов о том, что партнер по каналу вышел из строя. Если в течение промежутка времени, превышающего критический интервал (обычно равный 40 секундам), маршрутизатор RTB не получает сообщений от маршрутизатора RTA, то он объявляет о неработоспособности канала, связывающего его с маршрутизатором RTA. В этом случае маршрутизатор RTB посылает сообщение LSU, содержащее новую информацию о состоянии канала, включающую в себя:

- в сетях типа "точка-точка" объявляется о том, что маршрутизаторы DR и BDR отсутствуют;
- новая информация о состоянии канала посылается на адрес многоадресной рассылки 224.0.0.5;
- все OSPF-маршрутизаторы прослушивают информацию, рассылаемую с этого адреса;
- в сети множественного доступа маршрутизаторы DR и BDR продолжают существовать и поддерживают отношения смежности со всеми остальными OSPF-маршрутизаторами сети;
- если маршрутизатору DR или BDR требуется послать сообщение об изменении состояния канала, то он рассылает это обновление всем OSPF-маршрутизаторам на адрес 224.0.0.5;
- однако другие маршрутизаторы сети множественного доступа являются смежными только для маршрутизаторов DR и BDR и могут посылать сообщения LSU только им;
- по этой причине маршрутизаторы DR и BDR имеют свой собственный адрес многоадресной рассылки — 224.0.0.6;
- маршрутизаторы, которые не являются резервным или назначенным маршрутизатором (DR/BDR), посылают свои LSU-сообщения по адресу 224.0.0.6 или всем маршрутизаторам DR/BDR.

На рис. 3.15 маршрутизатор обнаруживает изменение состояния канала и рассылает методом многоадресной рассылки пакет LSU, содержащий информацию об изменении состояния канала, по адресу 224.0.0.6, который является адресом всех OSPF-маршрутизаторов, которые являются назначенными (DR) или резервными (BDR).



Рис. 3.15. Информация о состоянии канала протокола OSPF

Когда маршрутизатор DR получает сообщение LSU, направленное по адресу 224.0.0.6, и подтверждает это получение, он выполняет лавинную рассылку этого LSU-сообщения всем OSPF-маршрутизаторам сети по адресу 224.0.0.5. Каждый маршрутизатор подтверждает получение сообщения LSU, отправляя, в свою очередь, сообщение LSAck.

Если OSPF-маршрутизатор подсоединен к другой сети, то он выполняет лавинную рассылку сообщения LSU другим сетям путем пересылки этого сообщения назначенно-

му маршрутизатору DR сети множественного доступа или смежному маршрутизатору сети типа “точка-точка”. Маршрутизатор DR, в свою очередь, выполняет многоадресатную рассылку LSU-сообщения всем остальным OSPF-маршрутизаторам данной сети.

После получения сообщения LSU, содержащего новую информацию, OSPF-маршрутизатор обновляет свою базу данных состояния канала. После этого он выполняет алгоритм SPF с использованием этой новой информации для обновления своей таблицы маршрутизации. После того, как истекает время таймера удержания, маршрутизатор переключается на эту новую таблицу маршрутизации.

Если на маршрутизаторе Cisco уже существует какой-либо маршрут к определенному пункту назначения, то этот старый маршрут используется пока алгоритм SPF вычисляет новую информацию. Если алгоритм SPF вычисляет новый маршрут, то он не будет использоваться маршрутизатором до окончания выполнения алгоритма SPF.

Следует отметить, что даже в случае отсутствия изменений в состоянии канала информация о маршрутах протокола OSPF периодически обновляется. Каждая позиция сообщения LSA имеет свой собственный таймер устаревания информации. Для этого таймера время срабатывания по умолчанию равно 30 минутам. В случае устаревания информации в некоторой позиции LSA маршрутизатор, инициировавший эту позицию, посылает сообщение LSU в сеть для проверки того, что этот канал остается активным.

Конфигурирование протокола OSPF для одной зоны

Для того, чтобы сконфигурировать на маршрутизаторе протокол OSPF, необходимо включить этот протокол и сконфигурировать сетевые адреса маршрутизатора и задать информацию о зоне, как показано на рис. 3.16, выполнив следующие действия:

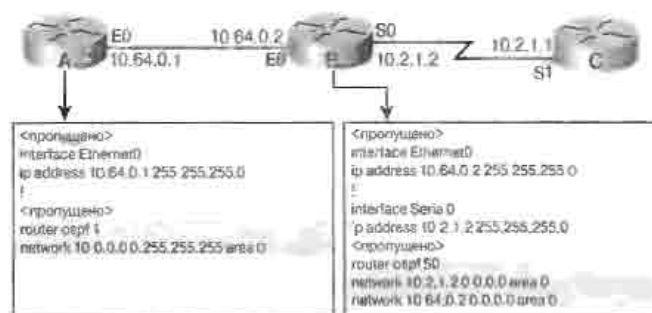


Рис. 3.16. Базовое конфигурирование протокола OSPF

Этап 1. Включить на маршрутизаторе использование протокола OSPF, используя команду:

```
router(config)# router ospf process-id
```

Идентификатор ID процесса (аргумент *process-id*) является номером процесса на локальном маршрутизаторе. Этот идентификатор ID используется для идентификации одного процесса среди нескольких процессов, работающих на одном и том же маршрутизаторе. Это номер может быть любым значением из диапазона от 1 до 65535. Нумерация процессов не обязательно должна начинаться с 1. Большинство сетевых администраторов используют один и тот же ID процесса во всей автономной системе

AS. На одном и том же маршрутизаторе могут выполняться несколько OSPF-процессов, однако это не рекомендуется, поскольку в этом случае создается несколько экземпляров баз данных, которые увеличивают служебную нагрузку на маршрутизатор.

Этап 2. Идентифицировать IP-сети на маршрутизаторе, используя команду

```
router(config-router)# network address wildcard-mask area area-id
```

Для каждой сети необходимо задать зону, к которой принадлежит эта сеть. Значение *address* может быть адресом сети, подсети или адресом интерфейса.

О том, как следует интерпретировать адрес, маршрутизатор узнает путем сравнения его с маской шаблона. Эта маска необходима потому что протокол OSPF, в отличие от протоколов RIPv1 и IGRP поддерживает маршрутизацию CIDR и VLSM. Аргумент *area-id* является обязательным даже в том случае, когда протокол OSPF конфигурируется лишь в одной отдельной зоне. Вновь следует отметить, что к одной зоне могут принадлежать несколько IP-сетей. Проектирование и реализация больших сетей OSPF начинается с конфигурирования маршрутизации OSPF в отдельной зоне. Протокол OSPF конфигурируется аналогично другим протоколам маршрутизации. Некоторые отличия состоят в том, как отдельные сети анонсируются и включаются в директиву **network**. Это вызвано тем, что протокол OSPF является протоколом состояния канала, а не дистанционно-векторным (как, например, протоколы RIPv1 и IGRP).

Для успешного функционирования протоколу OSPF требуются *идентификатор процесса* (*process identifier* — *process ID*) и *идентификатор маршрутизатора* (*router identifier* (*router ID*)). Идентификатор маршрутизатора берется с активного интерфейса. Если этот интерфейс выходит из строя, то данный процесс OSPF продолжаться не может. Для обеспечения устойчивой работы протокола OSPF в качестве идентификатора маршрутизатора конфигурируется адрес *петлевого интерфейса* (*loopback address*). Дополнительно в сетях множественного доступа выбирается назначенный маршрутизатор (*designated router* — DR). При распространении информации о состоянии канала этот маршрутизатор выступает от имени всех остальных маршрутизаторов. Возможна ситуация, когда в качестве назначенного маршрутизатора требуется выбрать некоторый заранее указанный маршрутизатор. В этом случае данному маршрутизатору присваивается наивысший приоритет.

Конфигурирование адреса петлевого интерфейса

Когда начинается процесс функционирования протокола OSPF, операционная система IOS Cisco использует наибольший локальный IP-адрес в качестве идентификатора своего OSPF-маршрутизатора. Если конфигурируется адрес петлевого интерфейса, то независимо от его значения используется этот адрес. IP-адрес петлевого интерфейса может быть назначен с помощью следующих команд:

```
router(config)#interface loopback number  
router(config-if)#ip address ip-address subnet-mask
```

ID маршрутизатора, полученный с петлевого интерфейса, обеспечивает устойчивость сети, поскольку этот интерфейс на его функционирование не влияют возможные

сбои в работе канала. Адрес петлевого интерфейса должен быть сконфигурирован до того, как OSPF-процесс начнет искать интерфейс, который заменит интерфейс с наибольшим IP-адресом. Рекомендуется использовать адрес петлевого интерфейса на всех ключевых маршрутизаторах OSPF-сети. Для того, чтобы избежать проблем с маршрутизацией, рекомендуется при конфигурировании IP-адреса петлевого интерфейса использовать 32-битовую маску подсети, как показано в примере 3.1.

Пример 3.1. Конфигурирование петлевого интерфейса с использованием маски узла

```
router(config)#interface loopback0
router(config-if)#ip address 192.168.1.1 255.255.255.255
```

32-битовая маска иногда называется маской узла, поскольку она относится только к одному узлу, а не к сети или подсети.

Изменение приоритета OSPF-маршрутизатора

На выбор маршрутизаторов DR/BDR пользователь может повлиять путем конфигурирования на маршрутизаторе значения приоритета, отличного от значения по умолчанию (равного 1). Присвоение маршрутизатору значения приоритета равного 0 гарантирует, что этот маршрутизатор не будет выбран в качестве назначенного маршрутизатора (DR) или резервного (BDR). Каждый OSPF-интерфейс может иметь свое, отличное от других значение приоритета. Значение приоритета (число в интервале от 0 до 255) может быть сконфигурировано с помощью команды **priority**, имеющей следующий синтаксис:

```
router(config-if)#ip ospf priority number
```

Для задания интерфейсу E0 приоритета, равного 0 (с тем, чтобы он не был выбран в качестве маршрутизатора DR/BDR) следует использовать команды, приведенные в примере 3.2.

Пример 3.2. Задание маршрутизатору приоритета равного нулю

```
RTB(config)#interface e0
RTB(config-if)#ip ospf priority 0
```

Для того, чтобы значение приоритета было учтено в процессе выбора маршрутизатора DR/BDR, оно должно быть установлено до того как это выбор будет производиться. Значение приоритета и другая существенная информация могут быть выведены с помощью команды **show ip ospf**, как показано в примере 3.3. Выводимая в данном примере информация показывает, какие маршрутизаторы были выбраны в качестве DR и BDR, тип сети (в данном случае широковещательная сеть множественного доступа), оценку канала (10) и интервалы таймера для данного конкретного интерфейса. В качестве таких интервалов выступают интервалы таймеров Hello (10), Dead (40), Wait (40) и Retransmit (5). Таймеры протокола OSPF описаны в следующем разделе.

Чем выше приоритет маршрутизатора, тем более вероятно, что он будет выбран в качестве назначенного (DR). Изменить приоритет интерфейса, участвующего в работе протокола OSPF, можно с помощью команды **ip ospf priority**.

В примере 3.3 по команде **show ip ospf interface** выводится значение приоритета интерфейса, а также другая существенная информация.

ПРИМЕЧАНИЕ

Для предотвращения распространения недействительных маршрутов, протокол OSPF всегда объявляет адреса петлевых интерфейсов с 32-битовой маской в качестве маршрутов узлов.

Пример 3.3. Использование команды `show ip ospf interface`

```
Routers#show ip ospf interface e0
Ethernet0 is up, line protocol is up
Internet Address 10.5.0.2, Area 0
Process ID 1, Router ID 10.6.0.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State Dr, Priority 1
Designated Router (ID) 10.6.0.2, Interface address 10.6.0.1
Backup Designated router (ID) 10.5.0.1, Interface address 10.5.0.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 2, Adjacent neighbor count is 2
Adjacent with neighbor 10.5.0.1 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```



Лабораторная работа: конфигурирование процесса маршрутизации протокола OSPF

В этой лабораторной работе требуется задать схему IP-адресации для OSPF-зоны, использующей два маршрутизатора. После этого требуется с конфигурировать и протестировать OSPF-маршрутизацию.



Лабораторная работа: конфигурирование протокола OSPF с адресами петлевых интерфейсов

В этой лабораторной работе можно наблюдать процесс выбора назначенного и резервного маршрутизаторов (DR и BDR) в сети множественного доступа. Для обеспечения устойчивости сети можно сконфигурировать адреса петлевых интерфейсов и назначить каждому OSPF-интерфейсу некоторое значение приоритета с тем чтобы принудительно выбрать какой-либо маршрутизатор в качестве назначенного (DR).

Изменение метрики, используемой протоколом OSPF для присвоения оценки каналу

Протокол OSPF использует оценку в качестве метрики при определении наилучшего маршрута. Операционная система IOS Cisco автоматически вычисляет оценку на основе ширины полосы пропускания интерфейса. Для вычисления оценки используется следующая формула:

$$10^8 / (\text{ширина полосы пропускания})$$

Для того, чтобы протокол OSPF правильно вычислял характеристики маршрутов, необходимо, чтобы все интерфейсы, подсоединенные к какому-либо каналу, договорились о его оценке. Эта оценка может быть изменена для того, чтобы оказать влияние на результат вычисления протоколом OSPF его оценки. Наиболее типичной ситуацией, в которой требуется изменять оценку, является использование маршрутизаторов разных производителей. Это связано с тем, что оценки канала, сделанные различными устройствами, могут оказаться отличными друг от друга.

Каналы имеют оценки по умолчанию, которые присваиваются на основе технологии, используемой для реализации данного канала. Сетевой администратор может изменить метрику оценки канала, используемую протоколом OSPF. В табл. 3.4 приведены оценки каналов, принимаемые по умолчанию.

Таблица 3.4. Стандартные оценки протокола OSPF

Передающая среда	Оценка
Последовательный канал 56 Кбит/с	1785
T1 (Последовательный канал 1,544 Мбит/с)	64
E1 (Последовательный канал 2,048 Мбит/с)	48
Сеть Ethernet 10 Мбит/с	10
Сеть Token Ring 16 Мбит/с	6
100 Mbps Fast Ethernet, FDDI	1

Задание оценки каналу осуществляется с использованием следующей команды конфигурирования интерфейса:

```
Router(config-if)#ip ospf cost number
```

Значение параметра *number* может находиться в интервале от 1 до 65535. Альтернативным способом повлиять на оценку канала протоколом OSPF является задание на интерфейсе значения полосы пропускания, как показано на рис. 3.4. Чем меньше число, тем лучшим считается канал.

Пример 3.4. Задание ширины полосы пропускания в протоколе OSPF

```
Router(config)# interface serial 0/0
Router(config-if)# bandwidth 64
```

Для данного последовательного интерфейса стандартным значением ширины полосы пропускания по является 1544.



Лабораторная работа: изменение метрик, используемой для вычисления оценки канала в протоколе OSPF

В данной лабораторной работе требуется сконфигурировать и протестировать маршрутизацию по протоколу OSPF. На данном интерфейсе можно изменить метрику, используемую протоколом OSPF, для вычисления оценки.

Конфигурирование аутентификации в протоколе OSPF

Уровень безопасности в сети повышается, если известно, что информация о маршрутизации поступила из конкретного источника. Протокол OSPF позволяет маршрутизаторам выполнять взаимную аутентификацию. По умолчанию маршрутизатор полагается на то, что информация о маршрутах поступает от того маршрутизатора, который должен ее отправлять. Маршрутизатор также полагается на то, что в процессе передачи эта информация не была искажена. Для того, чтобы гарантировать это, на маршрутизаторах одной зоны может быть сконфигурирована взаимная аутентификация.

Аутентификация представляет собой другой тип конфигурирования отдельных интерфейсов. Каждому OSPF-интерфейсу маршрутизатора может быть задан отличный от других ключ аутентификации, который выполняет функции пароля для маршрутизаторов OSPF одной и той же зоны. При конфигурировании OSPF-аутентификации используется команда со следующим синтаксисом:

```
router(config-if)#ip ospf authentication-key password
```

После того, как сконфигурирован пароль, в зоне можно включить функцию аутентификации с помощью команды, имеющей следующий синтаксис: (эта команда должна быть выполнена на всех маршрутизаторах, участвующих в аутентификации):

```
router(config-router)#area number authentication [message-digest]
```

Хотя ключевое слово **message-digest** не является обязательным, рекомендуется всегда использовать его в данной команде. По умолчанию пароли аутентификации пересылаются открытым текстом. Поэтому *анализатор пакетов (packet sniffer)* легко может перехватить пакет OSPF и расшифровать пароль. Однако при использовании ключевого слова **message-digest** вместо самого пароля пересылается дайджест сообщения, или хеш пароля. Если у получателя сконфигурирован соответствующий ключ аутентификации, то потенциальный взломщик не сможет понять смысл этого дайджеста.

Если выбрана аутентификация с использованием дайджеста сообщения, то ключ аутентификации не используется. Вместо этого на интерфейсе OSPF-маршрутизатора должен быть сконфигурирован ключ дайджеста сообщения. Эта команда имеет следующий синтаксис:

```
router(config-if)#ip ospf message-digest-key key-id md5  
[ encryption-type] password
```

Аутентификация MD5 создает дайджест сообщения. Он представляет собой кодированные данные, созданные на базе пароля и содержания пакета. Маршрутизатор-получатель использует для восстановления дайджеста совместно используемый пароль и этот пакет. Если дайджесты совпадают, то маршрутизатор считает, что источнику пакета можно доверять и содержимое пакета не было искажено или подделано в процессе передачи.

Тип аутентификации указывает вид аутентификации, если она используется. В случае аутентификации использованием дайджеста сообщения поле данных аутентификации содержит идентификатор ключа и длину приложенного к пакету дайджеста. Дайджест сообщения можно сравнить с водяным знаком, который не может быть подделан.



Лабораторная работа: конфигурирование аутентификации протокола OSPF

В этой лабораторной работе рассматривается повышение уровня безопасности в сети протокола OSPF путем конфигурирования аутентификации маршрутизаторов в зоне протокола OSPF.

Конфигурирование таймеров протокола OSPF

В некоторых случаях становится необходимым ускорение оповещения маршрутизаторов сети о сбоях в работе каналов. В протоколе OSPF для этой цели используются таймеры.

Для того, чтобы OSPF-маршрутизаторы могли обмениваться информацией, они должны иметь одинаковые интервалы рассылки сообщений Hello и критические интервалы. По умолчанию критический интервал имеет в четыре раза большее значение, чем интервал рассылки сообщений Hello. Это означает, что маршрутизатор имеет возможность четыре раза послать сообщение Hello до того, как он будет объявлен неработоспособным. В широковещательных сетях OSPF интервал сообщений Hello по умолчанию равен 10 секундам, а интервал критических сообщений по умолчанию равен 40 секундам. В нешироковещательных сетях OSPF интервал сообщений Hello по умолчанию равен 30 секундам, а интервал критических сообщений по умолчанию равен 120 секундам. Эти стандартные значения обеспечивают эффективное функционирование протокола OSPF, поэтому их не рекомендуется изменять. Сетевой администратор может изменить эти значения, однако для изменения значений таймеров необходимы достаточные основания полагать, что такое изменение повысит эффективность работы сети. При конфигурировании таймеров необходимо следить за тем, чтобы у всех маршрутизаторов эти значения совпадали. При конфигурировании на интерфейсе интервалов Hello и критического используются команды со следующим синтаксисом:

```
Router(config-if)# ip ospf hello-interval seconds
Router(config-if)# ip ospf dead-interval seconds
```



Лабораторная работа: конфигурирование таймеров протокола OSPF

В этой лабораторной работе требуется ускорить оповещение маршрутизаторов сети о сбоях в работе каналов.

Конфигурирование протокола OSPF в сетях NBMA

Другим типом OSPF-сетей являются нешироковещательные сети множественного доступа (nonbroadcast multiaccess — NBMA), которые могут включать в себя более двух узлов и пытающиеся выбрать назначенный (DR) и резервный (BDR) маршрутизаторы. Типичными сетями NBMA являются сети Frame Relay, X.25 и коммутируемая мультимегабитная служба данных (Switched Multimegabit Data Service — SMDS). Сети NBMA подчиняются условиям 2-го уровня эталонной модели OSI, выполнение которых предотвращает рассылку широковещательных и многоадресных сообщений. На рис. 3.17 показаны различные типы сетей, использующих протокол OSPF.

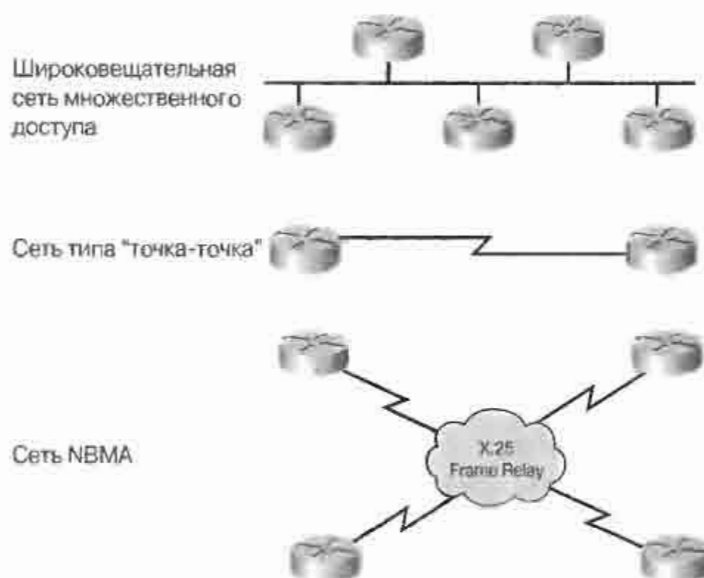


Рис. 3.17. Типы OSPF-сетей

В сетях NBMA при использовании протокола OSPF могут возникнуть проблемы, в частности, при обмене пакетами многоадресной рассылки Hello. В примере, показанном на рис. 3.18, маршрутизаторы RTA, RTB и RTC принадлежат к одной и той же подсети протокола IP и пытаются выбрать маршрутизаторы DR и BDR.

Однако эти маршрутизаторы не могут провести реальный выбор, если они не могут получать пакеты Hello многоадресной рассылки от всех остальных маршрутизаторов сети. При отсутствии административного вмешательства такой выбор может произойти довольно странным образом. В том, что происходит с маршрутизатором RTA, маршрутизатор RTC участия не принимает. Аналогичным образом, маршрутизатор RTC проходит процесс выбора не зная о маршрутизаторе RTA. Такой неосознанный выбор может привести к возникновению проблем, если центральный маршрутизатор RTB не будет выбран назначенным маршрутизатором (DR).

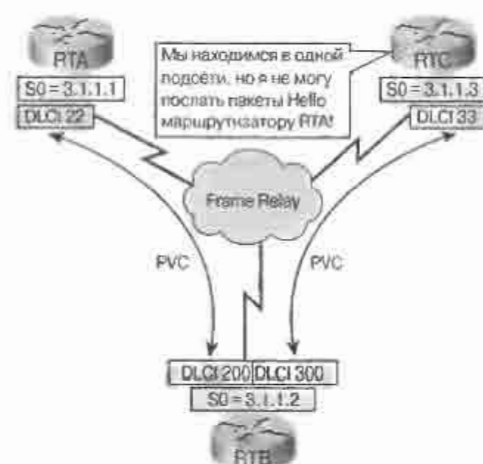


Рис. 3.18. Статус соседнего OSPF-устройства в сети NBMA

Операционная система IOS Cisco предлагает несколько способов конфигурирования протокола OSPF, позволяющих преодолеть ограничения сетей NBMA, включая использование OSPF-команд **neighbor**, подынтерфейсов типа “точка-точка” и конфигурации типа “точка-несколько точек”. Какие из этих решений могут быть использованы в сети NBMA, зависит от ее топологии. Перед выбором стратегии конфигурирования сети Frame Relay (или унаследованной сети X.25) необходимо уверенное понимание различных типов топологий сетей NBMA. В общем плане возможны два типа физических топологий в сетях Frame Relay:

- Полносвязная топология;
- Частично-связная топология (включающая в себя древовидную звездообразную топологию).

На рис. 3.19 показаны топологии протокола Frame Relay.

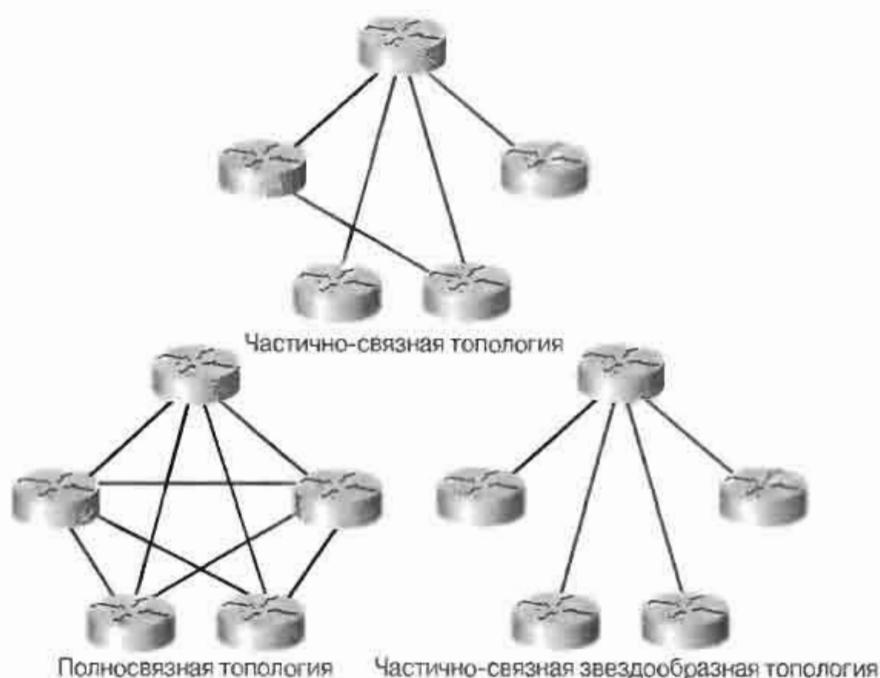


Рис. 3.19. Топологии сетей Frame Relay, использующих протокол OSPF

В последующих разделах описано конфигурирование протокола OSPF как в полностью связанных, так и в частично-связных сетях Frame Relay.

Полносвязные сети Frame Relay

Различные организации создают сети Frame Relay в первую очередь потому, что в таких сетях возможна поддержка более одного логического соединения на одном интерфейсе, что делает его удобным и гибким решением для каналов распределенных сетей WAN. Полносвязная топология позволяет воспользоваться способностью протокола Frame Relay поддерживать несколько постоянных виртуальных каналов (permanent virtual circuit — PVC) на одном последовательном интерфейсе. В полностью связанной топологии каждый маршрутизатор имеет каналы PVC со всеми остальными маршрутизаторами сети, как показано на рис. 3.20.

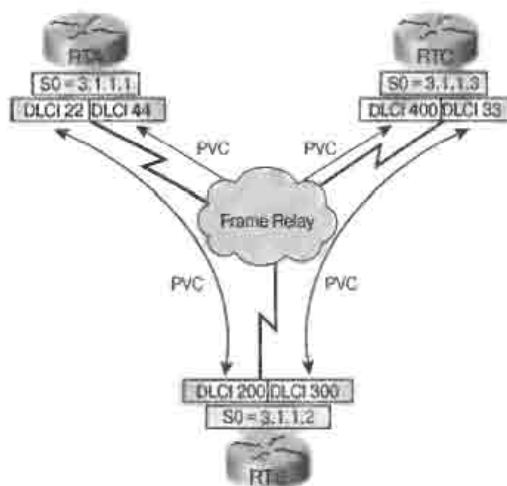


Рис. 3.20. OSPF-сеть Frame Relay с полносвязной топологией

Для того, чтобы протокол OSPF успешно функционировал в полносвязной топологии множественного доступа, не поддерживающей широковещание, необходимо вручную ввести на каждом маршрутизаторе адреса всех соседних OSPF-устройств по отдельности.

Команда **neighbor** протокола OSPF позволяет сообщить маршрутизатору IP-адреса всех его соседей, что позволит ему обмениваться с ними информацией о маршрутах без использования многоадресной рассылки. В примере 3.5 показано применение команды **neighbor**.

Пример 3.5. Использование команды **neighbor** протокола OSPF

```
RTA(config)#router ospf 1
RTA(config-router)#network 3.1.1.0 0.0.0.255 area 0
RTA(config-router)#neighbor 3.1.1.2
RTA(config-router)#neighbor 3.1.1.3
```

Явное указание адресов соседних устройств не является единственно возможным способом организовать работу протокола OSPF в такой среде. В следующем разделе описывается возможность использования подынтерфейсов, которая устраняет необходимость в использовании команды **neighbor**.

Конфигурирование подынтерфейсов для создания сетей типа "точка-точка"

Функция использования подынтерфейса операционной системы IOS Cisco может быть использована для разделения сети множественного доступа на несколько сетей типа "точка-точка".

На рис. 3.21 с каждым каналом PVC связывается отдельная IP-подсеть.

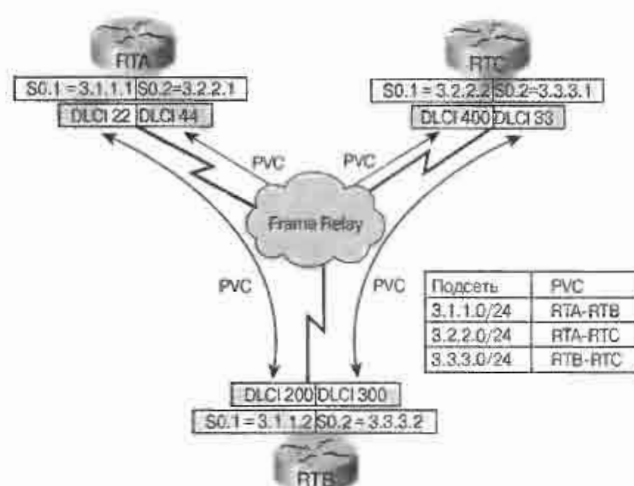


Рис. 3.21. Подынтерфейсы в полносвязной топологии OSPF-сети

Протокол OSPF автоматически распознает такую конфигурацию как сеть типа "точка-точка", а не сеть NBMA, даже в том случае, когда на интерфейсах сконфигурирован протокол Frame Relay. Следует вспомнить, что в OSPF-сетях типа "точка-точка" назначенный маршрутизатор DR не выбирается. Вместо этого маршрутизатор протокола Frame Relay для получения адреса партнера по каналу использует протокол обратного преобразования адресов (Reverse Address Resolution Protocol — RARP); это позволяет ему обмениваться информацией маршрутизации с другими маршрутизаторами. Полносвязная топология обладает многочисленными преимуществами, включая максимальную устойчивость к сбоям на отдельных каналах. К сожалению реализация полносвязной топологии может оказаться весьма дорогостоящей, поскольку каждый канал PVC должен арендоваться у провайдера. Для поддержки полносвязной топологии, включающей в себя 10 маршрутизаторов, потребовалось бы 45 каналов PVC. При использовании подынтерфейсов для создания сети типа "точка-точка" пришлось бы выделять 45 IP-подсетей и управлять ими, что повлекло бы за собой дополнительные расходы.

Сети Frame Relay с частично-связной топологией

Поскольку полносвязная топология является весьма дорогостоящей, многие организации вместо нее используют частично-связную топологию. Под такой топологией понимается такая конфигурация, в которой по крайней мере один маршрутизатор поддерживает соединения со всеми остальными маршрутизаторами сети, однако таким свойством обладают не все маршрутизаторы сети, т.е. топология не является полносвязной. Наиболее эффективной в финансовом отношении является древовидная звездообразная (hub-and-spoke) топология, в которой один маршрутизатор, выполняющий функции концентратора (hub) соединен со всеми остальными маршрутизаторами сети (spoke routers). Использование звездообразной топологии является эффективным в финансовом отношении решением в распределенных сетях WAN, однако оно имеет серьезный недостаток: выход из строя всего лишь одного устройства (маршрутизатора-концентратора) приводит к неработоспособности всей сети. Как правило, организации используют сети Frame Relay по причине их невысокой стоимости, а не потому, что они обладают высокой отказоустойчиво-

стью. Поскольку выделенные линии (в отличие от каналов Frame Relay) обычно используются для передачи критически важных данных, в таких ситуациях является целесообразным использование экономичной топологии, такой как звездообразная.

К сожалению, команда **neighbor**, успешно решавшая задачу в полносвязной топологии, не может этого сделать в древовидной звездообразной (hub-and-spoke) топологии. Маршрутизатор-концентратор на рис. 3.22 связан со всеми остальными маршрутизаторами и может посылать им информацию о маршрутах, используя команду **neighbor**, однако они могут посылать пакеты Hello только маршрутизатору-концентратору, но не друг другу.

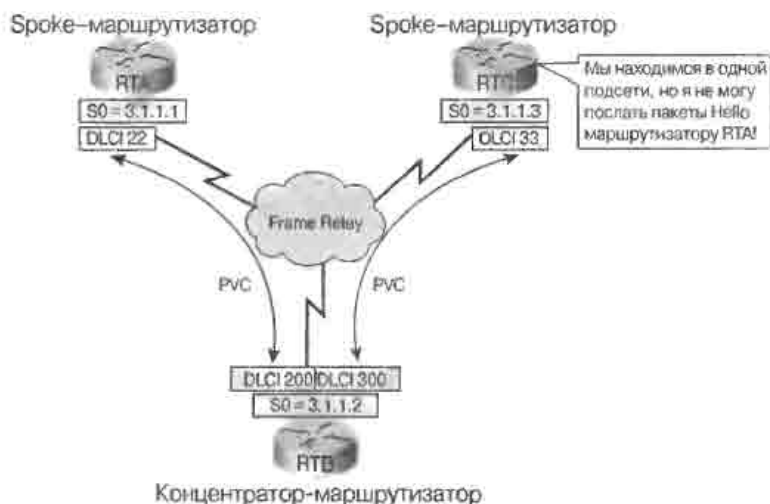


Рис 3.22. Сеть протокола OSPF с звездообразной топологией

Выбор маршрутизаторов DR/BDR, произойдет, однако лишь маршрутизатор-концентратор будет обладать информацией обо всех кандидатах. Поскольку для правильного функционирования такой OSPF-сети необходимо, чтобы в качестве назначенного маршрутизатора выступал маршрутизатор-концентратор, для всех остальных маршрутизаторов сети следует задать приоритет, равный нулю. Следует напомнить, что назначение маршрутизатору приоритета, равного нулю, исключает возможность выбора его в качестве назначенного или резервного. При использовании второго подхода к решению проблем такой топологии вопрос выбора маршрутизаторов DR/BDR вообще не ставится, а вместо этого сеть разбивается на отдельные соединения типа "точка-точка". В сетях типа "точка-точка", как показано на рис. 3.23, назначенный и резервный маршрутизаторы не выбираются. Хотя в таких сетях конфигурирование протокола OSPF осуществляется просто, использование сетей "точка-точка" со звездообразной топологией обладает существенными недостатками. В этом случае для каждого канала необходимо выделить отдельную подсеть, что приводит к усложнению WAN-адресации и вызывает трудности в управлении сетью. Вопрос о WAN-адресации можно обойти путем использования нумерованного протокола IP, однако во многих WAN-сетях применяются политики, не позволяющие использовать эту функцию. Есть ли реальная альтернатива конфигурации типа "точка-точка"? К счастью, операционная система IOS Cisco предлагает относительно новую альтернативу. Как показано в следующем разделе, физическая звездообразная топология может быть вручную переконфигурирована в сеть типа "точка-несколько точек".

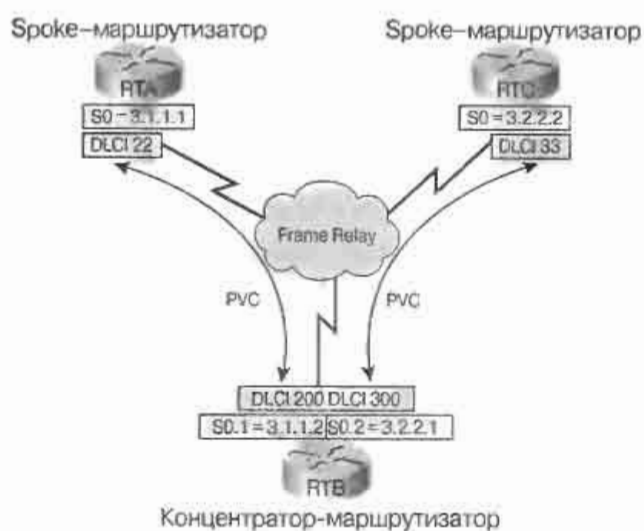


Рис. 3.23. Звездообразная топология OSPF-сети типа "точка-точка"

OSPF-сеть типа "точка-несколько точек"

В сети типа "точка-несколько точек" маршрутизатор-концентратор непосредственно соединен со всеми остальными маршрутизаторами, однако адреса всех WAN-интерфейсов принадлежат к одной и той же подсети, как показано на рис. 3.24.

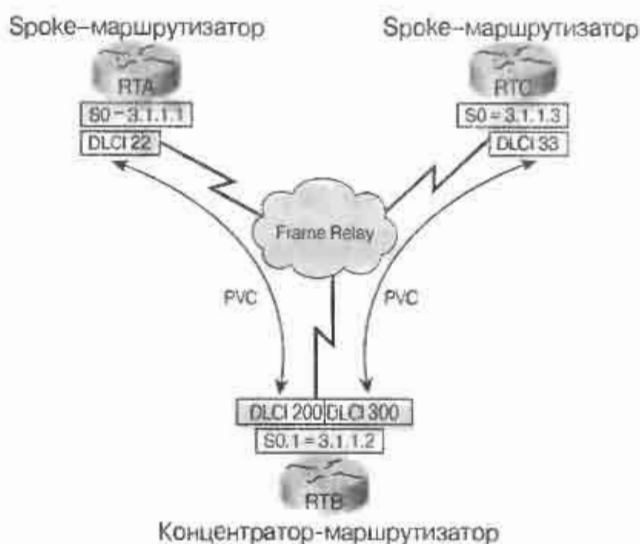


Рис. 3.24. Звездообразная топология OSPF-сети типа "точка-несколько точек"

Эта логическая топология рассматривалась ранее в настоящей главе, однако там отмечалось, что в сетях NBMA протокол OSPF не может полноценно выполнять свои функции. Однако путем ручного изменения типа сети на тип "точка-несколько точек" можно добиться корректного функционирования протокола OSPF и в сети с такой топологией. Обмен информацией о маршрутах между маршрутизаторами RTA и RTC при этом будет происходить через маршрутизатор RTB, который соединен виртуальными каналами с обоими маршрутизаторами.

Отметим, что при использовании этой функции в конфигурировании соседних устройств нет необходимости (они будут обнаружены протоколом обратного ARP (Inverse ARP)).

Сети типа “точка-несколько точек” обладают следующими свойствами:

- Между соседними маршрутизаторами устанавливаются отношения смежности;
- В таких сетях отсутствуют назначенные и резервные маршрутизаторы;
- Для сетей такого типа не инициируются сообщения LSA;
- Для интерфейсов типа “точка-несколько точек” и для соседних устройств в сетях такого типа приоритеты маршрутизаторов не задаются;
- При инициировании LSA для маршрутизатора интерфейс типа “точка-несколько точек” рассматривается всеми смежными соседними устройствами как набор каналов типа “точка-точка” ко всем смежным соседним устройствам данного интерфейса, наряду с тупиковым каналом (stub link), анонсирующим IP-адрес данного интерфейса с оценкой, равной нулю.

При лавинной рассылке с нешироковещательного интерфейса пакеты LSU и LSAck должны дублироваться для отправки их всем соседним устройствам данного интерфейса.

При конфигурировании соединения типа “точка-несколько точек” необходимо вручную переопределить установленный протоколом OSPF тип сети с помощью команды:

```
router(config-if)#ip ospf network point-to-multipoint
```

Необходимо также сконфигурировать интерфейс с помощью команды **frame-relay map ip**, имеющей следующий синтаксис:

```
router(config-if)#frame-relay map ip address dlcI broadcast
```

Ключевое слово **broadcast** позволяет маршрутизатору рассылать широковещательные сообщения через указанный идентификатор DLCI соседнему устройству (устройствам).

В сети с конфигурацией типа “точка-несколько точек” протокол OSPF рассматривает все соединения между маршрутизаторами в нешироковещательной сети, таким образом, как если бы они были каналами типа “точка-точка”. В таких сетях назначенный маршрутизатор не выбирается. Соседние устройства могут быть определены с помощью команды **neighbor** или динамически обнаружены с использованием протокола Inverse ARP.

В конечном итоге можно сказать, что использование протокола OSPF в сетях с соединениями типа “точка-несколько точек” обеспечивает эффективное функционирование сети, не вызывая проблем, связанных с администрированием сети.

Распространение в сети маршрута по умолчанию

Для получения доступа к сетям, которые не присутствуют в таблице маршрутизации, на граничном маршрутизаторе должен быть задан маршрут по умолчанию. Эта информация о маршруте по умолчанию должна быть распространена между всеми маршрутизаторами зоны протокола OSPF.

При использовании OSPF-маршрутизации таблицы маршрутизации домена позволяют получить доступ ко всем входящим в него сетям. Однако пользователям домена OSPF необходимо также получать доступ к сетям, не принадлежащим этому домену (например, к глобальной сети Internet).

Существует необходимость в стандартном маршруте, который бы позволял маршрутизаторам пересылать пакеты с неизвестными адресами в направлении маршрутизатора, в таблице маршрутизации которого, возможно, имеется адрес сети получателя для данного пакета. Сконфигурированный стандартный маршрут используется маршрутизаторами для генерирования “шлюза последней надежды” (“Gateway of Last Resort.”). В приведенной ниже команде конфигурируется стандартный статический маршрут к сети 0.0.0.0 с маской подсети 0.0.0.0.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [ interface | next-hop address]
```

Этот маршрут соответствует любому сетевому адресу, поскольку согласно правилу, адрес шлюза получается путем применения операции AND к адресу пункта назначения и маске подсети. Для распространения этого маршрута всем маршрутизаторам обычной зоны протокола OSPF используется следующая команда конфигурирования:

```
Router(config-router)# default-information originate
```

При использовании этой команды все маршрутизаторы данной зоны протокола OSPF будут знать этот стандартный маршрут при условии, что функционирует интерфейс граничного маршрутизатора, соединенный с этим стандартным маршрутом.



Лабораторная работа: распространение маршрутов по умолчанию в домене протокола OSPF

В этой лабораторной работе изучается процесс создания и распространения по сети протокола OSPF маршрутов по умолчанию, что позволяет всем узлам зоны OSPF осуществлять соединения с внешними сетями.

Общие вопросы конфигурирования протокола OSPF

Для эффективного, быстрого и успешного функционирования протокола OSPF сетевой администратор должен быть знаком с основными проблемами, которые могут возникать при его конфигурировании. OSPF-маршрутизация в отдельной зоне может функционировать неудовлетворительно по ряду причин. Прежде всего, OSPF-маршрутизатор для обмена информацией о маршрутах должен установить отношения смежности со всеми остальными маршрутизаторами данной зоны. Неудачный результат при установке таких отношений может быть вызван любой из приведенных ниже причин:

- сообщения Hello от обоих соседних устройств не рассылаются;
- таймеры рассылки сообщений Hello и критических сообщений различных маршрутизаторов имеют разные интервалы;
- интерфейсы маршрутизаторов соответствуют разным типам сетей;
- пароли или ключи аутентификации различных маршрутизаторов не совпадают.

При использовании протокола OSPF маршрутизация важна также для того, чтобы:

- все интерфейсы имели правильные адреса и маски подсетей;
- команды **network area** имели правильные маски шаблонов;
- команды **network area** назначали интерфейсам соответствующие зоны.

Тестирование конфигурации протокола OSPF

Для тестирования конфигурации протокола OSPF используется ряд команд **show**. Эти команды приведены в табл. 3.5.

Таблица 3.5. Команды протокола OSPF и команды вывода статистических данных

Команда	Описание
show ip protocol	Отображает параметры таймеров, фильтров, метрики, параметры сети и другую информацию, относящуюся ко всему маршрутизатору
show ip route	Отображает известные маршрутизатору маршруты и источники, из которых они получены. Использование этой команды является одним из лучших способов проверить соединения локального маршрутизатора с остальной частью объединенной сети
show ip ospf interface	Проверяет, были ли с конфигурированы интерфейсы в требуемых зонах. Если не указан адрес петлевого интерфейса, то адрес этого интерфейса рассматривается как идентификатор данного маршрутизатора. Эта команда также выводит значения интервалов таймеров, включая интервал рассылки сообщений Hello и отображает отношения смежности с соседними устройствами
show ip ospf	Выводит число выполнений алгоритма выбора кратчайшего пути (shortest path first — SPF). Она также выводит значение интервала рассылки сообщений об изменениях в состоянии канала в условиях, когда изменений в топологии сети не происходит
show ip ospf neighbor detail	Отображает подробный список соседних устройств, их приоритеты и состояние (например, состояния <i>init</i> , <i>exstart</i> , или <i>full</i>)
show ip ospf database	Отображает содержимое топологической базы данных, поддерживаемой данным маршрутизатором. Эта команда также отображает ID маршрутизатора и ID OSPF-процесса. При использовании в данной команде различных ключевых слов может быть отображен ряд типов баз данных. Более подробную информацию о ключевых словах можно получить по адресу www.cisco.com
clear ip route*	Очищает всю IP-таблицу маршрутизации
clear ip route a.b.c.d	Удаляет из таблицы маршрутизации только маршрут, заданный адресом a.b.c.d.
debug ip ospf	Выполняет отладку операций протокола OSPF

Резюме

Основные положения, которые обсуждались в настоящей главе, приведены ниже.

- Реализация OSPF-маршрутизации в отдельной зоне целесообразна в небольших сетях.
- Протокол OSPF конфигурируется аналогично другим протоколам маршрутизации. Отличия связаны с тем, что протокол OSPF является протоколом состояния канала связи.
- Для функционирования протокола OSPF необходимо задание идентификатора процесса и идентификаторов маршрутизаторов.

- Устойчивость функционирования протокола OSPF обеспечивается конфигурированием петлевого интерфейса.
- В широковещательных сетях множественного доступа выбирается назначенный маршрутизатор (designated router — DR). Этот маршрутизатор выступает от имени других маршрутизаторов при распространении в сегменте информации о состоянии канала. Для того, чтобы в качестве назначенного маршрутизатора был выбран заранее известный маршрутизатор, на интерфейсе конфигурируется приоритет протокола OSPF.
- Сетевой администратор может управлять оценками каналов и таймерами, которые оказывают влияние на распространение информации о состоянии каналов, а также повысить уровень безопасности в сети путем конфигурирования аутентификации маршрутизаторов.
- Общий обзор проблем, возникающих при конфигурировании протокола OSPF и команд тестирования конфигурации протокола OSPF.
- Протокол OSPF, являясь протоколом маршрутизации по состоянию канала, отличается от дистанционно-векторных протоколов, таких как протокол RIP. OSPF-маршрутизаторы принимают решения о наилучших маршрутах на основе полной информации о сетевой топологии. Метрикой, используемой для определения маршрута, является оценка, которая базируется на ширине полосы пропускания канала. При использовании иерархического проектирования протокол OSPF может быть эффективно использован в крупных объединенных сетях.
- Алгоритм выбора кратчайшего пути определяет свободный от петель маршрут с наименьшей оценкой к каналу или сети. Поскольку OSPF-маршрутизаторам требуется полная топология всей сети, а алгоритм SPF достаточно сложен, для реализации протокола OSPF требуются более мощные маршрутизаторы с большим объемом памяти.
- Алгоритм выбора кратчайшего пути был создан для сетей с соединениями типа “точка-точка”. Для реализации протокола OSPF во всем множестве доступных в настоящее время сетей ему требуется знать тип сети, в которой он функционирует. Для эффективной работы этого протокола в сетях множественного доступа необходимо выбрать назначенный маршрутизатор DR, который выступает в качестве фокальной точки при обмене информацией о состоянии канала, а также резервный маршрутизатор BDR повышающий надежность сети.
- До начала обмена информацией протокол OSPF устанавливает отношения смежности между соседними маршрутизаторами. Протокол Hello, входящий в состав OSPF, устанавливает отношения соседства между смежными маршрутизаторами.

В дополнение к уже изученному материалу данной главы рекомендуется ознакомиться с лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

Алгоритм выбора кратчайшего маршрута (SPF (shortest path first) algorithm). Алгоритм маршрутизации, осуществляющий итерации по всей длине маршрута для определения связующего дерева с кратчайшим маршрутом. Часто используется в алгоритмах маршрутизации по состоянию канала. Иногда называется алгоритмом Дейкстры (Dijkstra) по имени автора.

Идентификатор маршрутизатора (router identifier — router ID). IP-адрес, идентифицирующий маршрутизатор, принимающий участие в работе протокола OSPF. ID маршрутизатора берется с активного интерфейса с наивысшим IP-адресом или со сконфигурированного петлевого интерфейса.

Идентификатор процесса (process identifier — process ID). Числовое значение, назначаемое в процессе конфигурирования протокола OSPF, идентифицирующее каждый OSPF-процесс, протекающий на маршрутизаторе.

Лавинная рассылка (flooding). Процесс рассылки информации со всех портов, кроме того, на котором эта информация была получена.

Магистраль (backbone). Часть сети, которая является первичным маршрутом для потоков данных, поступающих в конкретную сеть из других сетей или направляемых ею в другие сети.

Назначенный маршрутизатор (designated router — DR). OSPF-маршрутизатор, который генерирует сообщения LSA в сетях множественного доступа и выполняет другие специальные функции, связанные с функционированием протокола OSPF. В каждой OSPF-сети множественного доступа, в которой имеется как минимум два маршрутизатора, имеется назначенный маршрутизатор, который выбирается с помощью протокола Hello, входящего в состав протокола OSPF. Выбор назначенного маршрутизатора позволяет уменьшить количество отношений смежности, требуемых в сети множественного доступа, что уменьшает объем передаваемых служебных данных протокола маршрутизации и размер топологической базы данных.

Объявление состояния канала (link-state advertisement — LSA). Широковещательный пакет, используемый протоколами состояния канала и содержащий информацию о соседних устройствах и оценках маршрутов. Принимающие этот пакет маршрутизаторы используют его для поддержки своих таблиц маршрутизации. Иногда называется пакетом состояния канала (link-state packet — LSP).

Петлевой интерфейс (loopback). Специальный IP-адрес (номер) (127.0.0.1), назначенный петлевому интерфейсу устройства, реализуемому программным обеспечением. Петлевому интерфейсу не соответствует никакого аппаратного интерфейса и он не имеет физического соединения с сетью.

Протокол Hello (Hello protocol). Протокол, используемый системами протокола OSPF для установки и поддержания соединений с соседними устройствами.

Резервный назначенный маршрутизатор (backup designated router — BDR). Маршрутизатор, принимающий на себя при необходимости функции назначенного маршрутизатора.

Сеть множественного доступа (multiaccess network). Сеть, в которой несколько устройств могут одновременно осуществлять соединения и обмениваться информацией.

Сниффер (sniffer). Программа или устройство, прослушивающее данные, проходящие по сети.

Соединение типа “точка-точка” (point-to-point). Связь между одним получателем и одним location.

Контрольные вопросы

1. В каком состоянии находятся маршрутизаторы сети OSPF после того, как были выбраны назначенный (DR) и резервный (BDR) маршрутизаторы?
 - A. В состоянии ExStart
 - B. В состоянии Full
 - C. В состоянии Loading
 - D. В состоянии Exchange
2. Какой тип пакетов OSPF используется для установки и поддержки отношений смежности между соседними маршрутизаторами?
 - A. Запрос информации о состоянии канала (Link-state request)
 - B. Подтверждение получения информации о состоянии канала (Link-state acknowledgement)
 - C. Сообщение Hello
 - D. Описание базы данных (Database description)
3. На чем основана принимаемая по умолчанию оценка канала в протоколе OSPF?
 - A. На величине задержки в канале
 - B. На величине полосы пропускания
 - C. На оценке эффективности работы сети
 - D. Определяется объемом передаваемых по сети данных
4. Какой адрес многоадресной рассылки представляет все OSPF-маршрутизаторы?
 - A. 224.0.0.6
 - B. 224.0.0.1
 - C. 224.0.0.4
 - D. 224.0.0.5
5. Какая команда может быть использована для изменения OSPF-приоритета на интерфейсе?
 - A. `ip priority number ospf`
 - B. `ip ospf priority number`
 - C. `ospf priority number`
 - D. `set priority ospf number`
6. Какой адрес многоадресной рассылки используется для рассылки сообщений LSU всем маршрутизаторам DR/BDR?
 - A. 224.0.0.6
 - B. 224.0.0.1
 - C. 224.0.0.4
 - D. 224.0.0.5

7. Какая общая функция используется в сетях NBMA?
 - A. Поддержка только двух маршрутизаторов
 - B. Поддержка более двух маршрутизаторов
 - C. Отсутствует выбор назначенного маршрутизатора DR
 - D. Полная поддержка широковещательных пакетов и пакетов многоадресатной рассылки
8. Какая команда позволяет маршрутизаторам сети OSPF обмениваться информацией обновления маршрутов без использования многоадресатной рассылки?
 - A. `ip ospf neighbor`
 - B. `ospf neighbor`
 - C. `neighbor`
 - D. `ip neighbor`
9. Какая из приведенных ниже команд отображает все известные маршрутизатору маршруты и источники, из которых они получены?
 - A. `show ip protocol`
 - B. `show ip route`
 - C. `show ip ospf`
 - D. `show ip ospf neighbor detail`



В этой главе...

- Описаны функции и основные положения протокола EIGRP
- Рассмотрена работа алгоритма DUAL
- Приведен список структур данных протокола EIGRP
- Описано конфигурирование протокола EIGRP
- Описано тестирование протокола EIGRP и устранение ошибок

Усовершенствованный протокол маршрутизации внутреннего шлюза

В настоящей главе описана фирменная Cisco-реализация усовершенствованного протокола маршрутизации внутреннего шлюза. В ней рассмотрено конфигурирование, тестирование протокола EIGRP и устранение ошибок. Также выполнено сравнение протокола EIGRP с протоколом маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP). Кроме этого, описаны основные понятия, технологии и структуры данных протокола EIGRP. После этого концептуального обзора рассматривается процесс конвергенции протокола EIGRP и его базовые операции, осуществляемые с использованием современного алгоритма маршрутизации EIGRP, называемого алгоритмом диффузии обновлений маршрутизации (Diffusing Update Algorithm — DUAL).

Рекомендуется также выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Обзор протокола EIGRP

Протокол EIGRP представляет собой фирменный протокол маршрутизации Cisco, основанный на протоколе IGRP.

В отличие от протокола IGRP, который является протоколом маршрутизации, использующим классы адресов, протокол EIGRP поддерживает бесклассовую междоменную маршрутизацию (classless interdomain routing — CIDR), которая позволяет сетевым проектировщикам максимально использовать адресное пространство, применяя маршрутизацию CIDR и маски подсети переменной длины (variable-length subnet mask — VLSM). От протокола IGRP он отличается более быстрой сходимостью (конвергенцией), повышенной масштабируемостью и более эффективной обработкой петель маршрутизации.

Кроме того, протокол EIGRP может заменить протокол информации о маршрутах Novell (Routing Information Protocol — RIP) или протокол поддержки таблицы маршрутизации AppleTalk (Routing Table Maintenance Protocol — RTMP), повышая эффективность работы сетей IPX и AppleTalk.

Протокол EIGRP часто называют гибридным протоколом маршрутизации, сочетающим в себе лучшие черты дистанционно-векторных алгоритмов и алгоритмов маршрутизации по состоянию канала. В техническом аспекте протокол EIGRP

представляет собой дистанционно-векторный протокол маршрутизации, который базируется на функциях, обычно присущих протоколам маршрутизации по состоянию канала. Протокол EIGRP также использует лучшие функции протокола OSPF, такие, как частичные обновления маршрутов и обнаружение соседних устройств. Однако EIGRP проще конфигурируется, чем протокол выбора кратчайшего маршрута (Open Shortest Path First — OSPF).

Протокол EIGRP является идеальным решением для крупных многопротокольных сетей, построенных на базе маршрутизаторов Cisco.

Процессы и технологии протокола EIGRP

Протокол EIGRP был обнародован в 1994 году как масштабируемая усовершенствованная версия фирменного дистанционно-векторного протокола Cisco, называемого протоколом маршрутизации внутреннего шлюза (IGRP). В нем используется та же дистанционно-векторная концепция, что и в протоколе IGRP, и он опирается на ту же информацию о маршрутах.

Однако у протокола EIGRP значительно улучшены характеристики конвергенции и повышена производительность. Это позволяет использовать более совершенную архитектуру, сохраняя, однако, оборудование, на котором ранее использовался протокол IGRP.

Режим совместимости

Протоколы EIGRP и IGRP полностью совместимы друг с другом. Это позволяет гармонично сочетать в сети маршрутизаторы, использующие протоколы EIGRP и IGRP. Это дает возможность использовать преимущества обоих протоколов. Одним из немногих отличий является то, что протокол EIGRP поддерживает работу нескольких протоколов, а в то время как IGRP такой функцией не обладает.

Вычисление метрики

Протоколы EIGRP и IGRP по-разному вычисляют метрику маршрута. Метрика протокола EIGRP получается из метрики IGRP путем умножения последней на коэффициент 256. Это объясняется тем, что EIGRP использует метрику длиной 32 бита, в то время как IGRP использует метрику длиной 24 бита. Путем умножения или деления на 256 протокол может легко обмениваться информацией с протоколом IGRP. Оба протокола, IGRP и EIGRP, для вычисления метрики используют приведенную ниже формулу.

$$\text{Метрика} = [K1 * \text{ширина полосы пропускания} + (K2 * \text{ширина полосы пропускания}) / (256 - \text{нагрузка}) + (K3 * \text{задержка})] [K5 / (\text{надежность} + K4)]$$

Стандартные значения коэффициентов равны:

$$K1 = 1$$

$$K2 = 0$$

$$K3 = 1$$

$$K4 = 0$$

$$K5 = 0$$

Если коэффициенты K4 и K5 равны 0, то слагаемое $[K5 / (\text{надежность} + K4)]$ на значение метрики не влияет. Таким образом, при стандартных значениях коэффициентов формула для метрики имеет вид:

$$\text{метрика} = \text{ширина полосы пропускания} + \text{задержка}$$

Для определения значений, требуемых при вычислении метрики, протоколы IGRP и EIGRP используют приведенные ниже формулы (следует обратить внимание на то, что для EIGRP эти значения умножаются на 256).

$$\begin{aligned}\text{Полоса пропускания для IGRP} &= (10\,000\,000 / \text{полоса пропускания}) \\ \text{Полоса пропускания для EIGRP} &= (10\,000\,000 / \text{полоса пропускания}) * 256 \\ \text{Задержка для IGRP} &= \text{задержка} / 10 \\ \text{Задержка для EIGRP} &= (\text{задержка} / 10) * 256\end{aligned}$$

Количество переходов

Для протокола EIGRP максимальное количество переходов равно 224. Этого более чем достаточно для поддержки даже самых крупных современных сетей. Для протокола IGRP это значение равно 255, в то время как протокол RIP допускает не более 15 переходов.

Автоматическое распространение информации в маршрутах

При использовании разных протоколов маршрутизации, таких, например, как OSPF и RIP обмен информацией между ними требует довольно сложного конфигурирования. Однако для протоколов IGRP и EIGRP такое совместное использование информации или распространение маршрутов происходит автоматически, при условии, что оба процесса используют один и тот же номер автономной системы.

На рис. 4.1 показано как маршрутизатор RTB автоматически распространяет известные протоколу EIGRP маршруты на автономную систему протокола IGRP и наоборот.

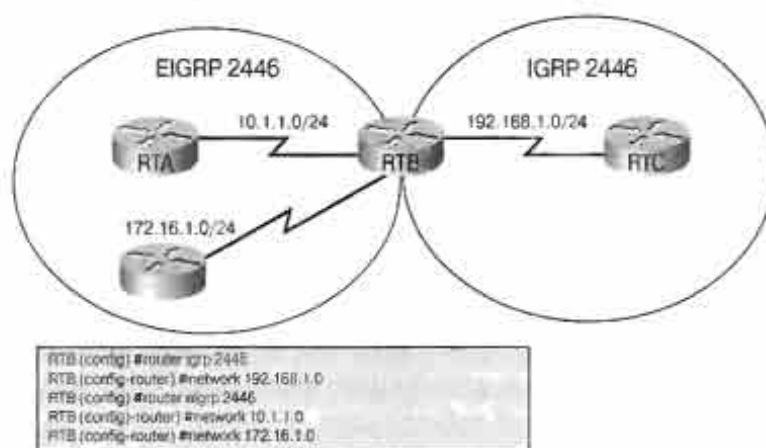


Рис. 4.1. Протоколы EIGRP и IGRP совместно используют информацию о маршрутах

Теги маршрутов

Протокол EIGRP создает теги для маршрутов, которые он получил от протокола IGRP (или от любого другого источника) как внешние, поскольку они не были изначально получены от маршрутизаторов EIGRP. Протокол IGRP не может различать внутренние и внешние маршруты.

В примере 4.1 приведен вывод по команде **show ip route** для маршрутизаторов; при этом маршруты протокола EIGRP помечены флагом 'D', а внешние маршруты помечены символами 'EX'. Маршрутизатор RTA различает маршруты, полученные при посредстве протокола EIGRP (сеть 172.16.0.0) и полученные от протокола IGRP (сеть 192.168.1.0). Протокол IGRP в таблице маршрутизации RTC не делает этого различия.

Пример 4.1. Вывод по команде show ip route

```
RTA#show ip route
<output omitted>
C 10.1.1.0 is directly connected, Serial0
D 172.16.1.0 [90/2681856] via 10.1.1.1, Serial0
D EX 192.168.1.1 [170/2681856] via 10.1.1.1, 00:00:04, Serial0
RTC#show ip route
<output omitted>
C 192.168.1.0 is directly connected, Serial0
I 10.0.0.0 [100/10476] via 192.168.1.1, 00:00:04 Serial0
I 172.16.0.0 [100/10476] via 192.168.1.1, 00:00:04, Serial0
```

Маршрутизатор RTC, который работает только с протоколом IGRP регистрирует все маршруты как маршруты протокола IGRP, несмотря на то, что маршруты к сетям 10.1.1.0 и 172.16.0.0 были получены от протокола EIGRP.

Преимущества использования протокола EIGRP:

Протокол EIGRP функционирует совершенно иным образом, чем IGRP. Будучи усовершенствованным дистанционно-векторным протоколом маршрутизации, EIGRP обновляя свой список соседних устройств и поддерживая информацию о маршрутах, функционирует как протокол состояния канала. Преимущества протокола EIGRP перед простыми дистанционно-векторными протоколами описаны ниже.

- **Быстрая конвергенция (Rapid convergence)** — На маршрутизаторах протокола EIGRP конвергенция происходит значительно быстрее, поскольку она базируется на современном алгоритме маршрутизации, называемом *DUAL*. Этот алгоритм гарантирует отсутствие петель в каждый момент времени на всем протяжении маршрута и позволяет всем маршрутизаторам, принадлежащим к данной топологии, выполнить одновременную синхронизацию.
- **Эффективное использование полосы пропускания (Efficient use of bandwidth)** — Протокол EIGRP позволяет эффективно использовать полосу пропускания путем рассылки частичных, ограниченных по объему обновлений маршрутизации и вследствие этого минимального использования ими полосы пропускания в условиях стабильной работы сети.
 - **Частичные, ограниченные обновления маршрутов (Partial, bounded updates)** — Маршрутизаторы EIGRP как правило рассылают частичные, поэтапные обновления маршрутизации, а не полные таблицы маршрутизации. Этот процесс аналогичен работе протокола OSPF, однако в отличие от маршрутизаторов OSPF, маршрутизаторы протокола EIGRP рассылают эти частичные обновления только тем маршрутизаторам, которым они действительно требуются, а не всем маршрутизаторам данной области. Вследствие этого такие обновления также называются ограниченными.
 - **Минимальное использование полосы пропускания в условиях стабильной работы сети** — Вместо регулярной рассылки обновлений маршрутизации маршрутизаторы EIGRP поддерживают постоянный контакт друг с другом путем рассылки небольших пакетов приветствия. Хотя пакеты приветствия рассылаются регулярно, из-за своего небольшого размера они весьма не-

значительно используют полосу пропускания, в отличие, например, от протоколов RIP и IGRP, которые рассылают соседним устройствам свою полную таблицу маршрутизации каждые 30 или 90 секунд, соответственно.

- **Поддержка масок подсети VLSM и маршрутизации CIDR** — В отличие от протокола IGRP, протокол EIGRP обеспечивает полную поддержку бесклассового IP путем обмена масками подсетей в сообщениях обновления маршрутов.
- **Поддержка нескольких протоколов сетевого уровня** — Протокол EIGRP поддерживает протоколы IP, IPX и AppleTalk путем использования зависящих от протокола модулей (protocol-dependent module — PDM).

Независимость от маршрутизируемых протоколов

Модули PDM избавляют протокол EIGRP от необходимости выполнения многих обременительных преобразований. Эволюция сетевых протоколов, например, протокола IP, может потребовать замены модуля протокола, но не обязательно модернизации всей сети EIGRP.

Терминология протокола EIGRP

Маршрутизаторы протокола EIGRP поддерживают информацию о маршрутах и о топологии сети, которая легко доступна, поскольку находится в памяти RAM, и могут быстро реагировать на происходящие в сети изменения. Как и протокол OSPF, EIGRP хранит эту информацию в нескольких таблицах, также называемых базами данных протокола.

Протокол EIGRP работает с маршрутами своими особыми способами. Все маршруты предоставляется особый статус и они могут быть помечены тегами, в которых записана дополнительная полезная информация.

Таблица соседних устройств

Таблица соседних устройств (neighbor table) является наиболее важной таблицей в протоколе EIGRP. Каждый маршрутизатор EIGRP поддерживает таблицу соседних устройств, в которой перечислены смежные маршрутизаторы. Эту таблицу можно сравнить с базой данных отношений смежности, которую использует протокол OSPF. Для каждого протокола, который поддерживается протоколом EIGRP, имеется своя таблица соседних устройств.

При обнаружении новых соседних устройств их адреса и интерфейсы заносятся в эти таблицы. Эта информация хранится в структуре данных о соседних устройствах. При отправке пакета приветствия соседнее устройство объявляет время удержания. Это промежуток времени указывает, как долго маршрутизатор рассматривает свое соседнее устройство как достижимое и работоспособное. Иными словами, если за период удержания от маршрутизатора не поступило пакета приветствия, то считается, что время удержания истекло. По истечении времени удержания дистанционно-векторный алгоритм DUAL, используемый протоколом EIGRP, информируется об изменении в топологии и должен заново вычислить параметры новой топологии.

Ниже описаны отдельные поля, содержащиеся в таблице соседних устройств.

- **Адрес соседнего устройства, поле адреса (Neighbor address (Address))** — Адрес сетевого уровня соседнего устройства.

- **Время удержания (Hold time, Hold Uptime)** — Временной интервал, по истечении которого, в случае отсутствия каких-либо сообщений от соседнего устройства, канал рассматривается как неработоспособный. Первоначально в качестве ожидаемого пакета рассматривался только пакет приветствия, однако в текущих версиях программного обеспечения IOS Cisco любой пакет протокола EIGRP, полученный после первого пакета приветствия переустанавливает таймер на нулевое значение.
- **Таймер цикла обмена сообщениями (Smooth Round-Trip Timer — SRTT)** — Среднее время, которое требуется для того, чтобы отправить пакет соседнему устройству и получить от него ответный пакет. Этот таймер определяет интервал повторной передачи (retransmit interval — RTI).
- **Счетчик очереди (Queue count — Q Cnt)** — Число пакетов которые находятся в очереди и ожидают передачи. Если это значение постоянно больше нуля, то, вероятно, маршрутизатор испытывает переполнение. Значение 0 означает, что пакетов протокола EIGRP в очереди нет.
- **Последовательный номер (Sequence Number — Seq No)** — Номер последнего пакета, полученного от данного соседнего устройства. Протокол EIGRP использует это поле для подтверждения приема пакета, переданного соседним устройством и для идентификации пакетов которые переданы с нарушением порядка. Таблица соседних устройств обеспечивает надежную упорядоченную доставку пакетов и может рассматриваться как аналог протокола TCP, используемого для надежной доставки IP-пакетов.

Топологическая таблица

Топологическая таблица (topology table) включает в себя все таблицы маршрутизации протокола EIGRP, имеющиеся на устройствах данной автономной системы. Используемый в протоколе EIGRP дистанционно-векторный алгоритм DUAL получает информацию из таблицы соседних устройств и из топологической таблицы и на ее основе вычисляет маршруты с наименьшей оценкой к каждому пункту назначения. Маршрутизаторы протокола EIGRP следят за этой текущей информацией и благодаря этому могут быстро идентифицировать альтернативные маршруты и переключиться на них в случае необходимости. Первичный маршрут (successor) помещается в их таблицу маршрутизации. Копия его также помещается в топологическую таблицу.

Все маршрутизаторы EIGRP поддерживают топологическую таблицу для каждого сконфигурированного на них сетевого протокола. В этой таблице содержатся маршруты ко всем пунктам назначения, которые стали известны маршрутизатору. Все известные маршруты содержатся также в топологической таблице.

Ниже описаны все поля топологической таблицы.

- **Предполагаемое расстояние (FD is xxxx)** — Предполагаемое расстояние (feasible distance — FD) представляет собой наименьшую вычисленную метрику к каждому пункту назначения. Например, в примере 4.2 предполагаемое расстояние до получателя 32.0.0.0 составляет 2195456, на что указывает значение поля FD, равное 2195456.

Пример 4.2. Топологическая таблица протокола EIGRP

```
Router#show ip eigrp topology
IP-EIGRP Topology Table for process 100
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply.
R - Reply Status
P 32.0.0.0/8, 1 successors, FD is 2195456
   via 200.10.10.10 (2195456/281600), Serial1
P 170.32.0.0/16/8, 1 successors, FD is 2195456
   via 199.55.32.10 (2195456/2169856) Ethernet0
   via 200.10.10.5 (2195456/281600), Serial0
P 200.10.10.8/30, 1 successors, FD is 2169856
   via connected, Serial1
P 200.10.10.12/30, 1 successors, FD is 2681856
   via 200.10.10.10 (2681856/2169856), Serial1
P 200.10.10.0/24, 1 successors, FD is 2169856 via summary (2169856/0),
Null0
P 3200.10.10.4/30, 1 successors, FD is 2169856
   via connected, Serial0
P 205.205.205.0/24, 1 successors, FD is 2221056
   via 199.55.32.10 (2221056/2195456), /Ethernet0
   ia 200.10.10.5 (2707456/2195456), Serial0
```

- **Источник маршрута (Route source (via xxx.xxx.xxx.xxx))** — В поле источника маршрута содержится идентификационный номер маршрутизатора, который первоначально анонсировал этот маршрут. Это поле заполняется только для маршрутов, которые стали известны извне от других сетей протокола EIGRP. При использовании маршрутизации, основанной на политиках, особенно полезным может оказаться присваивание маршрутам тегов, содержащих дополнительную информацию. Например, в примере 4.2 источником маршрута к сети 32.0.0.0 является 200.10.10.10 (via 200.10.10.10).
- **Сообщенное расстояние (Reported distance)** — Под *сообщенным расстоянием маршрута (reported distance — RD)* понимается расстояние которое смежный соседний маршрутизатор сообщает конкретному получателю. В примере 4.2 сообщенное расстояние к сети 32.0.0.0 равно 281600, на что указывает значение поля RD, равное (2195456 / 281600).
- **Поле информации об интерфейсе (Interface information)** — В этом поле записан номер интерфейса, через который можно достичь пункта назначения.
- **Статус маршрута (Route status)** — Различаются пассивные маршруты (passive — P), под которыми понимаются устойчивые и готовые к использованию маршруты, и активные (active — A), в отношении которых дистанционно-векторный алгоритм DUAL протокола EIGRP продолжает процесс пересчета маршрута.

Протокол EIGRP сортирует топологическую таблицу таким образом, чтобы первичные маршруты находились в верхней части таблицы, а за ними следовали резервные. В нижней части этой таблицы находятся маршруты, которые алгоритм таблицы DUAL рассматривает как возможные петли маршрутизации.

Первичные маршруты

Первичным называется маршрут, выбираемый в качестве основного для достижения определенного пункта назначения. Этот маршрут устанавливается алгоритмом DUAL на основе информации, содержащейся в таблице соседних устройств и в топологической таблице, и помещается в таблицу маршрутизации. Для каждого конкретного маршрута может быть до четырех первичных маршрутов. Они могут иметь как равные, так и неравные оценки и рассматриваются как наилучшие свободные от петель маршруты к данному пункту назначения. Копии первичных маршрутов помещаются также в топологическую таблицу.

Резервные маршруты

Под *потенциально первичным (feasible successor — FS)* понимается резервный маршрут. Эти маршруты устанавливаются одновременно с первичными, однако хранятся только в топологической таблице. В топологической таблице могут храниться несколько резервных маршрутов. Наличие резервного маршрута для достижения получателя не является обязательным.

Маршрутизатор рассматривает устройства на резервном маршруте как соседние устройства в нисходящем направлении, т.е. считает, что они находятся ближе к пункту назначения, чем он сам. Они выражают анонсированную соседним маршрутизатором оценку маршрута к пункту назначения. Если первичный маршрут становится недействительным, то маршрутизатор ищет установленный резервный маршрут. Статус этого маршрута повышается до первичного. Резервный маршрут к пункту назначения должен иметь меньшую анонсированную оценку, чем у существующего первичного маршрута. Если резервный маршрут не был установлен на основе имеющейся информации, то маршрутизатор присваивает этому маршруту статус активного (Active) и рассылает пакеты запросов всем соседним устройствам для пересчета топологии. После получения ответов на эти запросы маршрутизатор может на основе содержащихся в них данных установить новые первичные маршруты или резервные маршруты. После этого маршрутизатор присваивает маршруту статус пассивного (Passive).

Выбор первичного маршрута и резервных маршрутов

Возникает вопрос: каким образом маршрутизатор EIGRP определяет, какие маршрутизаторы являются первичными, а какие — резервными? Предположим, что в таблице маршрутизации маршрутизатора RTA имеется маршрут через к сети Network Z через маршрутизатор RTB (рис. 4.2). С точки зрения маршрутизатора RTA, маршрутизатор RTB находится на текущем первичном маршруте к сети Network Z, поэтому RTA пересылает пакеты, предназначенные для сети Network Z в направлении RTB. Маршрутизатор RTA должен иметь по крайней мере один первичный маршрут к сети Network Z для того, чтобы алгоритм DUAL мог поместить его в таблицу маршрутизации.

Может ли маршрутизатор RTA иметь более одного первичного маршрута к сети Network Z? Если маршрутизатор RTC объявляет о наличии у него маршрута к сети Network Z с такой же метрикой, как и у маршрутизатора RTB, то RTA также рассматривает RTC в качестве первичного маршрута и алгоритм DUAL устанавливает второй маршрут к сети Network Z через RTC (рис. 4.3).

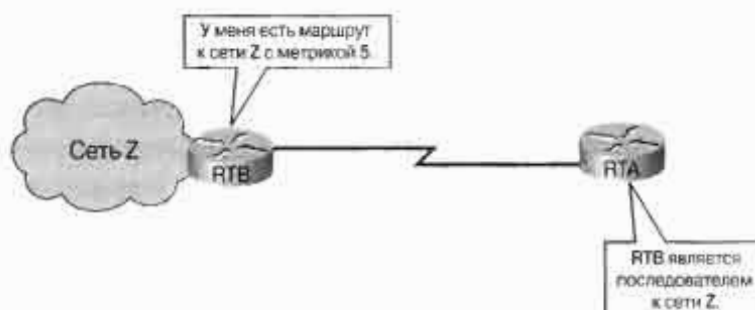


Рис. 4.2. Первичный маршрут и резервные маршруты протокола EIGRP

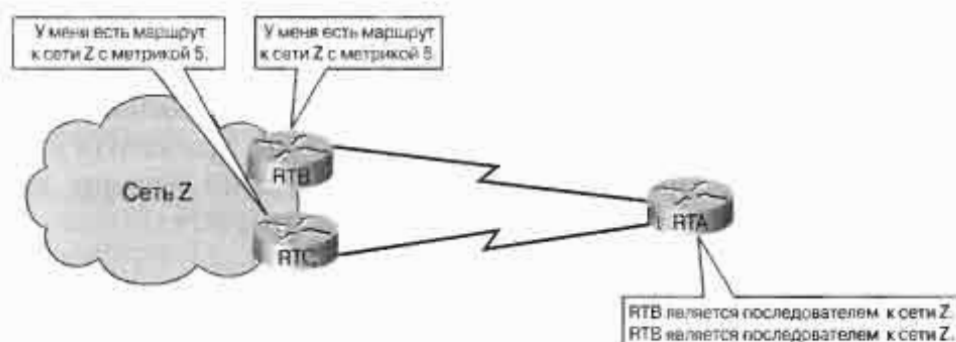


Рис. 4.3. Первичные маршруты и резервные маршруты протокола EIGRP (2)

Любое из других соседних устройств маршрутизатора RTA, которое анонсирует свободный от петель маршрут к сети Network Z (однако с сообщенным расстоянием, большим, чем метрика наилучшего маршрута и меньшим, чем предполагаемое расстояние), идентифицируется в топологической таблице как лежащее на резервном маршруте (рис. 4.4).

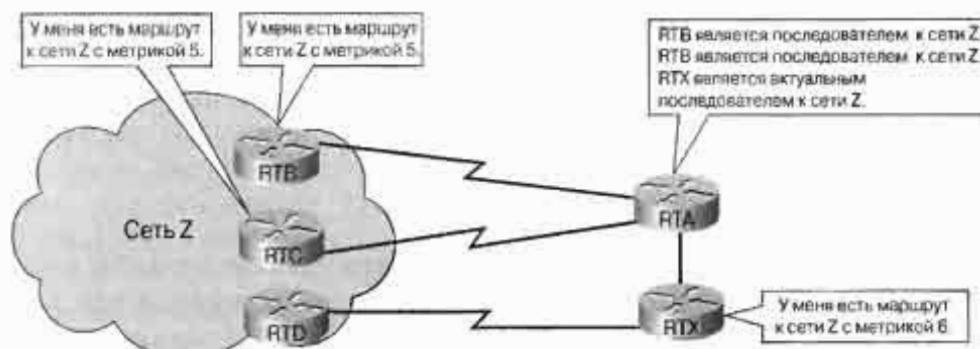


Рис. 4.4. Первичные маршруты и резервные маршруты протокола EIGRP(3)

Маршрутизатор рассматривает свои устройства на резервных маршрутах как соседние устройства, находящиеся в нисходящем направлении, т.е. как устройства, расположенные ближе к получателю, чем он сам. Если по каким-либо причинам первичный маршрут не может выполнять свои функции, то алгоритм DUAL может быстро найти резервный маршрут на основе данных топологической таблицы и установить новый маршрут к пункту назначения. Если резервный маршрут к пункту назначения отсутствует, то алгоритм DUAL переводит маршрут в активное состояние (Active state). Позиции статуса маршрута топологической таблицы могут иметь одно из двух значений: ак-

тивное состояние (Active) или пассивное (Passive). Эти состояния отражают статус маршрута, указываемого данной позицией, а не состояние позиции.

Под пассивным понимается маршрут, который устойчив и готов к использованию. Под активным понимается маршрут, который в настоящий момент пересчитывается алгоритмом DUAL. Такой пересчет происходит в том случае, когда маршрут становится недоступным и DUAL не может найти резервного маршрута. В этом случае маршрутизатор должен запросить помощь у соседних устройств в нахождении нового, свободного от петель маршрута к пункту назначения. Соседние маршрутизаторы обязаны ответить на этот запрос. Если у соседнего маршрутизатора имеется соответствующий маршрут, то он отвечает, предоставляя информацию о первичном маршруте(маршрутах). В противном случае соседний маршрутизатор уведомляет отправителя о том, что у него также нет маршрута к этому пункту назначения.

Избыточное количество пересчетов маршрутов свидетельствует о нестабильной работе сети и понижает ее производительность. Для предотвращения проблем, связанных с конвергенцией, алгоритм DUAL перед тем, как прибегнуть к пересчету, всегда пытается найти резервный маршрут. Если резервный маршрут имеется, то алгоритм DUAL может установить новый маршрут без пересчета.

Застревание активных маршрутов

Если один или более маршрутизаторов, которым был разослан запрос, не отвечает в течение активного времени, равного 180 секундам (3 минутам), то маршрут (маршруты) переводится в состояние “застревания” (*stuck in active*). В этом случае протокол EIGRP исключает из своей таблицы соседних устройств маршрутизаторы, которые не ответили на запрос и регистрирует в системном журнале сообщение об ошибке “stuck in active” для маршрутов, которые были активными.

Таблица маршрутизации

Используя алгоритм DUAL протокол EIGRP выбирает наилучшие маршруты к пунктам назначения из топологической таблицы и помещает их в свою таблицу маршрутизации. Каждый маршрутизатор EIGRP поддерживает для каждого установленного на нем протокола свою отдельную таблицу маршрутизации.

Создание тегов для маршрутов

В топологической таблице может быть записана дополнительная информация о каждом маршруте. Протокол EIGRP классифицирует маршруты как внутренние или внешние. Для выполнения такой классификации EIGRP создает соответствующий тег для каждого маршрута. Внутренними называются маршруты внутри данной автономной системы протокола EIGRP.

Внешними называются маршруты, берущие свое начало вне данной автономной системы протокола EIGRP. Маршруты, полученные или перераспределенные от других протоколов маршрутизации, таких как RIP, OSPF или IGRP, считаются внешними.

Статические маршруты, которые начинаются вне автономной системы, являются внешними. В качестве тега маршруту может быть присвоено значение из диапазона от 0 до 255.

Все внешние маршруты заносятся в топологическую таблицу и им назначается тег, содержащий приведенную ниже информацию.

- Идентификационный номер (ID маршрутизатора) маршрутизатора EIGRP, который распространил маршрут в сеть EIGRP;
- Номер автономной системы получателя;
- Протокол, используемый во внешней сети;
- Оценка или метрика, полученная от внешнего протокола;
- Конфигурируемый тег администратора.

В примере 4.3 показана конкретная позиция топологической таблицы для внешнего маршрута.

Пример 4.3. Информация тега маршрута

```
Router# show ip eigrp topology 204.100.50.0
IP=EIGRP topology entry for 204.100.50.0/24
State is Passive, Query origin flag is 1. 1 Successor(s), FD is
2297856
Routing Descriptor Blocks:
10.1.0.1 (Serial0), from 10.1.0.1, Send flag is 0x0
Composite metric is (2297856/128256), Route is External
Vector metric:
Minimum bandwidth is 1544 Kbit
Total delay is 25000 microseconds
Reliability is 255/255
Load is 1/255
Minimum MTU is 1500
Hop count is 1
External data:
Originating router is 192.168.1.1
AS number of route is 0
External protocol is Connected, external metric is 0
Administrator tag is 0 (0x00000000)
```

Для задания строгой и точной политики маршрутизации рекомендуется воспользоваться функцией задания маршрутам тегов и, в особенности, тегом администратора (в данном примере выделен полужирным шрифтом). Тег администратора может быть любым числом из диапазона от 0 до 255; в сущности это обычный тег, который можно использовать для реализации какой-либо специальной стратегии маршрутизации. Внешние маршруты могут приниматься, отвергаться или распространяться на основе любого из тегов маршрута, в том числе и тега администратора. Поскольку пользователь может задать тег администратора любым удобным для него способом, функция задания тегов маршрутам предоставляет большую свободу в управлении сетью. Этот уровень точности и гибкости оказывается особенно полезным в тех случаях, когда сеть протокола EIGRP взаимодействует с сетью протокола граничного шлюза, которая базируется на использовании политик.

Функции и технологии протокола EIGRP

Протокол EIGRP включает в себя много новых технологий, каждая из которых улучшает операционную эффективность, повышает скорость конвергенции и расширяет набор функций протокола IGRP и других протоколов маршрутизации. Эти технологии можно подразделить на приведенные ниже четыре категории.

- Обнаружение соседних устройств и восстановление утерянной с ними связи.
- Надежный транспортный протокол (Reliable Transport Protocol).
- Алгоритм DUAL конечных состояний машины.
- Модули конкретных протоколов.

Обнаружение соседних устройств и восстановление утерянной с ними связи

Обычные простые дистанционно-векторные маршрутизаторы не устанавливают связей со своими соседними устройствами. Маршрутизаторы, использующие протоколы RIP и IGRP просто выполняют широковещательную или многоадресную рассылку обновлений маршрутизации с соответствующим образом сконфигурированных интерфейсов. В отличие от них маршрутизаторы протокола EIGRP активно устанавливают связи со своими соседними устройствами, во многом так же, как это делают маршрутизаторы протокола OSPF. На рис. 4.5 проиллюстрирована установка связей между смежными устройствами протокола EIGRP. Маршрутизаторы EIGRP устанавливают отношения смежности с соседними маршрутизаторами путем рассылки небольших пакетов приветствия. Эти пакеты приветствия по умолчанию рассылаются каждые 5 секунд на каналах с большой полосой пропускания и каждые 60 секунд на низкоскоростных многоточечных каналах. Маршрутизатор EIGRP предполагает, что до тех пор, пока от известных ему соседних устройств поступают пакеты приветствия, они (и их маршруты) остаются действующими (они называются пассивными).



Рис. 4.5. Соседние устройства протокола EIGRP обмениваются информацией о маршрутах

Формируя отношения смежности маршрутизаторы EIGRP получают возможности:

- динамически узнавать о новых маршрутах, появляющихся в сети;
- идентифицировать маршрутизаторы, которые стали недостижимыми или неработоспособными;
- вновь обнаруживать маршрутизаторы, которые ранее были недостижимы.

Надежный транспортный протокол

Надежный транспортный протокол (Reliable Transport Protocol — RTP) представляет собой протокол транспортного уровня, который может гарантировать упорядоченную доставку пакетов EIGRP всем соседним устройствам. В сетях протокола IP узлы используют протокол TCP для упорядочения пакетов и своевременной их доставки. Однако протокол EIGRP независим от используемого сетевого протокола; это означает, что он не полагается на протокол TCP/IP для обмена информацией маршрутизации, как это делают протоколы RIP, IGRP и OSPF. Для того, чтобы быть независимым от IP, протокол EIGRP использует надежный транспортный протокол в качестве своего фирменного протокола транспортного уровня для гарантированной доставки информации о маршрутах.

EIGRP может активизировать протокол RTP для обеспечения службы надежной или негарантированной доставки в зависимости от конкретной ситуации. Например, пакеты приветствия не требуют дополнительной нагрузки на сеть, вызываемой гарантированной доставкой, поскольку они рассылаются часто и их размер должен быть небольшим. Тем не менее гарантированная (надежная) доставка информации о маршрутах действительно может ускорить конвергенцию, поскольку маршрутизаторы EIGRP не ожидают истечения времени таймера перед повторной передачей.

Использование надежного транспортного протокола позволяет протоколу EIGRP одновременно осуществлять многоадресную и одноадресную рассылку, что обеспечивает максимальную эффективность.

Машина конечных состояний алгоритма DUAL

Главным компонентом протокола EIGRP является алгоритм, основной задачей которого является вычисление маршрутов. Полное название этой технологии — машина конечных состояний (finite-state machine — FSM) алгоритма DUAL. FSM является абстрактной машиной, а не механической машиной с движущимися деталями. Машина FSM определяет набор возможных состояний, через которые можно пройти, какие события вызывают эти состояния и какие события являются результатом этих состояний. Проектировщики используют FSM для описания того, как устройство, компьютерная программа или алгоритм маршрутизации реагируют на некоторый набор входных событий. Машина FSM алгоритма DUAL содержит все логические операции, необходимые для вычисления и сравнения маршрутов в сети протокола EIGRP.

Алгоритм DUAL следит за всеми маршрутами, анонсированными соседними устройствами и использует составную (композиционную, composite) метрику для каждого маршрута с целью их сравнения. Алгоритм DUAL также гарантирует, что каждый маршрут не содержит петлю. После соответствующих вычислений алгоритм DUAL заносит маршруты с наименьшими оценками в таблицу маршрутизации. Эти маршруты известны как первичные. Копии этих первичных маршрутов заносятся также в топологическую таблицу.

Протокол сохраняет важную маршрутную и топологическую информацию в таблице соседних устройств и в топологической таблице, откуда она легко может быть получена. Эти таблицы предоставляют алгоритму DUAL всеобъемлющую маршрутную информацию в случае нарушений в работе сети. Используя информацию этих таблиц алгоритм DUAL может при необходимости быстро находить альтернативные маршруты. Если какой-либо канал становится неработоспособным, то DUAL ищет

в топологической таблице альтернативный маршрут, также называемый *потенциально первичным* или *резервным* (*feasible successor*).

Пакеты, направленные в сеть-получатель, немедленно пересылаются по резервному маршруту, который в этот момент получает статус первичного, как показано на рис. 4.6.

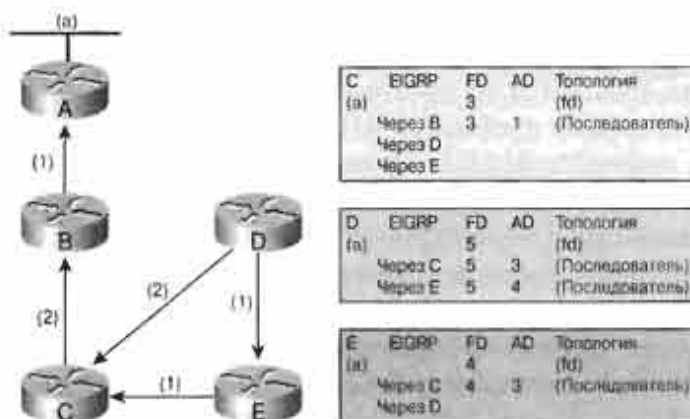


Рис. 4.6. Конвергенция в соответствии с вычислениями алгоритма DUAL протокола EIGRP

Следует обратить внимание на то, что в примере на рис. 4.6 маршрутизатор D не имеет идентифицированного первичного маршрута. Вероятное расстояние FD (вычисленная оценка) для маршрута от маршрутизатора D к маршрутизатору A равно 2, а анонсированное расстояние (advertised distance — AD), через маршрутизатор C равно 3. Поскольку AD меньше, чем метрика наилучшего маршрута, но больше чем расстояние FD, ни один резервный маршрут не заносится в топологическую таблицу. Маршрутизатор C имеет идентифицированный резервный маршрут, так же как и маршрутизатор E, поскольку маршрут свободен от петель, а расстояние AD до маршрутизатора следующего перехода меньше, чем расстояние FD для первичного маршрута.

Модули PDM

Одним из наиболее привлекательных качеств протокола EIGRP является его модульная структура. Модульное проектирование на различных уровнях обеспечивает максимальный уровень масштабируемости и адаптируемости. Поддержка различных сетевых (маршрутизируемых) протоколов, таких как IP, IPX и AppleTalk, реализована в протоколе EIGRP посредством модулей PDM. Теоретически EIGRP может быть легко адаптирован к новым или модифицированным сетевым протоколам (например, IPv6) путем добавления нового модуля PDM. На рис. 4.7 показана общая схема работы модуля PDM.

Каждый модуль PDM отвечает за выполнение всех функций, связанных с соответствующим сетевым протоколом. В частности, модуль IP-EIGRP отвечает за выполнение описанных ниже функций.

- Отправка и получение информации протокола EIGRP, содержащей данные протокола IP.
- Уведомление алгоритма DUAL о получении новой информации, относящейся к IP-маршрутизации.

- Поддержка результатов принятых алгоритмом DUAL решений о маршрутизации в таблице IP-маршрутизации.
- Дальнейшее распространение информации о маршрутах, которая стала известной другим поддерживающим IP протоколам маршрутизации.

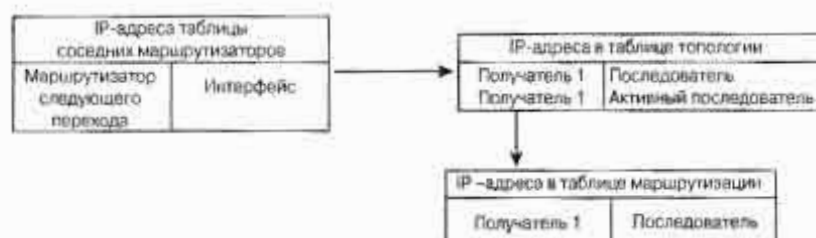


Рис. 4.7. Модули PDM протокола EIGRP

Типы пакетов протокола EIGRP

Как и протокол OSPF, EIGRP использует несколько различных типов пакетов для поддержки различных своих таблиц и установки сложных (комплексных) связей с соседними маршрутизаторами. Ниже описываются пять типов пакетов протокола EIGRP:

- пакеты приветствия (Hello);
- пакеты подтверждения (Acknowledgment);
- пакеты обновления маршрутов (Update);
- пакеты запросов (Query);
- пакеты ответов на запросы (Reply).

Пакеты приветствия

Протокол EIGRP использует пакеты приветствия для обнаружения соседних маршрутизаторов, их тестирования и повторного обнаружения после сбоев. Повторное обнаружение происходит в том случае, если маршрутизаторы не получают друг от друга пакетов приветствия в течение времени удержания, но позднее восстанавливают связь.

Маршрутизаторы EIGRP рассылают пакеты приветствия с фиксированным (задаваемым в файле конфигурации) интервалом, который называется интервалом рассылки приветствия (hello interval). Принимаемый по умолчанию интервал приветствия зависит от ширины полосы пропускания интерфейса, как показано в табл. 4.1.

Таблица 4.1 Интервалы рассылки приветствия

Ширина полосы пропускания	Тип канала	Интервал приветствия по умолчанию	Время удержания по умолчанию
1,544 Мбит/с или менее	Протокол Multipoint Frame Relay	60 секунд	180 секунд
Более 1,544 Мбит/с	Линия T1, соединения "точка-точка"	5 секунд	15 секунд

Для отправки пакетов приветствия протокол EIGRP использует многоадресатную рассылку. В сетях протокола IP маршрутизаторы EIGRP рассылают пакеты приветствия с использованием многоадресатной рассылки.

Маршрутизатор протокола EIGRP сохраняет информацию о соседних устройствах в соответствующей таблице, называемой таблицей соседних устройств. В этой таблице для каждого соседнего устройства имеется поле последовательного номера (Sequence Number — Seq No), в котором записывается номер последнего полученного от этого устройства пакета протокола EIGRP. В таблице соседних устройств также имеется поле времени удержания (Hold Time), в котором записано время получения последнего пакета. Для того, чтобы у соседнего маршрутизатора сохранялся статус пассивного (т.е. достижимого и работоспособного), необходимо, чтобы за время удержания от него поступил хотя бы один пакет.

Если же в течение времени удержания от него не поступило пакетов, то протокол EIGRP рассматривает этот соседний маршрутизатор как неработоспособный и алгоритм DUAL начинает пересчитывать таблицу маршрутизации. По умолчанию время удержания в три раза больше интервала приветствий, однако администратор может сконфигурировать оба таймера по своему желанию.

В протоколе OSPF для осуществления связи требуется, чтобы соседние маршрутизаторы имели одинаковые значения интервалов приветствия и блокировки. В протоколе EIGRP такое ограничение отсутствует. В нем соседние маршрутизаторы узнают об интервалах таймеров путем обмена пакетами приветствия. Эта информация используется для установки устойчивой связи несмотря на различные интервалы таймеров.

Пакеты приветствия всегда рассылаются методом негарантированной доставки и не требуют подтверждения.

Пакеты подтверждения

Маршрутизатор EIGRP использует пакеты подтверждения для уведомления других маршрутизаторов о получении им пакета EIGRP в течение сеанса "надежного" обмена данными. Надежный транспортный протокол может обеспечить надежную связь между узлами EIGRP. Для того, чтобы обеспечить гарантированную доставку принимающий узел должен подтвердить получение сообщения от узла-отправителя. Для этой цели используются пакеты подтверждения, которые можно назвать пакетами приветствия "без данных". В отличие от многоадресатных пакетов приветствия пакеты подтверждения являются одноадресатными и посылаются одному конкретному узлу. Подтверждение также может быть осуществлено путем совмещения передачи прямых и обратных пакетов других типов пакетов EIGRP, таких как пакеты ответов на запросы.

Пакеты обновлений маршрутов

Пакеты обновлений маршрутов используются в тех случаях, когда маршрутизатор обнаруживает новое соседнее устройство. В этих случаях маршрутизатор EIGRP посылает одноадресатные пакеты обновления маршрутов этому новому соседнему устройству для того, чтобы оно могло добавить эту информацию в свою топологическую таблицу. Для того, чтобы передать новому соседнему устройству всю топологическую информацию может потребоваться более одного пакета.

Пакеты обновления используются также в тех случаях, когда маршрутизатор обнаруживает изменение топологии сети. В этом случае маршрутизатор рассылает

многоадресатные пакеты обновления всем своим соседним устройствам, предупреждая их об изменении топологии.

Все пакеты обновления рассылаются методом гарантированной доставки.

Пакеты запросов и ответов на запросы

Маршрутизатор протокола EIGRP использует пакеты запросов каждый раз, когда ему требуется конкретная информация от какого-либо из своих соседних устройств. Пакет ответа используется для ответа на запрос.

Если у маршрутизатора EIGRP исчезает первичный маршрут и он не может найти резервного маршрута, то алгоритм DUAL переводит маршрут в активное состояние (Active state). После этого маршрутизатор выполняет многоадресатную рассылку запроса всем своим соседям для нахождения первичного маршрута к сети получателя. Соседние устройства должны послать ответы на запросы, в которых либо предоставляется информация о первичном маршруте, либо сообщается об отсутствии у них такой информации.

Запросы могут быть как много- так и одноадресатными, в то время как ответы на запросы всегда являются одноадресатными. Оба типа пакетов рассылаются методом гарантированной доставки.

Конвергенция протокола EIGRP

Алгоритм DUAL обеспечивает исключительно быструю конвергенцию (сходимость) протокола EIGRP. Для того, чтобы лучше понять процесс конвергенции с использованием алгоритма DUAL, рассмотрим схему, показанную на рис. 4.8. Маршрутизатор RTA может получить доступ к сети 24 через три различных маршрутизатора: RTX, RTY или RTZ.

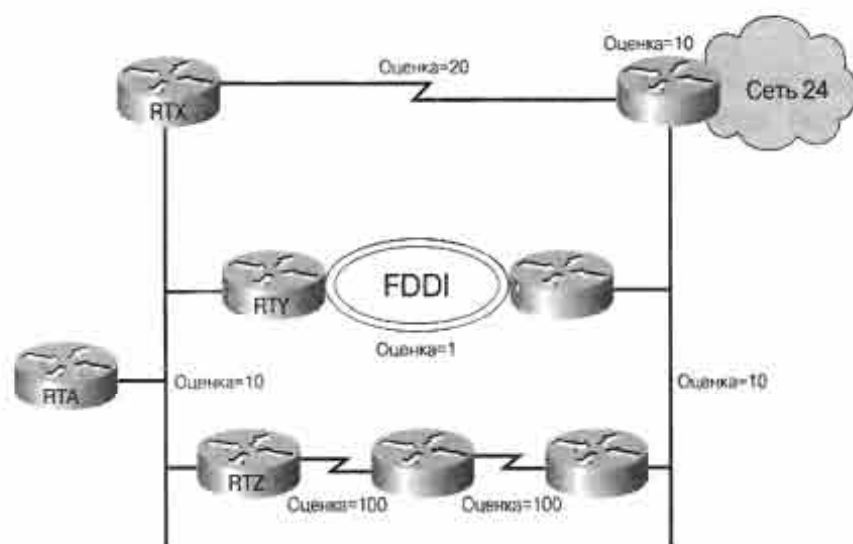


Рис. 4.8. Конвергенция протокола EIGRP

На рис. 4.8 для упрощения вычислений композитная метрика протокола EIGRP заменена оценкой для канала. Топологическая таблица маршрутизатора RTA включает в себя список всех маршрутов, анонсированных соседними с ним устройствами. Как по-

казано в табл. 4.2, маршрутизатор RTA хранит для каждой сети реальную (вычисленную) оценку доступа к этой сети, а также анонсированную оценку (сообщенное расстояние) от своего соседнего устройства, как показано в табл. 4.2.

Таблица 4.2 Композитная метрика

Соседнее устройство	Вычисленная оценка маршрута к сети Network 24	Сообщенное расстояние до сети Network 24
RTY	31	21
RTZ	230	220
RTX	40	30

Сначала RTY является первичным маршрутом к сети 24, поскольку имеет меньшую чем у других вычисленную оценку. Наименьшая вычисленная метрика RTA к сети 24 равна 31; это значение представляет собой предполагаемое расстояние FD к сети 24.

Для выбора резервного маршрута, который бы стал первичным маршрутом к сети 24 маршрутизатор RTA выполняет состоящий из трех этапов процесс, описанный ниже.

Этап 1. Определяется, какие соседние устройства имеют расстояние RD к сети 24, которое меньше расстояния FD RTA к сети 24. Это расстояние FD равно 31; RD RTX равно 30, а RD RTZ равно 220 (см. табл. 4-2). Таким образом, RD RTX меньше текущего FD, в то время как RD RTZ больше текущего FD.

Этап 2. Определяется минимальная вычисленная оценка к сети 24 из оставшихся доступных маршрутов. Вычисленная оценка маршрута через RTX равна 40, в то время как вычисленная оценка через RTZ равна 230. Таким образом, RTX обеспечивает наименьшую вычисленную оценку.

Этап 3. Определяется, удовлетворяют ли маршрутизаторы удовлетворяющие критериям этапа 1, также и критериям этапа 2. Маршрутизатор RTX удовлетворяет и тем, и другим, поэтому он является резервным маршрутом.

Если маршрутизатор RTY становится неработоспособным, то маршрутизатор RTA немедленно переходит к использованию маршрутизатора RTX (резервного маршрута) для пересылки пакетов в сеть 24. Способность осуществлять немедленное переключение на резервный маршрут является основной предпосылкой исключительно быстрой конвергенции протокола EIGRP.

Может ли RTZ быть резервным маршрутом? Используя описанный выше трех-этапный процесс, RTA выясняет, что RTZ анонсирует оценку 220, которая не меньше, чем расстояние FD RTA, равное 31. Следовательно, RTZ пока не может быть резервным маршрутом (пока еще). Расстояние FD может измениться только во время перехода из активного в пассивное состояние, а этот переход пока еще не произошел, поэтому это расстояние остается равным 31. До этого момента, поскольку для сети 24 еще не произошел переход в активное состояние, алгоритм DUAL осуществляет процесс, называемый *локальным вычислением (local computation)*.

Маршрутизатор RTA не может найти резервных маршрутов, поэтому он в конечном итоге переходит от пассивного к активному состоянию для сети 24 и запрашивает свои соседние устройства об этой сети. Этот процесс называется *вычислением диффузии (diffusing computation)*. При переходе сети 24 в активное состояние это расстояние FD переустанавливается. Это позволяет RTA в конечном итоге принять RTZ в качестве первичного маршрута к сети 24.

Конфигурирование протокола EIGRP

В настоящем разделе рассматриваются базовые процедуры конфигурирования протокола EIGRP. Особое внимание уделяется способам, какими протокол EIGRP устанавливает связи со смежными маршрутизаторами, вычисляет первичные и запасные маршруты и при необходимости реагирует на сбои в известных маршрутах к конкретным пунктам назначения.

Конфигурирование протокола EIGRP для IP

Несмотря на сложность алгоритма DUAL, конфигурирование протокола EIGRP может оказаться относительно простым. Команды конфигурирования протокола EIGRP различаются в зависимости от сетевого протокола, для которого он конфигурируется. В настоящем разделе описывается конфигурирование EIGRP для протокола IP. Этот процесс проиллюстрирован на рис. 4.9.

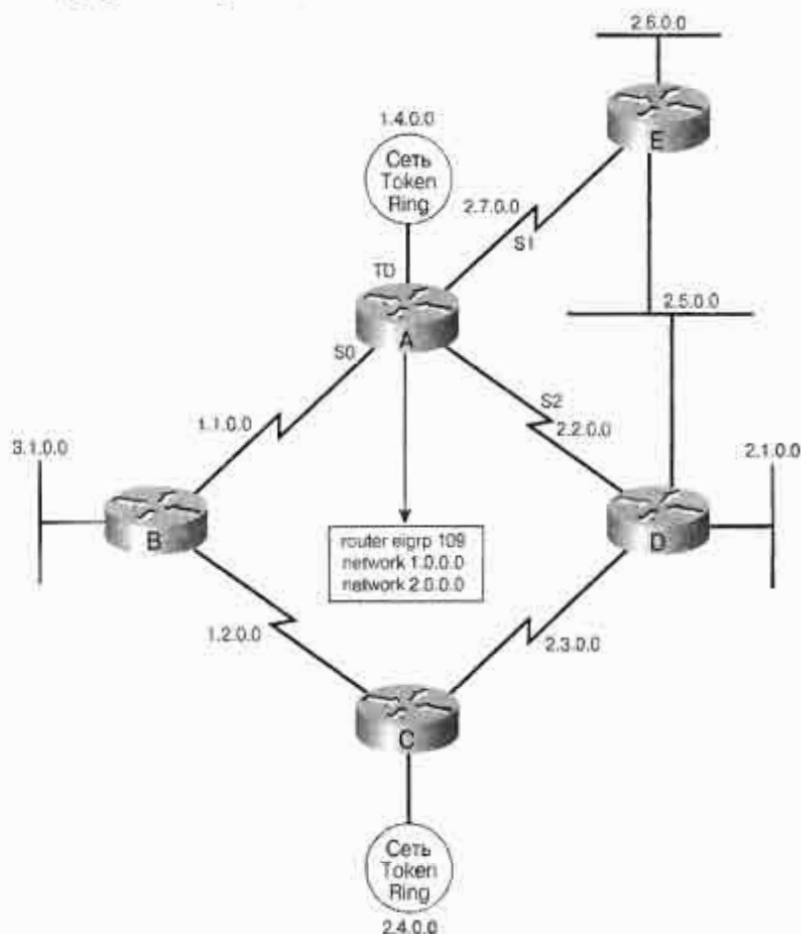


Рис. 4.9. Конфигурирование EIGRP для протокола IP

Для того, чтобы сконфигурировать EIGRP для протокола IP следует выполнить описанные ниже этапы.

Этап 1. Для включения протокола EIGRP и определения автономной системы следует выполнить команду:

```
router(config)# router eigrp autonomous-system-number
```

В этой команде параметр *autonomous-system-number* представляет собой номер, идентифицирующий уникальную автономную систему. Он указывает на все маршрутизаторы, принадлежащие к данной объединенной сети. Это значение должно соответствовать всем маршрутизаторам в этой объединенной сети.

- Этап 2.** Указать, какие сети принадлежат к данной автономной системе EIGRP на локальном маршрутизаторе с помощью следующей команды:

```
router(config-router)# network network-number
```

Параметр *network-number* представляет собой номер сети, какие интерфейсы данного маршрутизатора участвуют в работе протокола EIGRP и какие сети анонсируются этим маршрутизатором. Номер сети вводится с учетом класса IP-адреса. Например, сети 2.2.0.0 и 2.7.0.0 вводятся с использованием команды **network**, как описано ниже.

```
Router_A(config-router)#network 2.0.0.0
```

Команда **network** конфигурирует только подсоединенные сети. Например, сеть 3.1.0.0 (на рис. 4.9 крайняя слева) не является непосредственно подсоединенной к маршрутизатору Router A. Следовательно эта сеть не является частью конфигурации маршрутизатора Router A.

- Этап 3.** При конфигурировании последовательных каналов, использующих протокол EIGRP важно задать полосу пропускания на данном интерфейсе. Если полоса пропускания для таких интерфейсов не изменена, то протокол EIGRP принимает для полосы пропускания значение по умолчанию для канала вместо истинной ширины полосы пропускания. Если канал имеет меньшую скорость, то маршрутизатор может оказаться не в состоянии выполнить конвергенцию, либо может произойти потеря изменений маршрутизации или выбран неоптимальный маршрут. Значение полосы пропускания конфигурируется с помощью команды:

```
router(config-if)# bandwidth kilobits
```

Команда для задания полосы пропускания является ЕДИНСТВЕННОЙ, которая используется в процессе маршрутизации и должна быть установлена в соответствии со скоростью канала для данного интерфейса.

- Этап 4.** Cisco также рекомендует добавлять в конфигурацию каждого маршрутизатора EIGRP следующую команду:

```
router(config-if)# igrp log-neighbor-changes
```

Эта команда позволяет записать в системный журнал перемены в состояниях смежности (соседних устройств) для анализа устойчивости системы маршрутизации и помогает обнаруживать возникающие проблемы.



Лабораторная работа: конфигурирование протокола EIGRP

В этой лабораторной работе требуется сконфигурировать протокол EIGRP на двух маршрутизаторах и протестировать соединение с помощью команды **ping**.

Конфигурирование полосы пропускания в сетях NBMA

При проектировании протокола EIGRP в среде нешироковещательной сети множественного доступа (nonbroadcast multiaccess — NBMA), такой как сеть протокола Frame Relay, необходимо придерживаться следующих трех правил:

- Скорость передачи данных протокола EIGRP не должна превышать согласованной скорости передачи информации (committed information rate — CIR) виртуального канала (virtual circuit — VC);
- Агрегированный (совокупный) объем данных протокола EIGRP по всем виртуальным каналам не должен превышать скорость канала на интерфейсе;
- Полоса пропускания, выделенная протоколу EIGRP на каждом канале VC должна быть одной и той же в обоих направлениях.

При правильном понимании этих правил и следовании им протокол EIGRP эффективно работает в среде распределенной сети WAN. Если при конфигурировании протокола EIGRP в сети WAN не приняты соответствующие меры предосторожности, то потоки данных EIGRP могут вызвать в сети переполнение.

Конфигурирование полосы пропускания в многоточечной сети

Задание в конфигурации команды **bandwidth** в среде NBMA зависит от того, как спроектированы виртуальные каналы VC. Если в многоточечной конфигурации последовательный канал имеет много каналов VC и все эти каналы равномерно совместно используют полосу пропускания, то в команде **bandwidth** должна быть задана полоса пропускания, равная сумме всех скоростей CIR. Например, в сети на рис. 4.10 скорость CIR каждого канала VC установлена равной 56 Кбит/с и, поскольку имеется 4 канала VC, полоса пропускания должна быть установлена равной 224 (4 x 56).

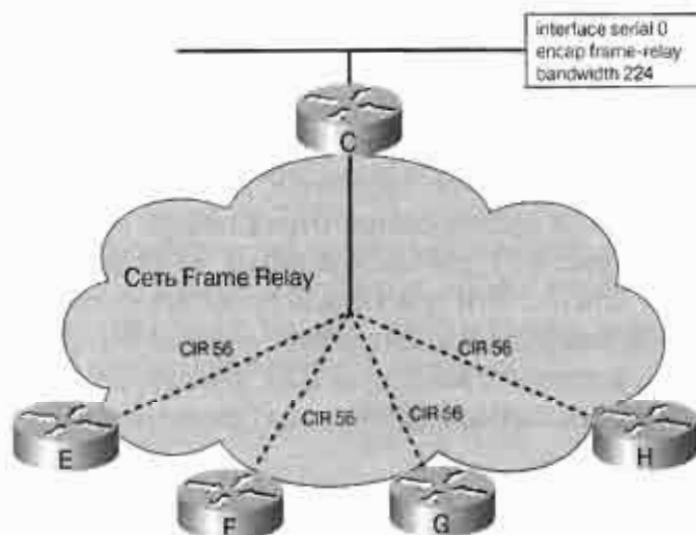


Рис. 4.10. Конфигурирование протокола EIGRP в многоточечной среде сети WAN

Конфигурирование полосы пропускания в гибридной многоточечной сети

Если в многоточечной сети каналы VC имеют разные скорости передачи, то требуется более сложное конфигурирование. При этом могут быть применены два основных подхода, описанные ниже.

- **Выбрать наименьшую для всех каналов скорость CIR и умножить ее на количество виртуальных каналов VC**—Как показано на рис. 4.11, такой подход применен к физическому интерфейсу. Недостаток такого подхода состоит в том, что каналы с большой полосы пропускания могут оказаться недозагруженными.

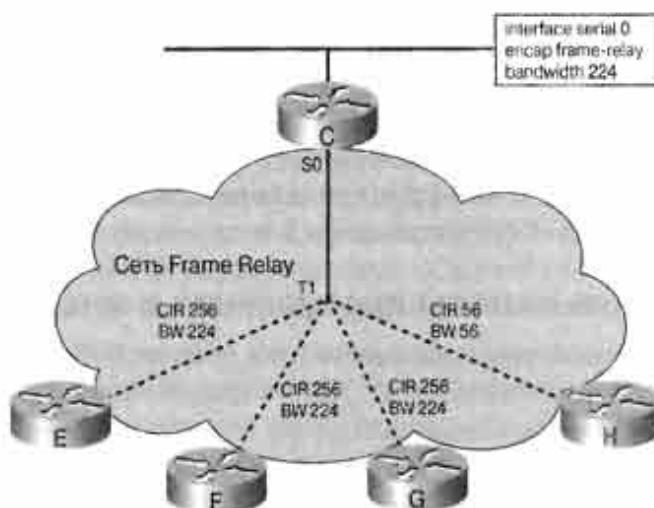


Рис. 4.11. Конфигурирование протокола EIGRP в среде многоточечной гибридной сети WAN

- **Использование подынтерфейсов**—Команда **bandwidth** может быть сконфигурирована на каждом подынтерфейсе, что позволяет использовать разные скорости на каждом канале VC. В этом случае подынтерфейсы конфигурируются для каналов с различающимися скоростями CIR. Каналы, имеющие одну и ту же сконфигурированную скорость CIR представляются как единый подынтерфейс с полосой пропускания, отражающей совокупную скорость CIR всех каналов. На рис. 4.12 три виртуальных канала VC имеют одинаковую CIR, равную 256 Кбит/с. Эти три канала группируются вместе как один многоточечный последовательный интерфейс — serial 0.1. Единственный остающийся канал VC, имеющий меньшую CIR, равную 56, может быть определен как последовательный подынтерфейс типа “точка-точка” — serial 0.2.

Использование команды **ip bandwidth-percent**

Команда **ip bandwidth-percent** задает в процентном отношении часть полосы пропускания, которую протокол EIGRP может использовать на каком-либо интерфейсе. По умолчанию протокол EIGRP может использовать до 50% полосы пропускания интерфейса для обмена информацией маршрутизации. При вычислении этой процентной части команда **ip bandwidth-percent** использует значение, установленное командой **bandwidth**.

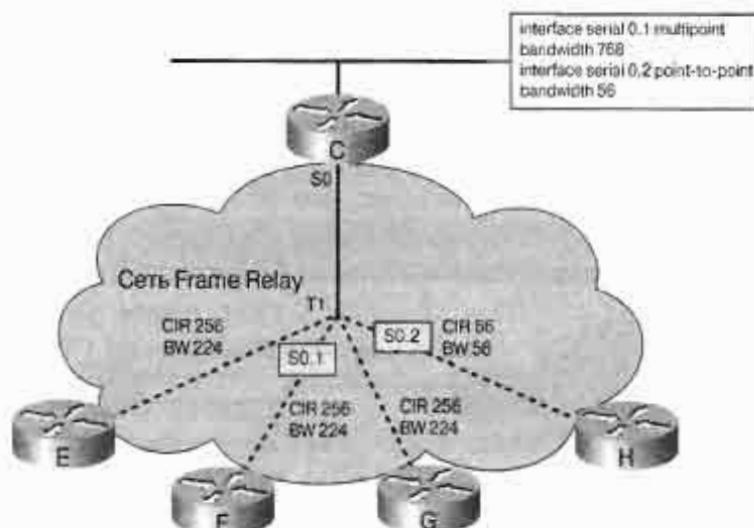


Рис. 4.12. Конфигурирование протокола EIGRP в гибридной многоточечной среде сети WAN (предпочтительный вариант)

Команду **ip bandwidth-percent** следует использовать в тех случаях, когда установленная для канала полоса пропускания не соответствует его истинной скорости. Значение полосы пропускания может быть искусственно занижено по различным причинам, в частности, для управления метрикой маршрутизации или для того, чтобы отрегулировать избыточную нагрузку в многоточечной конфигурации протокола Frame Relay. Независимо от причины занижения, следует сконфигурировать EIGRP таким образом, чтобы заменить искусственно заниженную установку полосы пропускания на более высокое значение с помощью команды **ip bandwidth-percent**. В некоторых случаях значение, задаваемое этой командой, может даже превышать 100%.

Например, предположим, что реальная полоса пропускания последовательного канала маршрутизатора равна 64 Кбит/с, однако ее значение искусственно занижено и установлено равным 32 Кбит/с. На рис. 4.13 показано как следует изменить поведение протокола EIGRP таким образом, чтобы он ограничивал объем потоков данных протокола маршрутизации реальной полосой пропускания последовательного интерфейса. В приведенном примере конфигурации для процесса EIGRP, функционирующего для автономной системы 24, полоса пропускания в процентах для последовательного интерфейса serial 0 устанавливается равной 100%. Поскольку 100% от 32 Кбит/с равно 32 Кбит/с, протоколу EIGRP предоставляется возможность использовать половину реальной полосы пропускания, равной 64 Кбит/с. Более подробно эта ситуация проиллюстрирована на рис. 4.13.

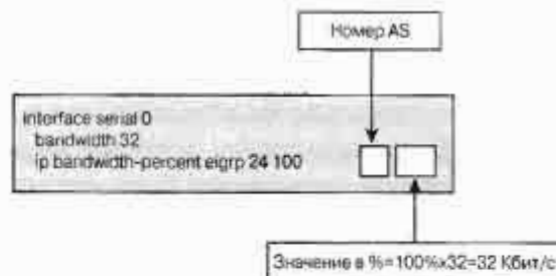


Рис. 4.13. Применение команды **ip bandwidth-percent** в протоколе EIGRP

Конфигурирование обобщения маршрутов протокола EIGRP

Протокол EIGRP автоматически обобщает маршруты на границе сети, использующей IP-адреса с классами (т.е. на границе сети, в которой сетевой адрес включает в себя класс адреса). Это означает, что, несмотря на то, что маршрутизатор RTC подсоединен только к подсети 2.1.1.0, он объявляет, что он подсоединен ко всей сети 2.0.0.0 класса A. В большинстве случаев автоматическое обобщение полезно, поскольку позволяет сделать таблицы маршрутизации максимально компактными (рис. 4.14).



Рис. 4.14. Автоматическое обобщение маршрутов протокола EIGRP

Однако в некоторых обстоятельствах автоматическое обобщение может оказаться нежелательным. Если в сети есть подсети, не являющиеся непрерывными, как, например, в сети, показанной на рис. 4.15, то для правильной работы механизма маршрутизации автоматическое обобщение следует отключить.

Для отключения автоматического обобщения используются следующая команда:

```
router(config-router)#no auto-summary
```

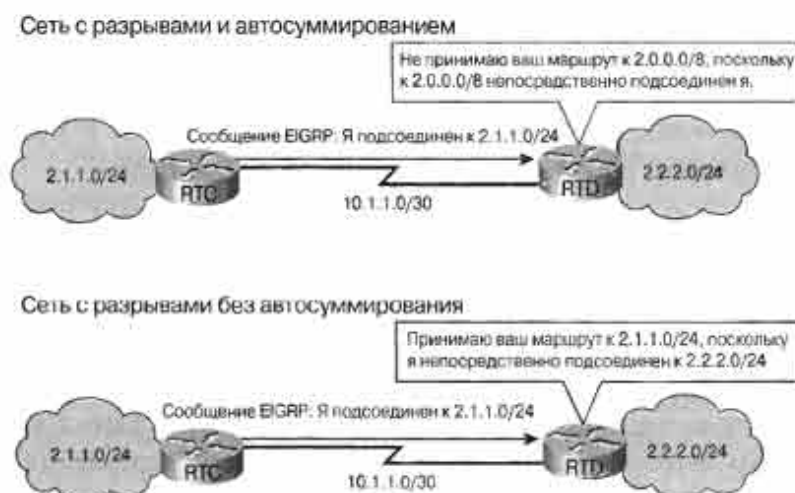


Рис. 4.15. Основанное на использовании классов автоматическое обобщение протокола EIGRP

При использовании протокола EIGRP можно вручную сконфигурировать префикс, который будет использоваться в качестве обобщенного адреса. Ручное конфигурирование обобщения маршрутов осуществляется отдельно для каждого интерфейса, поэтому первым должен быть выбран интерфейс, который распространяет обобщение маршрутов. После этого обобщенный адрес может быть определен с помощью команды **ip summary-address eigrp**, синтаксис которой приводится ниже.

```
router(config-if)#ip summary-address eigrp autonomous-system-number  
ip-address mask administrative-distance
```


Обобщенные маршруты протокола EIGRP по умолчанию имеют административное расстояние равное 5. Однако оно может быть изменено при конфигурировании на любое значение из диапазона от 1 до 255.

Маршрутизатор RTC, показанный на рис. 4.15, может быть сконфигурирован с использованием команд, приведенных в примере 4.4.

Пример 4.4. Ручное обобщение маршрутов

```
RTC(config)#router eigrp 2446
RTC(config-router)#no auto-summary
RTC(config-router)#exit
RTC(config)#interface serial0
RTC(config-if)#ip summary-address eigrp 2446 2.1.0.0 255.255.0.0
Thus, RTC will add a route to its table, as follows:
D 2.1.0.0/16 is a summary, 00:00:22, Null0
```

Обобщенный маршрут имеет в качестве источника Null0, а не реальный интерфейс. Это объясняется тем, что этот маршрут используется только для целей анонсирования и не представляет маршрута, который маршрутизатор RTC может избрать для достижения этой сети. В RTC этот маршрут имеет административное расстояние равное 5.

Для маршрутизатора RTD на рис. 4.15, обобщение маршрутов не имеет значения, однако он принимает этот маршрут и назначает ему административное расстояние “нормального” маршрута EIGRP (которое по умолчанию равно 90). В конфигурации для RTC автоматическое обобщение маршрутов отключено командой **no auto-summary**. Если бы автоматическое обобщение маршрутов не было отключено, то маршрутизатор RTD получил бы два маршрута: сконфигурированный вручную обобщенный адрес (2.1.0.0/16) и автоматически назначенный, использующий классы адрес (2.0.0.0/8). В большинстве случаев при ручном обобщении следует использовать команду **no auto-summary**.

Тестирование базовой конфигурации протокола EIGRP

Для тестирования работы протокола EIGRP могут быть использованы разнообразные команды **show**. В табл. 4.3 приведены основные варианты команды **show** для протокола EIGRP и кратко описаны их функции.

Таблица 4.3. Основные команды Show протокола EIGRP

Команда	Описание
show ip eigrp neighbors [<i>type number</i>] [<i>details</i>]	Отображает таблицу соседних устройств протокола EIGRP. Опции <i>type</i> и <i>number</i> используются для указания интерфейса. Ключевое слово details расширяет вывод
show ip eigrp interfaces [<i>type number</i>] [<i>as-number</i>] [<i>details</i>]	Отображает информацию протокола EIGRP для каждого интерфейса. Необязательные ключевые слова ограничивают вывод конкретным интерфейсом или автономно системой. Ключевое слово details расширяет вывод

Окончание табл. 4.3

Команда	Описание
<code>show ip eigrp topology [as-number] [ip-address] mask]</code>	Отображает все допустимые резервные маршруты топологической таблицы протокола EIGRP. Необязательные ключевые слова могут использоваться для фильтрации вывода на основе номера автономной системы или конкретного сетевого адреса
<code>show ip eigrp topology [active pending zero-successors]</code>	В зависимости от использованного ключевого слова отображает все маршруты в топологической таблице, которые являются активными, готовятся к пересчету, или не имеют первичных маршрутов
<code>show ip eigrp topology all-links</code>	Отображает не только резервные маршруты, но и все маршруты топологии сети протокола EIGRP
<code>Show ip eigrp traffic [as-number]</code>	Отображает число отправленных и полученных пакетов протокола EIGRP. Вывод команды может быть отфильтрован путем задания необязательного номера автономно системы.

Функция IOS Cisco **debug** также предоставляет полезные команды мониторинга протокола EIGRP, перечисленные в табл. 4.4.

Таблица 4.4. Основные команды отладки протокола EIGRP

Команда	Описание
<code>debug eigrp fsm</code>	Эта команда позволяет наблюдать работу резервного маршрута протокола EIGRP и проверить, что процесс маршрутизации устанавливает и удаляет обновления маршрутов
<code>debug eigrp packet</code>	Вывод по этой команде отображает передачу и получение пакетов протокола EIGRP. Этими пакетами могут быть пакеты приветствия, обновления маршрутов, запроса или ответа на запрос. В выводе отображаются последовательные номера и номера подтверждений, используемые алгоритмом надежной транспортировки протокола EIGRP

Лабораторная работа: тестирование базовой конфигурации протокола IGRP

В этой лабораторной работе требуется сконфигурировать протокол EIGRP на двух маршрутизаторах и протестировать установки, используя команду **ping** и другие команды протокола IGRP.

Резюме

В данной главе были рассмотрены приведенные ниже основные вопросы.

- Протокол EIGRP является фирменным протоколом Cisco, который базируется на протоколе IGRP.
- Протокол EIGRP обеспечивает быструю сходимость, повышенную масштабируемость и эффективную обработку петель маршрутизации.
- Протокол EIGRP может заменить протоколы RIP Novell и RTMP AppleTalk, обеспечивая повышенную эффективность работы сетей IPX и AppleTalk.

- Протокол EIGRP представляет собой усовершенствованный дистанционно-векторный протокол маршрутизации, использующий функции, которые обычно ассоциируются с протоколами маршрутизации по состоянию канала. Этот протокол также использует некоторые лучшие функции протокола OSPF, такие как частичные обновления и обнаружение соседних устройств.
- Протокол EIGRP является идеальным решением для крупных многопротокольных сетей, построенных преимущественно на маршрутизаторах Cisco.
- В этой главе также описаны действия и команды, которые используются для конфигурирования, тестирования и устранения ошибок в сетях протокола EIGRP.

В дополнение к уже изученному материалу данной главы рекомендуется ознакомиться с лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

Алгоритм диффузии (распространения) обновлений маршрутов (Diffusing Update Algorithm — DUAL). Алгоритм обеспечения конвергенции, используемый усовершенствованным протоколом IGRP (Enhanced IGRP), который в любой момент обеспечивает отсутствие петель в сети путем вычисления маршрутов. Алгоритм DUAL позволяет маршрутизаторам, участвующим в изменении топологии, синхронизироваться одновременно, не затрагивая при этом другие маршрутизаторы, на которые происходящее в сети изменение не влияет.

Вероятное расстояние (feasible distance — FD). Наименьшее вычисленное значение метрики к пункту назначения.

Задержка (delay). Промежуток времени между началом какого-либо действия отправителем и первым ответом, который он получает. Задержкой также называется время, требуемое пакету для перемещения от источника к пункту назначения по заданному маршруту.

Застывание маршрута (stuck in active). Этим термином описывается состояние маршрутизатора в том случае, если от одного или более маршрутизаторов, которым был послан запрос, не поступает ответа в течение активного времени, равного 180 секунд (3 минуты).

Надежный транспортный протокол (Reliable Transport Protocol). Протокол транспортного уровня, который может гарантировать упорядоченную доставку пакетов протокола EIGRP всем соседним устройствам.

Первичный маршрут (successor). Маршрут, выбранный в качестве основного для достижения какого-либо пункта назначения.

Потенциально первичный маршрут (feasible successor — FS). Резервный маршрут. Такие маршруты идентифицируются одновременно с первичными, однако хранятся только в топологической таблице.

Сообщенное расстояние (reported distance — RD). Расстояние, которое смежное соседнее устройство сообщает конкретному получателю.

Таблица соседних устройств (neighbor table). Таблица, используемая маршрутизаторами EIGRP для поддержки списка соседних маршрутизаторов. Таблица соседних устройств создается для каждого протокола, который поддерживается протоколом EIGRP.

Топологическая таблица (topology table). Таблица маршрутов, создаваемая на основе всех таблиц маршрутизации протокола EIGRP в автономной системе и предоставляющая маршрутизаторам информацию обо всех маршрутах к получателям в автономной системе.

Контрольные вопросы

1. Как сконфигурировать автоматическое перераспределение маршрутов между протоколами IGRP и EIGRP?
 - A. Сконфигурировать оба протокола с разными номерами автономных систем.
 - B. Сконфигурировать оба протокола с разными DS-номерами.
 - C. Сконфигурировать оба протокола с одинаковыми номерами автономных систем.
 - D. Сконфигурировать оба протокола с одинаковыми DS-номерами.
2. Какой из приведенных ниже протоколов сочетает в себе преимущества протоколов маршрутизации по состоянию канала и дистанционно-векторных протоколов?
 - A. RIP
 - B. OSPF
 - C. IGRP
 - D. EIGRP
3. Какой из приведенных ниже алгоритмов используется для достижения быстрой конвергенции?
 - A. Алгоритм Дейкстры (Dijkstra)
 - B. Алгоритм диффузии обновлений маршрутизации (Diffusing Update)
 - C. Алгоритм конвергенции (Convergence algorithm)
 - D. Алгоритм конвергенции DUAL
4. Какой из приведенных ниже протоколов поддерживается протоколом EIGRP с помощью модулей PDM?
 - A. IS-IS
 - B. SNMP
 - C. IPX
 - D. DHCP
5. Какая из приведенных ниже таблиц включает в себя позиции маршрутов для всех пунктов назначения, известных маршрутизатору, и поддерживается для каждого сконфигурированного протокола маршрутизации?
 - A. Топологическая таблица
 - B. Таблица маршрутизации
 - C. Таблица соседних устройств
 - D. Таблица первичных маршрутов

6. Какой из перечисленных ниже объектов устанавливает отношения смежности в протоколе EIGRP?
 - A. Машина конечных состояний (finite-state machine) алгоритма DUAL
 - B. Пакеты приветствия
 - C. Топологическая таблица
 - D. Надежный транспортный протокол (Reliable Transport Protocol)
7. Что из нижеперечисленного гарантирует упорядоченную доставку пакетов EIGRP всем соседним устройствам?
 - A. Машина конечного состояния (finite-state machine) алгоритма DUAL
 - B. Пакеты приветствия
 - C. Топологическая таблица
 - D. Надежный транспортный протокол (Reliable Transport Protocol)
8. Что делает алгоритм DUAL после того, как он выяснит все маршруты, сравнит их друг с другом и убедится, что они свободны от петель?
 - A. Заносит в таблицу маршрутизации до четырех маршрутов с наименьшими оценками
 - B. Определяет оптимальный маршрут и анонсирует его своим соседним устройствам с помощью пакетов приветствия
 - C. Поддерживает другие сетевые протоколы с помощью модулей PDM
 - D. Рассылает одноадресатные запросы соседним маршрутизаторам
9. Каким образом протокол EIGRP предотвращает образование петель маршрутизации через внешние маршруты?
 - A. Путем отказа от внешних маршрутов, которые помечены идентификатором маршрутизатора ID, совпадающим с их собственным
 - B. Путем сохранения идентификационных данных соседних устройств, являющихся потенциально первичными
 - C. Путем отказа от маршрутов ко всем соседним маршрутизаторам, которые имеют анонсированную композитную метрику, меньшую чем наилучшая текущая метрика маршрутизатора
 - D. Путем сохранения всех маршрутов соседних маршрутизаторов, которые имеют идентифицированные петли в своих таблицах маршрутизации
10. Какой интервал рассылки приветствий используется протоколом EIGRP в соединениях с большой полосой пропускания, таких как последовательные каналы типа "точка-точка" или многоточечные каналы?
 - A. 5 секунд
 - B. 10 секунд
 - C. 60 секунд
 - D. 120 секунд



В этой главе...

- Описаны локальные сети (LAN) спецификации Ethernet/802.3
- Рассмотрены различные типы коммутации в локальных сетях
- Рассмотрены принципы проектирования локальных сетей
- Описаны основные процессы, происходящие при коммутации на 2-м уровне при использовании мостов и коммутаторов

Коммутация в локальных сетях и проектирование локальных сетей

В настоящее время при проектировании новых сетей все реже используются мосты и концентраторы, а в первую очередь используются *коммутаторы* и *маршрутизаторы*.

В настоящей главе обсуждаются возможные проблемы локальных сетей и предлагаются решения, которые могут повысить их производительность. Описано такое явление как *переполнение (congestion)*, его воздействие на производительность сети и преимущества сегментации сети. Кроме того рассматриваются достоинства и недостатки использования мостов, коммутаторов и маршрутизаторов с целью сегментации LAN и влияние этих устройств на пропускную способность сети. Приводятся основные требования к проектированию локальных сетей, цели проектирования и факторы, влияющие на эффективность проектируемой сети. В заключение рассматриваются достоинства таких технологий коммутации, как *Ethernet*, *Fast Ethernet*, *Gigabit Ethernet* и применение виртуальных локальных сетей VLAN при проектировании LAN. Рекомендуется ознакомиться с лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Локальные сети спецификации Ethernet/802.3

Наиболее часто используемой структурой локальной сети LAN является Ethernet. Эта технология используется для передачи данных между сетевыми устройствами, такими как компьютеры, принтеры и файловые серверы.

История развития сетей Ethernet/802.3

С момента начала широкого использования технологий сетей LAN они базировались на шинной топологии и использовали кабельные инфраструктуры толстого (thick) или тонкого (thin) Ethernet. Для лучшего понимания современного состояния коммутации в локальных сетях важно понять некоторые ограничения этих первоначальных вариантов технологии Ethernet. Ниже приводятся основные характеристики технологии толстого Ethernet.

- Ограничение длины сегмента расстоянием 500 метров, вызываемое ослаблением и ухудшением качества сигнала.
- Необходимость в связи с вышеупомянутым в использовании *повторителей (repeater)* через каждые 500 метров.
- Ограничения на количество и расположение рабочих станций.
- Большие расходы и технические трудности при проводке кабелей через здания.
- Относительная простота добавления новых пользователей.
- Совместное использование полосы пропускания 10 Мбит/с.
- Недостаточно надежные соединения или обрыв общей шины полностью прекращают связь в сети LAN.

Тонкий Ethernet характеризуется следующими особенностями.

- Требуется меньших финансовых затрат и пространства, чем толстый Ethernet.
- Добавление новых пользователей прерывает работу сети.
- Совместное использование полосы пропускания 10 Мбит/с.
- Недостаточно надежные соединения или обрыв общей шины полностью прекращают связь в сети LAN.

Добавление таких устройств, как концентраторы (хабы) внесло улучшение в технологии толстого и тонкого Ethernet. Концентратор представляет собой устройство 1-го уровня и иногда называется многопортовым повторителем. Введение в сети концентраторов позволяет обеспечить доступ к сети большему количеству пользователей. Активные концентраторы, усиливающие сигнал, также позволяют увеличить протяженность сети, как показано на рис. 5.1. При получении сигналов данных концентратор не принимает решений, а лишь регенерирует и усиливает сигналы, которые он получает от подсоединенных к нему устройств. В сетях с шинной топологией ненадежное подсоединение одной рабочей станции или обрыв кабеля в любом месте может вывести сеть LAN из строя. В новых Ethernet-технологиях, использующих концентраторы или коммутаторы, обрыв кабеля соединения одного пользователя не влияет на работу других пользователей этой сети. С другой стороны, сам концентратор или коммутатор может стать причиной неработоспособности сети. Ethernet по своей природе является технологией совместного использования, в которой все пользователи претендуют на одну и ту же полосу пропускания, как показано на рис. 5.2. Эту ситуацию можно сравнить с положением на автодороге, когда несколько автомобилей пытаются одновременно занять одну и ту же полосу движения. Поскольку дорога имеет только одну полосу, в каждый момент на нее может выехать только один автомобиль. Введение в сеть концентратора приводит к тому, что большее количество пользователей претендуют на одну и ту же полосу пропускания.

Концентратор решает многие из этих проблем

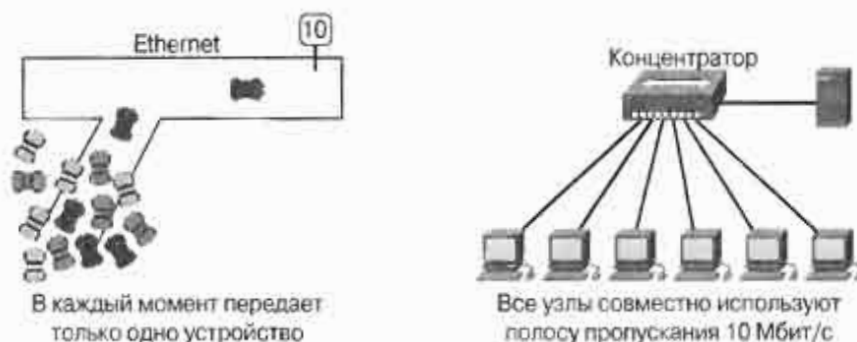


Рис. 5.1. Концентраторы

Коллизии являются неизбежным побочным продуктом Ethernet-технологий. Коллизия возникает в том случае, когда два или более устройств одновременно пытаются осуществить передачу данных. Эту ситуацию можно сравнить с въездом двух автомобилей на одну и ту же полосу движения, в результате чего происходит столкновение. В результате движение на дороге приходится останавливать до ликвидации результатов столкновения. Если количество коллизий в сети превышает некоторый уровень, то сеть практически перестает отвечать на запросы пользователей, что свидетельствует о том, что произошло переполнение или слишком много пользователей пытаются одновременно получить к ней доступ. Устройства 1-го уровня, такие как повторители и концентраторы, лишь усиливают сигнал, что позволяет реализовать сети большей протяженности. Устройства 2-го уровня способны осуществлять более интеллектуальные операции, чем устройства 1-го уровня. Устройства 2-го уровня принимают решения о пересылке данных основываясь на адресах управления доступом к передающей среде (*Media Access Control — MAC*), содержащихся в заголовках фреймов передаваемых данных.

Коллизии: аналогии из жизни



Рис. 5.2. Коллизии

Мост представляет собой устройство 2-го уровня, используемое для разделения (сегментации) сети и способное собирать и выборочно передавать фреймы данных от одного сетевого сегмента к другому. Эти функции мосты выполняют путем изучения MAC-адресов всех устройств в подсоединенных к мосту сегментах. Используя эту информацию мосты строят адресные таблицы и пересылают или блокируют передачу данных на основе этих таблиц. Таким путем уменьшается размер *коллизийных доменов (collision domain)* и повышается эффективность работы сети. Мосты не ограничивают широковещания, однако обеспечивают больший контроль над работой сети и уменьшают количество коллизий.

Коммутатор также является устройством 2-го уровня и может рассматриваться как многопортовый мост. Как показано на рис. 5.3, коммутатор помогает уменьшить количество коллизий в сети путем более эффективного контроля потоков данных. Коммутатор может принимать интеллектуальные решения на основе MAC-адресов устройств, содержащихся в передаваемых фреймах данных. Как и другие устройства 2-го уровня, коммутатор изучает MAC-адреса устройств всех сегментов, подсоединенных к его портам; эта информация заносится в таблицу коммутации, находящуюся в адресуемой по содержимому памяти (*content-addressable memory — CAM*).

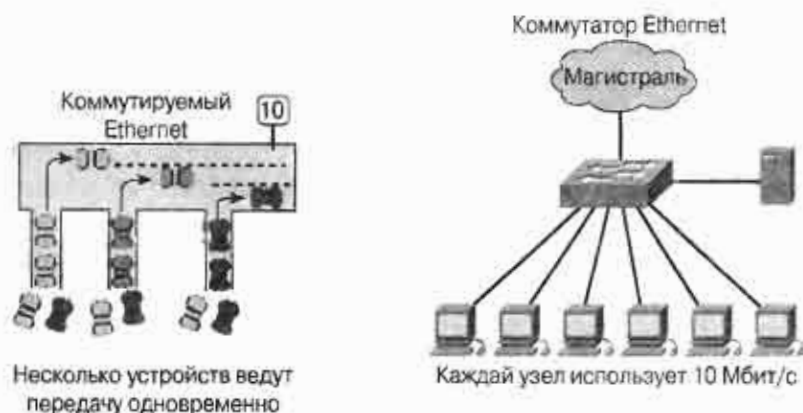


Рис. 5.3. Коммутаторы 2-го уровня

После создания между двумя устройствами виртуального канала между ними устанавливается предназначенный только для них коммуникационный канал. Использование в сети коммутатора приводит к *микросегментации (microsegmentation)* сети. Теоретически это создает свободную от коллизий среду между отправителем и получателем, что позволяет в максимальной степени использовать доступную полосу пропускания. Использование коммутатора также облегчает одновременное создание нескольких виртуальных каналов связи. Это можно сравнить с разделением дорожного пространства на несколько полос, при котором каждому автомобилю выделяется отдельная полоса. На рис. 5.4 показаны различия между концентратором 1-го уровня и коммутатором 2-го уровня. Недостатком устройств 2-го уровня является их неспособность останавливать *широковещание (broadcast)*, при котором фреймы направляются всем устройствам сети. В случае когда широковещание превышает определенный уровень, работа сети становится неустойчивой, что выражается в неопределенном времени ее реакции на запросы.

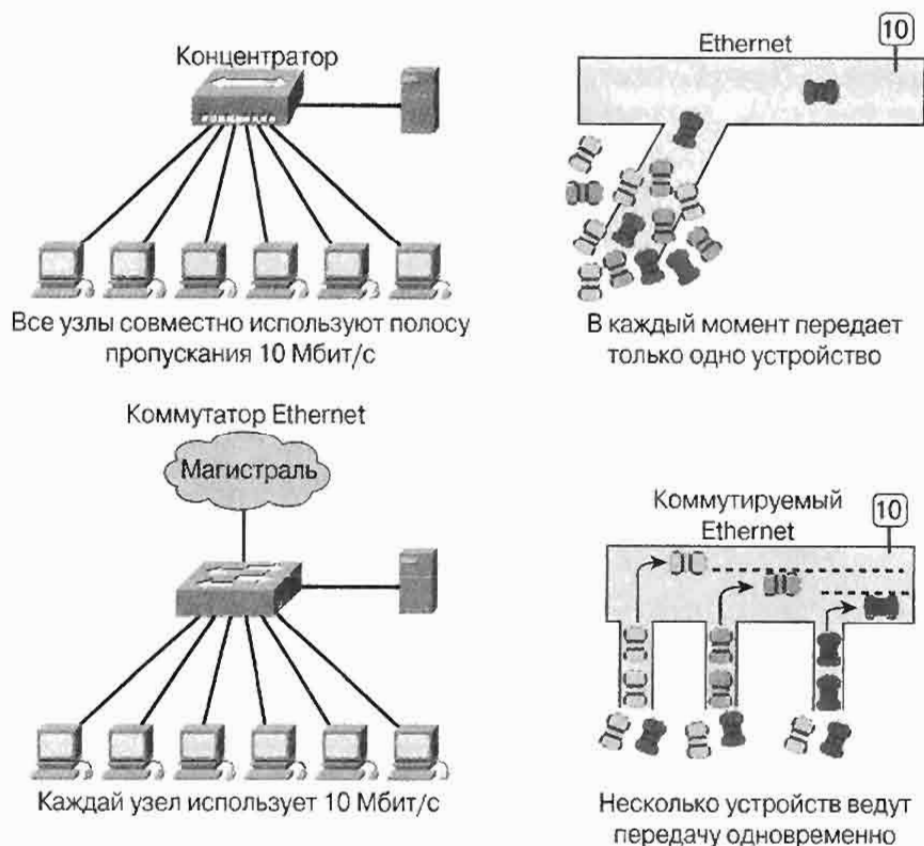


Рис. 5.4. Сравнение коммутаторов и маршрутизаторов с концентраторами

Маршрутизатор представляет собой устройство 3-го уровня. Он принимает решение о пересылке пакетов данных на основе сетевых адресов устройств, отличающихся от их индивидуальных MAC-адресов 2-го уровня. Адреса доступных маршрутизатору сетей заносятся в таблицы маршрутизации (*routing tables*). Эти адреса могут также задаваться системным администратором или получаться от соседних маршрутизаторов в результате работы протоколов маршрутизации. Целью работы маршрутизаторов является исследование входящих пакетов (данных 3-го уровня), выбор для них наилучшего пути по сети и передача их на соответствующий выходной порт. Маршрутизаторы могут останавливать широковещательные пакеты. Вследствие этого они уменьшают количество не только коллизионных, но и широковещательных доменов (*broadcast domain*). В крупных сетях маршрутизаторы являются наиболее важными устройствами для управления потоками данных. В принципе они позволяют компьютеру любого типа осуществлять связь с любым другим компьютером в любой точке планеты. Как показано на рис. 5.5, в локальных сетях обычно используются комбинации устройств 1-го, 2-го и 3-го уровней. На рис. 5.5 показан концентратор (1-й уровень), 2 коммутатора (2-й уровень) и маршрутизатор (3-й уровень). Характер использования этих устройств и их количество определяются конкретными потребностями организации, в которой используется сеть.

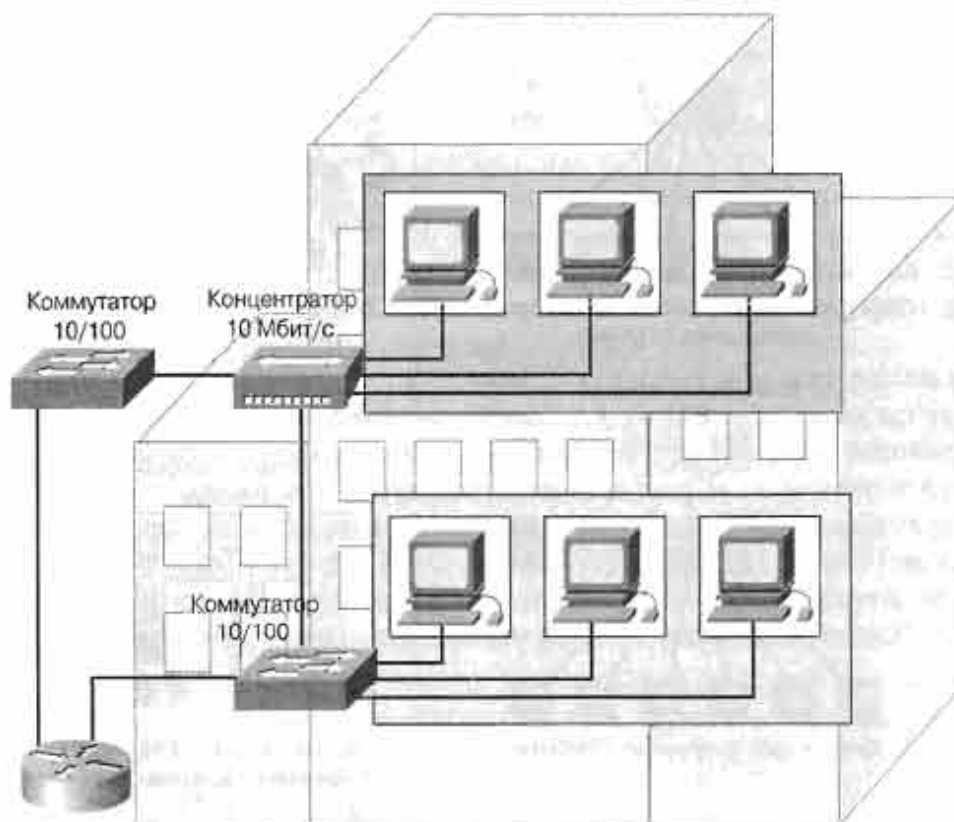


Рис. 5.5. Современная локальная сеть

Факторы, влияющие на производительность сети

В современных сетях LAN все чаще возникают перегрузки, вызывающие переполнение. Кроме постоянно растущего числа пользователей этих сетей имеются и другие факторы, увеличивающие нагрузку на традиционные сети LAN. Эти факторы проиллюстрированы на рис. 5.6 и описанные ниже.

- Возможность многозадачности, обеспечиваемая операционными системами настольных компьютеров (Windows, UNIX и Macintosh) позволяет одновременно выполнять несколько сетевых приложений. Эти возросшие возможности увеличивают потребность в сетевых ресурсах.
- Поскольку три наиболее распространенные операционные системы настольных компьютеров (Windows, UNIX и Macintosh) обеспечивают многозадачность, пользователи могут одновременно начать несколько сетевых операций. В версии Windows 95, представляющей собой развитие многозадачной ОС DOS/Windows, у пользователей может появиться потребность в увеличенных сетевых ресурсах.
- Несмотря на увеличение использования интенсивно потребляющих ресурсы приложений, таких как World Wide Web, приложения типа «клиент/сервер» позволяют сетевым администраторам централизовать обработку информации, что облегчает ее поддержку и защиту. Приложения типа «клиент/сервер» освобождают локальные рабочие станции от необходимости поддержки больших объемов информации и, соответственно, от потребности в жестких дис-

ках большого объема для ее хранения. Учитывая значительный финансовый выигрыш от использования приложений “клиент/сервер”, в будущем следует ожидать еще более широкого их распространения.



- В сегменте 10 Мбит/с слишком много пользователей
- Большинство пользователей имеют доступ к одному или двум серверам
- Интенсивно использующие сеть приложения, такие как создание цветных изображений, CAD/CAM, графика и реляционные базы данных

Рис. 5.6. Типичные причины переполнения в сетях

Элементы сетей Ethernet/802.3

Наиболее часто используемой архитектурой локальной сети LAN является Ethernet. Эта технология используется для передачи данных между сетевыми устройствами, такими как компьютеры, принтеры и файловые серверы, подсоединенные к общей для них физической передающей среде. Как показано на рис. 5.7, Ethernet использует для передачи и приема данных в одной и той же физической среде метод широковещания.

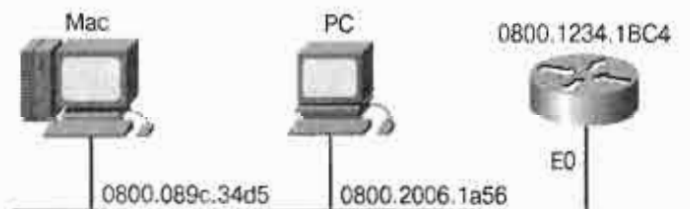
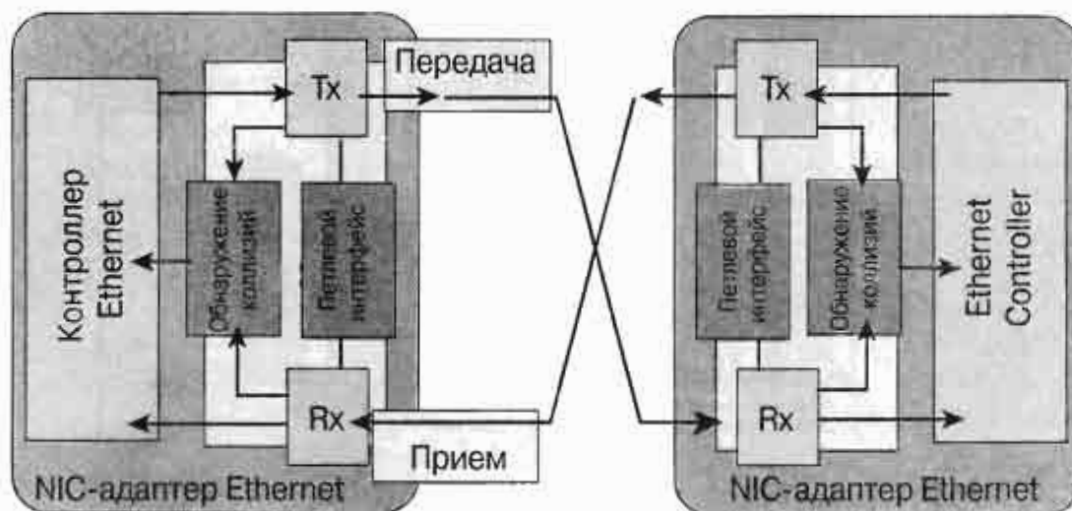


Рис. 5.7. Интерфейс сети The Ethernet/802.3

Полудуплексные сети Ethernet

Базовый Ethernet представляет собой полудуплексную технологию. Как показано на рис. 5.8, каждый узел Ethernet перед передачей своих данных прослушивает сеть с целью выяснения, не занята ли она передачей данных других узлов. Если сеть занята, то передача данных откладывается. Несмотря на это возможен случай когда два или

более узла начинают передачу одновременно, что приводит к коллизии. В случае коллизии узел, первым ее обнаруживающий, посылает в сеть сигнал о заторе (jam). После получения такого сигнала каждый узел в течение случайным образом выбираемого промежутка времени ожидает перед повторной попыткой передать свои данные. Этот промежуток времени случайной длительности определяется платой сетевого интерфейса с помощью специального алгоритма. По мере того, как к сети присоединяются новые узлы, вероятность коллизий все возрастает.



- Наиболее важными функциями являются: прием (Rx), передача (Tx) и обнаружение коллизий
- Взаимодействие устройств на физическом уровне обеспечивается рядом электронных схем, из которых состоит плата сетевого интерфейса

Рис. 5.8. Схема полудуплексной сети Ethernet

В сети Ethernet часто возникают заторы вследствие того, что пользователи запускают приложения, интенсивно использующие сетевые ресурсы, такие как приложения “клиент/сервер”, в которых узлы передают данные чаще и в течение более длительных промежутков времени. Плата сетевого интерфейса, используемая устройствами локальных сетей, состоит из ряда электронных схем. Это позволяет устройствам взаимодействовать друг с другом на физическом уровне.

Дуплексные сети Ethernet

Технология дуплексного Ethernet позволяет устройствам сети одновременно передавать одни пакеты и получать другие.

Одновременный прием и передача требуют использования в кабеле двух пар проводов и коммутируемых соединений между всеми узлами сети. Такое соединение рассматривается как соединение типа “точка-точка” и исключает возможность коллизий. Поскольку оба узла могут передавать данные и получать их в одно и то же время, вопрос о полосе пропускания не возникает. Дуплексный Ethernet может использовать существующую общую передающую среду при условии, что она удовлетворяет минимальным стандартам Ethernet. Для одновременной передачи и приема на каждом узле должен иметься выделенный для этого порт. Для создания соединений типа “точка-точка” в дуплексном Ethernet спецификаций 10BASE-T, 100BASE-TX (FastEthernet)

или 1000BASE-TX (Gigabit Ethernet) может использоваться неэкранированная витая пара (unshielded twisted-pair — UTP). Для соединений Ethernet-спецификаций 100BASE-FX (FastEthernet) и 1000BASE-X (Gigabit Ethernet) может также использоваться оптоволоконный кабель. Сетевые интерфейсы (карты сетевого интерфейса, порты и т.д.) на всех подсоединенных устройствах должны обладать дуплексными возможностями и поддерживать соответствующие скорости. Спецификация 10-Гигабит была стандартизована, но реализуется только в оптоволоконной среде. При использовании медных проводов коммутатор дуплексного Ethernet или Fast Ethernet пользуется двумя парами проводов в кабеле для создания непосредственного соединения между передачей (transmit — TX) на одном конце канала и приемом (receive — RX) на другом. Если две станции соединены таким образом, то при одновременной передаче и приеме на отдельных неконкурирующих каналах создается свободная от коллизий среда. При передаче данных по медному проводу UTP Gigabit Ethernet использует для одновременной передачи в обоих направлениях сложную систему электрических цепей. Все версии Ethernet, которые поддерживают использование оптоволоконного кабеля, используют два strands: один для передачи TX, а другой для приема RX. Сама по себе LAN-коммутация уменьшает вероятность коллизий, поскольку каждое соединение между двумя портами представляет собой выделенную линию. Дуплексная передача, удваивая полосу пропускания, радикально повышает эффективность работы сети. Дуплексная передача между станциями осуществляется посредством создания соединений Ethernet типа «точка-точка». Эта функция может оказаться важной при интенсивном обмене данными между устройствами, например, между коммутатором и сервером или двумя коммутаторами. Дуплексная передача создает свободную от коллизий среду. Поскольку оба узла могут одновременно принимать данные и передавать их, вопрос о полосе пропускания не возникает и не обсуждается. Например, в соединениях 10 Мбит/с дуплексная технология обеспечивает 10 Мбит/с для приема и 10 Мбит/с для передачи, что фактически предоставляет соединению пропускную способность 20 Мбит/с. аналогичным образом для соединения 100 Мбит/с фактически обеспечивается полоса пропускания 200 Мбит/с, как показано на рис. 5.9. При дуплексной связи возможна поддержка нескольких маршрутов передачи данных со скоростями до 2 Гбит/с.



Рис. 5.9. Дуплексная технология

Начальные сведения о коммутации в локальных сетях

Коммутация представляет собой технологию, которая уменьшает нагрузку в локальной сети путем уменьшения количества передаваемых данных и увеличения полосы пропускания. В настоящее время в локальных сетях LAN концентраторы часто заменяются коммутаторами (*switch*), которые могут работать в уже существующей кабельной инфраструктуре и, таким образом, их установка не нарушает сложившегося характера работы сети. Для уменьшения количества коллизий и расширения полосы пропускания LAN коммутаторы используют микросегментацию. Коммута-

торы LAN также поддерживают такие функции как дуплексная коммуникация и одновременные сеансы связи между несколькими устройствами. Дуплексная коммуникация позволяет двум устройствам одновременно получать друг от друга данные и посылать их. Фактически использование полного дуплекса удваивает пропускную способность сети LAN. В дуплексной коммутируемой LAN отсутствуют коллизии.

При пересылке данных через коммутатор возможны три режима коммутации: с промежуточным хранением (*store-and-forward*), сквозной (*cut-through*) и коммутация без фрагментации (*fragment-free switching*). Под латентностью или задержкой (*latency* или *delay*) понимается время прохождения пакета через коммутатор. Латентность каждого режима зависит от того, каким образом коммутатор обрабатывает и пересылает поступающие фреймы. Более быстрый режим коммутации уменьшает латентность коммутатора. Для выполнения функций коммутации коммутаторы и мосты LAN, функционирующие на 2-м уровне эталонной модели OSI, пересылают фреймы на основе MAC-адресов сетевых устройств. Если MAC-адрес 2-го уровня неизвестен, то устройство осуществляет лавинную рассылку, пытаясь таким путем достичь пункта назначения фрейма. Коммутаторы и мосты LAN также пересылают все широковещательные пакеты. Это может привести к лавинному шторму, т.е. ситуации, когда фреймы бесконечно циркулируют по образующимся в сети петлям. Для предотвращения петель используется протокол связующего дерева (*Spanning Tree Protocol*). Этот протокол представляет собой технологию, которая позволяет коммутаторам обмениваться друг с другом информацией и, таким образом, обнаруживать в сети петли. Протокол связующего дерева допускает существование в сети избыточных маршрутов, которые рассматриваются как резервные, однако для предотвращения петель временно отключает некоторые порты коммутаторов.

Сегментация в локальных сетях

Сегментация в сети LAN используется для двух целей: для изолирования потоков данных внутри сегментов и для увеличения полосы пропускания, приходящейся на одного пользователя, за счет уменьшения размеров коллизионных доменов.

При отсутствии сегментации сети LAN, превосходящие размерами небольшую рабочую группу, быстро становятся clogged и коллизии практически полностью закрывают полосу пропускания. Сегментация в сети LAN может быть реализована с помощью мостов, коммутаторов и маршрутизаторов. Каждое из этих устройств обладает своими достоинствами и недостатками. Сеть может быть подразделена на области меньшего размера, называемые сегментами. Каждый сегмент использует метод доступа CSMA/CD и поддерживает обмен данными между своими пользователями. На рис. 5.10 приведен пример сегментированной локальной сети Ethernet. Вся сеть состоит из 15 компьютеров (6 файловых серверов и 9 PC). Если разделить эту сеть на сегменты, то при коммуникации внутри сегмента на одни и те же 10 Мбит/с будет приходиться меньшее количество пользователей/устройств. Как показано на рис. 5.11, каждый сегмент рассматривается как отдельный коллизионный домен (*collision domain*).

Разделив всю сеть на три сегмента, сетевой администратор может уменьшить вероятность переполнения внутри каждого из них. При передаче данных внутри сегмента все пять устройств делят между собой полосу пропускания сегмента шириной 10 Мбит/с. В сегментированной локальной сети Ethernet данные, прошедшие по сегменту, передаются в сетевую магистраль (*backbone*) с помощью мостов (*bridge*), маршрутизаторов (*router*) или коммутаторов (*switch*). Магистральный (четвертый) сегмент передает данные всех трех остальных сегментов.

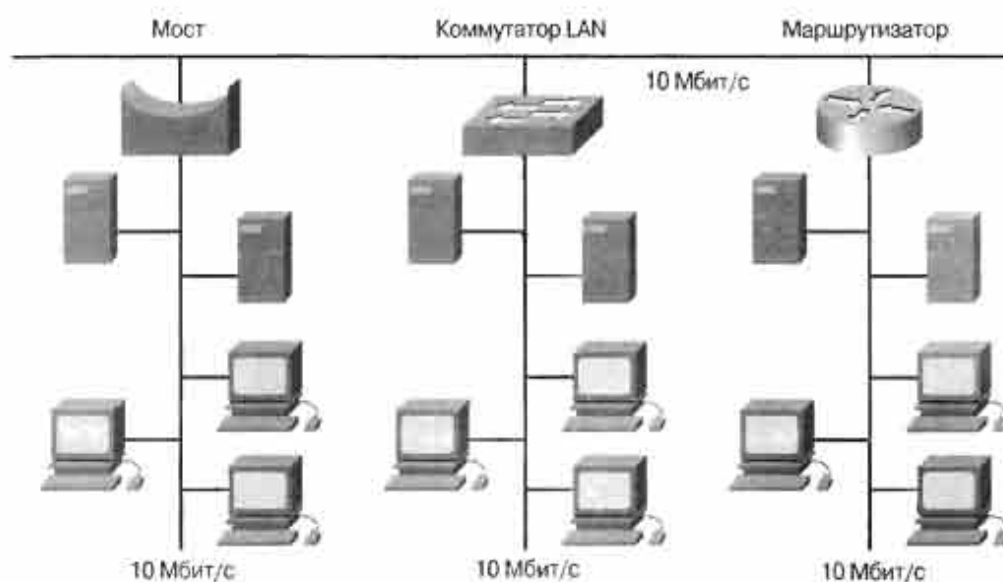


Рис. 5.10. Сегментированная сеть

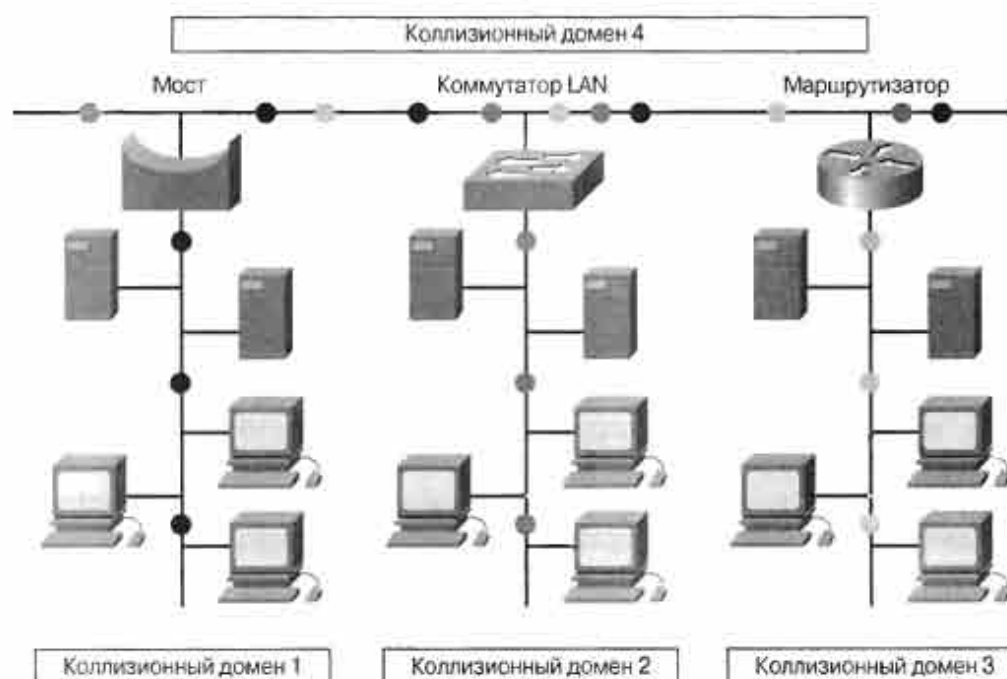


Рис. 5.11. Коллизийные домены

Основной характеристикой LAN-коммутации является микросегментации, которая позволяет создавать выделенные сегменты и предоставляет выделенную полосу пропускания каждому пользователю сети. Каждый пользователь получает доступ сразу ко всей полосе пропускания сети и ему не приходится конкурировать за доступную полосу пропускания с остальными пользователями. Это означает что пары устройств, подсоединенные к одному коммутатору, могут осуществлять связь одновременно с минимальным количеством коллизий. Микросегментация уменьшает количество коллизий за счет уменьшения размера коллизийных доменов. Это увеличивает пропускную способность для каждого устройства, подсоединенного к сети.

Сегментация с использованием мостов

Локальная сеть Ethernet, использующая для сегментации мосты, обеспечивает большую ширину полосы пропускания в расчете на одного пользователя, поскольку на один сегмент приходится меньше пользователей. И наоборот, локальные сети, в которых мосты не используются, обеспечивают меньшую полосу пропускания, поскольку в несегментированной LAN оказывается больше пользователей. На рис. 5.12 приведен пример локальной сети, сегментированной с помощью моста.

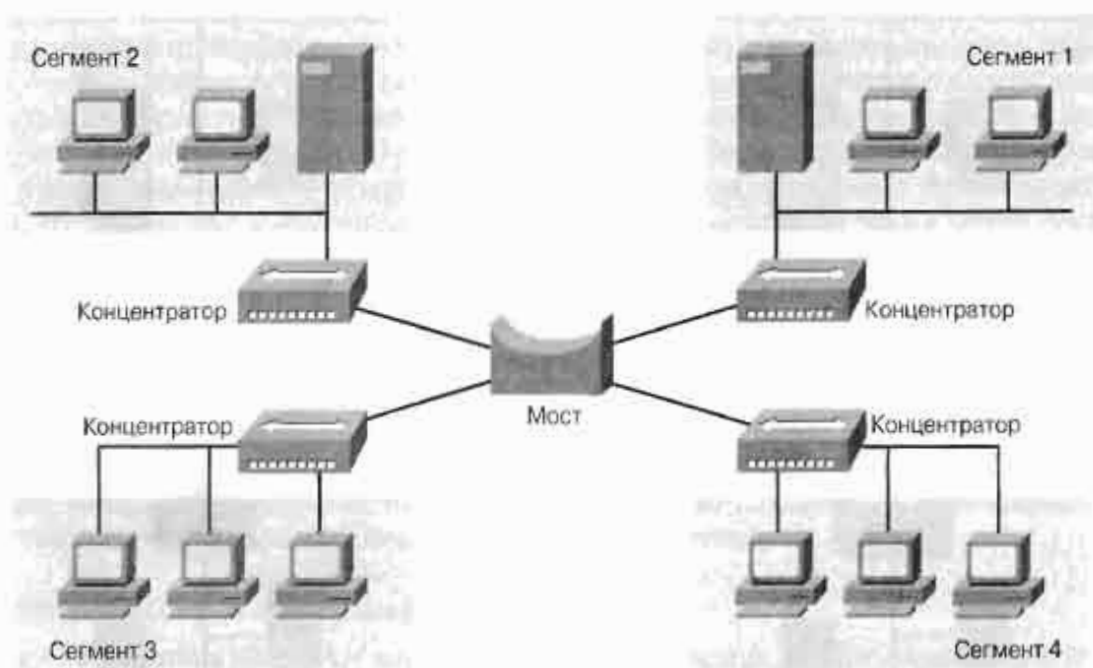


Рис. 5.12. Сегментация с использованием мостов

Мосты “изучают” характер расположения сегментов сети путем построения адресных таблиц, в которых содержатся адреса всех сетевых устройств и сегментов, необходимых для получения доступа к данному устройству. На рис. 5.13 приведен пример того, как мост использует адресную таблицу для идентификации всех узлов сети.

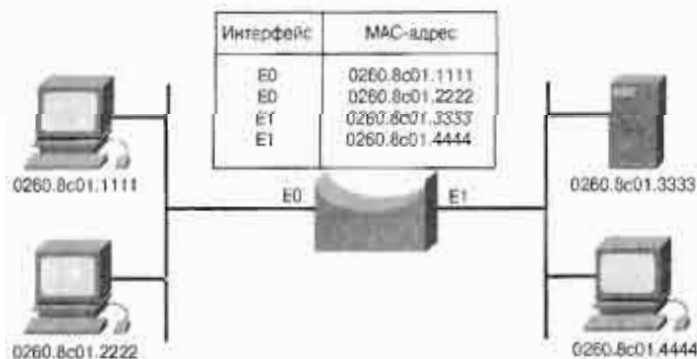


Рис. 5.13. Пример адресной таблицы

Мосты являются устройствами 2-го уровня, которые направляют фреймы данных в соответствии с MAC-адресами фреймов. Кроме того мосты являются “прозрачными” для всех остальных устройств сети.

Как показано на рис. 5.14, мост узнает о расположении устройств А, В, С и D, изучая MAC-адреса отправителей. Если мост регистрирует поступление фрейма, но не знает ни адреса отправителя, ни адреса получателя, то он добавляет адрес отправителя в свою адресную таблицу и направляет фрейм на все интерфейсы, за исключением того, на который этот фрейм поступил. При получении ответа мост исследует адрес отправителя и добавляет эту станцию в свою адресную таблицу. В дальнейшем для связи этих устройств мост использует данные адресной таблицы.

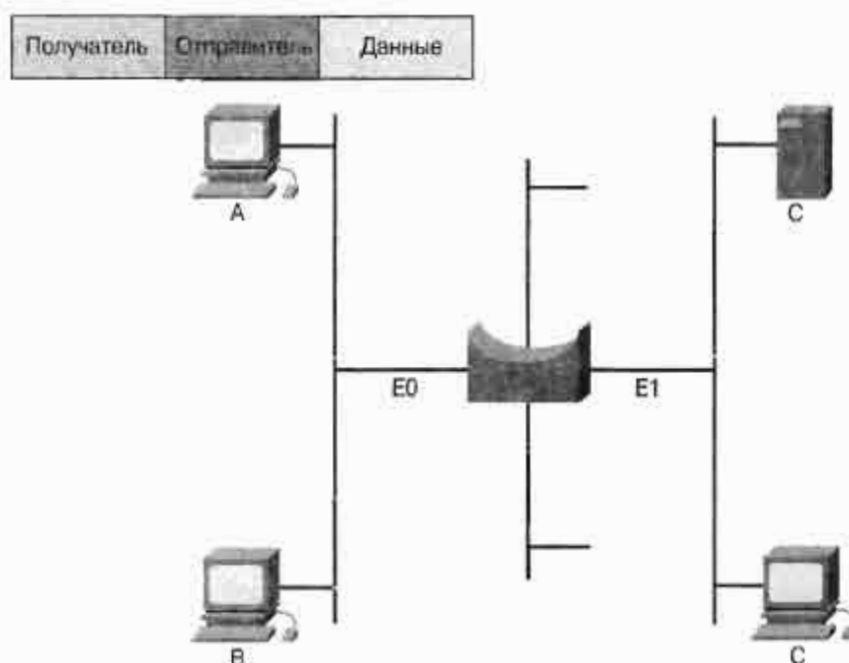


Рис. 5.14. Сегментация с использованием мостов

Мосты увеличивают латентность сети на 10-30%. Это увеличение латентности связано с тем, что мосту при передаче данных требуется дополнительное время на принятие решения. Мост рассматривается как устройство с функциями хранения и дальнейшей отправки, поскольку он должен проанализировать поле адреса пункта назначения фрейма и вычислить контрольную сумму CRC в поле контрольной последовательности фрейма перед отправкой фрейма на все порты. Если порт пункта назначения в данный момент занят, то мост может временно сохранить фрейм до освобождения порта.

Для выполнения этих операций требуется некоторое время, что замедляет процесс передачи и увеличивает латентность.

Сегментация с использованием маршрутизаторов

Маршрутизаторы представляют собой более современные устройства, чем обычные мосты. Мост является пассивным элементом сети и действует на уровне канала связи. Маршрутизатор действует на сетевом уровне (*network layer*) и в своих решениях отно-

сительно направления данных между сегментами опирается на адреса протокола сетевого уровня. Маршрутизаторы дают наивысший уровень сегментации, направляя данные на концентратор, к которому подсоединены рабочие станции. Маршрутизатор принимает решение о выборе сегмента для передачи данных, анализируя адрес пункта назначения, содержащийся в пакете данных, и используя таблицу маршрутизации (routing table) для выработки направляющих инструкций, как показано на рис. 5.15.

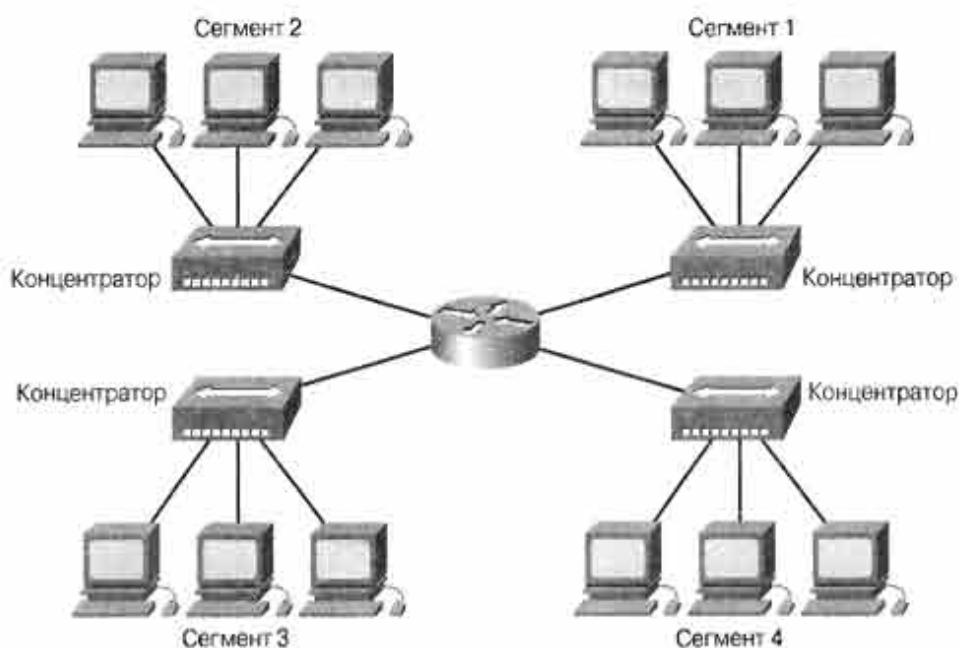


Рис. 5.15. Сегментация с использованием маршрутизаторов

Для того, чтобы определить наилучший путь следования пакета к пункту назначения маршрутизатору требуется изучить полученный пакет. Этот процесс требует времени. Протоколы, требующие для каждого пакета подтверждения (acknowledgment) адресатом его получения, известные как протоколы, ориентированные на подтверждение (acknowledgment-oriented protocols), имеют сниженную на 30—40% производительность.

Протоколы, требующие минимального подтверждения (протоколы скользящего окна) (sliding-window protocols) вызывают потерю пропускной способности на 20-30%. Это связано с уменьшением потока данных между отправителем и получателем (т.е. меньшего количества подтверждений).

Сегментация с использованием коммутаторов

Использование коммутации (switching) в локальных сетях смягчает проблемы, связанные с недостаточной шириной полосы пропускания и с возможностью переполнений, которые могут возникать, например, между несколькими PC и удаленным файл-сервером. Коммутатор разделяет локальную сеть на микросегменты, состоящие из двух станций, как показано на рис. 5.16. При этом один большой коллизионный домен делится на несколько малых доменов, свободных от коллизий. Хотя LAN-коммутатор устраняет возможность коллизий между доменами, отдельные станции, находящиеся внутри сегмента, по-прежнему остаются в одном коллизионном домене. Вследствие этого все узлы, подключенные к коммутатору, могут получить широковещательный сигнал всего от одного узла. Среди других преимуществ

стоит отметить малую латентность и высокую скорость пересылки на каждом порте интерфейса, а также совместимость с уже установленными сетевыми адаптерами, концентраторами и кабельной системой.



Рис. 5.16. Сегментация с помощью коммутаторов

Технология коммутуемого Ethernet (switched Ethernet) базируется на типовом Ethernet. При ее использовании каждый узел непосредственно соединен с одним из портов коммутатора или с сегментом, который, в свою очередь, соединен с одним из портов коммутатора. Таким образом на коммутаторе создается соединение с полосой пропускания 10 Мбит/с, 100 Мбит/с или 1000 Мбит/с между каждым узлом и соответствующим сегментом. Компьютер, непосредственно соединенный с коммутатором, имеет собственный коллизийный домен и полную полосу пропускания в 10 Мбит/с. Например, 12-портовый коммутатор, к каждому порту которого подсоединено одно устройство, создает 12 коллизийных доменов.

Локальная сеть, использующая топологию (topology) коммутуемого Ethernet, ведет себя так, как если бы она имела только два узла — узел отправителя и узел получателя. Этим двум узлам предоставляется полоса пропускания в 10 Мбит/с. Вследствие этого практически вся полоса пропускания может быть использована для передачи данных. За счет более эффективного использования полосы пропускания коммутуемый Ethernet обеспечивает более высокую скорость передачи, чем сети Ethernet, в которых используются только мосты и концентраторы. В коммутуемом Ethernet доступная ширина полосы пропускания может достигать величины, близкой к 100%.

Коммутация в сети Ethernet увеличивает доступную полосу пропускания путем создания выделенных сегментов (т.е. соединений типа “точка-точка”) и объединения этих сегментов в виртуальную сеть внутри коммутатора. Эта виртуальная сеть существует только тогда, когда двум узлам требуется обменяться информацией. Этим объясняется название “виртуальный канал” (virtual circuit)— он существует только при необходимости и создается внутри коммутатора.

Недостатком коммутаторов является их более высокая стоимость. Однако некоторые предприятия могут использовать постепенную замену концентраторов коммутаторами, до того момента когда все концентраторы окажутся замененными. Во время процесса замены скорости и возможности коммутаторов постепенно возрастают, а стоимость уменьшается. В настоящее время практически все новые LAN-сети Ethernet проектируются с ориентацией исключительно на технологию коммутации.

Основные операции коммутатора

Коммутация представляет собой технологию, которая уменьшает вероятность переполнения в сетях Ethernet, Token Ring и Fiber Distributed Data Interface (FDDI). В сетях LAN коммутаторы часто используются для замены совместно используемых концентраторов. Коммутаторы LAN разрабатываются таким образом, чтобы они могли быть установлены в уже существующие кабельные сетевые инфраструктуры без нарушения уже сложившегося характера работы сети. В современных коммуникациях все коммутирующие устройства выполняют две основные операции:

- **Коммутация фреймов данных.** Эта операция состоит в получении фрейма из входной передающей среды и передаче его в выходную среду.
- **Поддержка операций по коммутации.** При своей работе коммутатор строит и поддерживает таблицы коммутации.

Под *мостовыми операциями (bridging)* понимается технология, в которой устройство, известное как мост, соединяет два или более сегментов сети LAN. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Мост передает дейтаграммы из одного сегмента к получателям, находящимся в других сегментах. Когда включается питание и начинается функционирование моста, он изучает MAC-адреса поступающих дейтаграмм и строит таблицу адресов известных ему получателей. Если мосту известно, что пункт назначения дейтаграммы находится в том же сегменте где и ее отправитель, то дейтаграмма отбрасывается, поскольку в ее передаче нет необходимости. Если мосту известно, что получатель находится в другом сегменте, то он передает ее только в этот сегмент. Если же сегмент пункта назначения неизвестен, то мост передает дейтаграмму во все сегменты, кроме того, в котором находится отправитель этой дейтаграммы. Такая передача называется лавинной рассылкой (flooding). Основным достоинством моста является ограничение перемещения потоков данных лишь некоторыми сетевыми сегментами. Как мосты, так и коммутаторы соединяют между собой сегменты сети LAN, используют MAC-адреса для определения сегмента, в который требуется передать дейтаграмму и уменьшают объем передаваемых данных. В современных сетях коммутаторы выполняют большее количество функций, чем мосты, поскольку они позволяют осуществлять большее количество соединений, работают с гораздо большими скоростями, чем мосты, а также поддерживают новые функции, такие как виртуальные локальные сети (virtual LAN — VLAN). В мостах коммутацию обычно осуществляет программное обеспечение, в то время как в коммутаторах коммутация обычно выполняется аппаратно.

В настоящем разделе обсуждаются основные операции коммутаторов сетей LAN. На рис. 5.17 показана LAN-сеть с тремя рабочими станциями, LAN-коммутатор и адресная таблица этого коммутатора. LAN-коммутатор имеет четыре порта (или сетевых соединения). Станции А и С подсоединены к 3-му интерфейсу коммутатора, а станция В к 4-му интерфейсу. Вероятнее всего, что в реальной сети станции А и С будут подсоединены к концентратору, который будет подсоединен к 3-му интерфейсу. Как показано на рис. 5.17, станции А требуется передать данные станции В.

Операции, выполняемые LAN-коммутатором

- Пересылает пакеты на основе данных таблицы пересылки
 - Пересылает пакеты на основе MAC-адреса (2-й уровень)
- Функционирует на 2-м уровне модели OSI
- Узнает расположение станции путем исследования адреса отправителя
 - Осуществляет рассылку со всех портов если адрес получателя является широковещательным, многоадресным или неизвестен
 - Осуществляет пересылку в том случае, если получатель расположен на другом интерфейсе

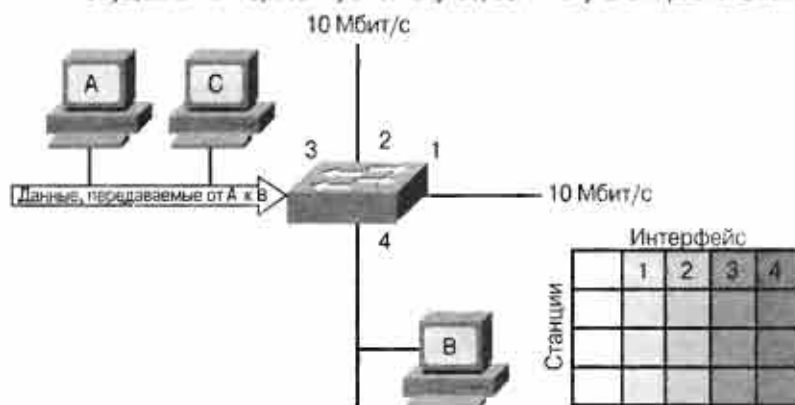


Рис. 5.17. Операции LAN-коммутатора

Следует помнить о том, что при прохождении потоков данных по сети коммутатор функционирует на 2-м уровне; это означает, что коммутатор просматривает адрес MAC-уровня. При передаче фреймов станцией А и получении их коммутатором, последний просматривает MAC-адрес отправителя и сохраняет его в адресной таблице, как показано на рис. 5.18. При прохождении данных через коммутатор в адресной таблице создается новая позиция, в которую заносится адрес станции-отправителя и интерфейс коммутатора, к которому она подсоединена. После этого коммутатору известно где подсоединена станция А. Как показано на рис. 5.19, после поступления фрейма данных на коммутатор он лавинным образом рассылается на все порты, поскольку станция-получатель пока неизвестна.

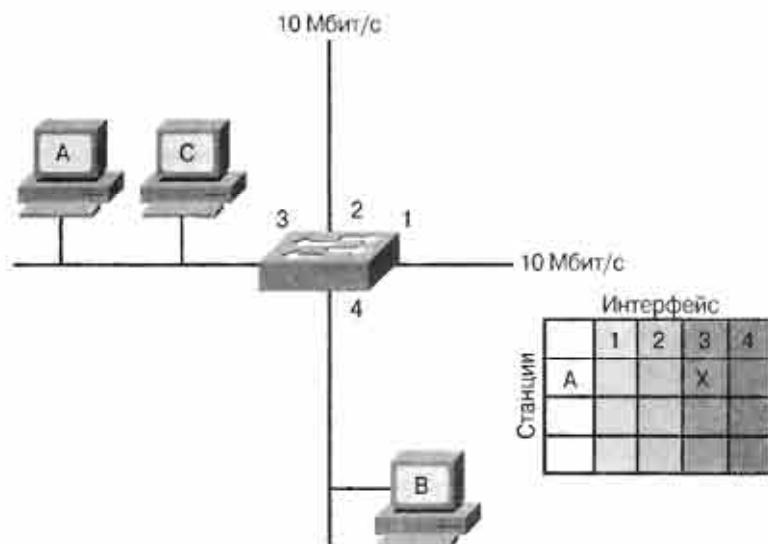


Рис. 5.18. Построение адресной таблицы

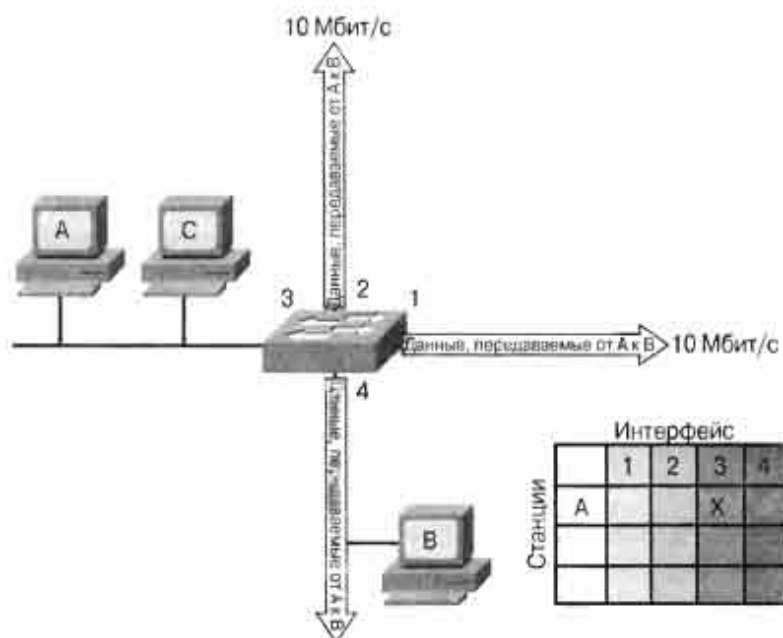


Рис. 5.19. Лавинная рассылка на все порты

Однако после создания соответствующей позиции в адресной таблице поступает ответ от станции В к станции А. Теперь коммутатору известно, что станция В подсоединена к 4-му интерфейсу, как показано на рис. 5.20.

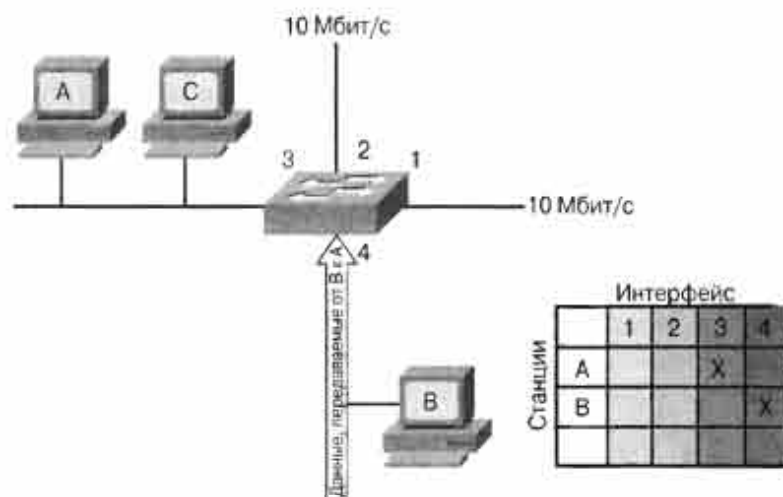


Рис. 5.20. Ответ на лавинную рассылку

Данные поступают на коммутатор, однако следует обратить внимание на то, что теперь коммутатор не выполняет лавинной рассылки. Коммутатор отправляет данные только на 3-й интерфейс, поскольку ему известно, что станция А расположена в сегменте, подсоединенном к этому интерфейсу (рис. 5.21).

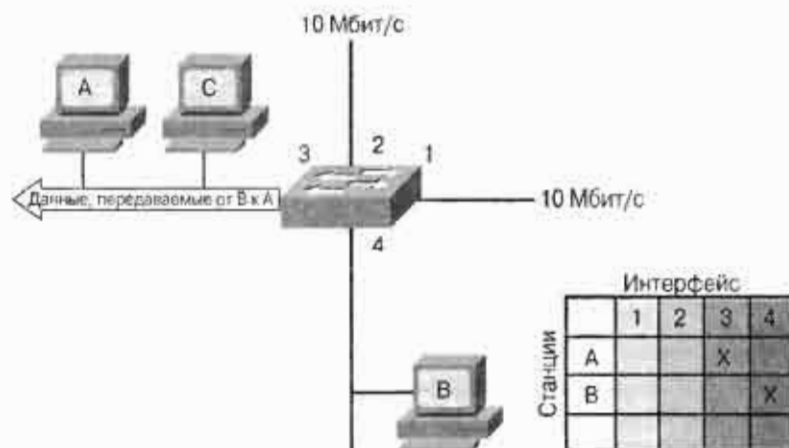


Рис. 5.21. Передача данных известной станции

Первоначальная передача указала MAC-адрес станции, от которой поступили данные, что позволило коммутатору более эффективно осуществлять передачу данных.

Задержка в коммутаторах сетей Ethernet

Каждый коммутатор, используемый в LAN Ethernet, увеличивает задержку в сети. Однако эта задержка зависит от типа коммутатора и используемого метода коммутации. Как будет показано далее, различные режимы коммутации (с промежуточным хранением, без фрагментации или *быстрая коммутация*) отличаются друг от друга тем, когда они принимают решение о пересылке входящего фрейма. Латентность, связанная с «принятием мостом решения», добавляется к времени, которое требуется фрейму для входа на порт коммутатора и выхода с него и вместе с ними определяет общую задержку коммутатора. Следует отметить, что концентратор, который выполняет только пересылку фреймов (не выполняя фильтрации и не принимая никаких решений) имеет лишь задержку, связанную с передачей фрейма с одного порта на другой. Может показаться, что эти крошечные доли секунды не имеют особого значения, однако следует помнить, что пересылка данных происходит со скоростями порядка 10 Мбит/с, т.е. на один бит приходится одна десятиллионная доля секунды, 100 Мбит/с — на один бит одна стомиллионная доля секунды или 1000 Мбит/с — одна миллиардная доля секунды. Сетевые устройства работают с невероятно высокими скоростями, поэтому учитывается даже каждая наносекунда.

Коммутация на 2-м и 3-м уровнях

В сетях используются два метода коммутации фреймов данных: коммутация на 2-м уровне, показанная на рис. 5.22, и коммутация на 3-м уровне, показанная на рис. 5.23. Под коммутацией понимается процесс приема входящего фрейма на одном интерфейсе и отправка его через другой интерфейс. Для маршрутизации пакетов маршрутизаторы используют коммутацию 3-го уровня, в то время как коммутаторы (имеются в виду коммутаторы 2-го уровня) используют для пересылки фреймов коммутацию 2-го уровня.



Рис. 5.22. Коммутация на 2-м уровне

Различие между коммутацией на 2-м уровне и на 3-м уровне определяется тем, какая находящаяся во фрейме информация используется для определения требуемого выходного интерфейса. При использовании коммутации 2-го уровня пересылка фреймов осуществляется на основе информации MAC-адреса. При использовании коммутации 3-го уровня пересылка фреймов осуществляется на основе информации сетевого адреса. При выполнении коммутации на 2-м уровне устройство не интересуется информацией сетевого уровня, которая используется для коммутации на 3-м уровне. При коммутации на 2-м уровне коммутатор просматривает во фрейме MAC-адрес пункта назначения. Если ему известно расположение адреса получателя, то коммутатор отправляет информацию на соответствующий интерфейс. При использовании коммутации 2-го уровня коммутатор строит и поддерживает таблицу коммутации, в которой фиксируется, какие MAC-адреса принадлежат определенным портам или интерфейсам.

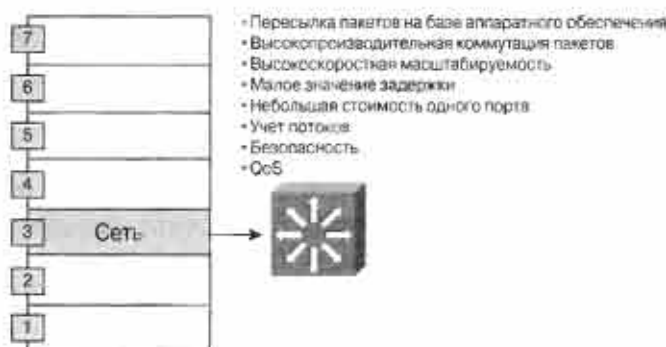


Рис. 5.23. Коммутация на 3-м уровне

Если коммутатор 2-го уровня не знает куда отправить фрейм, то он рассылает его широкоэвещательно со всех своих портов для получения информации о пункте назначения. При получении ответного фрейма от получателя коммутатор узнает расположение нового адреса и добавляет эту информацию в свою таблицу коммутации. Адреса 2-го уровня определяются производителем телекоммуникационных устройств. Они являются уникальными и состоят из двух частей: кода производителя (manufacturing — MFG) и уникального идентификатора устройства. Код MFG назначается производителю *Институтом инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers — IEEE)*. Уникальный идентификатор назначается устройству его производи-

телем. За исключением сетей системной сетевой архитектуры (Systems Network Architecture — SNA) пользователи практически не могут контролировать адресацию на 2-м уровне, поскольку адреса 2-го уровня являются для конкретных устройств фиксированными, в то время как адреса 3-го уровня могут быть изменены пользователем. Кроме того, адреса 2-го уровня образуют плоское (без иерархии) адресное пространство, в котором все адреса уникальны. Коммутация 3-го уровня выполняется на сетевом уровне. При ее использовании маршрутизатор анализирует содержащуюся в пакете информацию и пересылает пакеты получателям на основе их адресов сетевого уровня. При использовании коммутации 3-го уровня также поддерживается маршрутизация, т.е. выбор наилучшего пути к пункту назначения. Адреса 3-го уровня в большинстве случаев задаются сетевым администратором. Адресация на 3-м уровне используется, в частности, такими протоколами, как Internet Protocol (IP), Internetwork Packet Exchange (IPX) и AppleTalk. При задании адресов 3-го уровня создаются локальные области, которые адресуются как единое целое (аналогично названию страны, штата, города или улицы) и в рамках которых локальным устройствам присваиваются индивидуальные номера. При переезде пользователя в другое здание его конечные станции могут получить новые адреса 3-го уровня, однако адреса 2-го уровня останутся неизменными. Поскольку маршрутизаторы функционируют на 3-м уровне эталонной модели OSI, они могут принадлежать к иерархической структуре адресации и сами создавать ее. Вследствие этого маршрутизируемая сеть может для каждого сегмента связать структуру логической адресации с физической инфраструктурой, такой как подсеть протоколов TCP/IP или сеть протокола IPX. Характер перемещения потоков данных в плоских (коммутируемых) сетях и в маршрутизируемых (иерархических) сетях принципиально различен. Иерархические сети предоставляют возможность более гибкого управления потоками данных, поскольку сетевая иерархия позволяет определять оптимальные маршруты и ограничивать величину широковещательных доменов.

Смысл коммутации 2-го и 3-го уровня

Возросшая мощность процессоров и высокие требования приложений типа “клиент/сервер” и мультимедийных приложений вызвали потребность в большей ширине полосы пропускания в традиционных средах совместного пользования. Это побуждает проектировщиков сетей к замене в монтажных шкафах концентраторов на коммутаторы.

Для удовлетворения потребности в большей ширине полосы пропускания в локальных сетях коммутаторы 2-го уровня используют микросегментацию (microsegmentation). Это отчасти решает проблему, однако в настоящее время сетевые проектировщики столкнулись с возросшими требованиями к межсетевым коммуникациям. Например, каждый раз, когда пользователь получает доступ к серверу и другим ресурсам, расположенным в различных подсетях, поток данных должен пройти через устройство 3-го уровня. Потенциально может образоваться переполнение, которое угрожает нарушить работу сети. Для того чтобы избежать его возникновения, сетевой проектировщик может добавить дополнительные устройства 3-го уровня во всей сети что снижает нагрузку на централизованные маршрутизаторы. Могут быть также установлены коммутаторы 3-го уровня, использующие технологии маршрутизации. Таким образом, коммутатор увеличивает ширину полосы пропускания, отделяя друг от друга коллизийные домены и избирательно направляя потоки данных на соответствующие сегменты сети.

Симметричная и асимметричная коммутация

Свойство симметрии при коммутации позволяет дать характеристику коммутатора с точки зрения ширины полосы пропускания для каждого его порта. Как показано на рис. 5.24, симметричный коммутатор обеспечивает коммутируемые соединения между портами с одинаковой шириной полосы пропускания, например, в случаях когда все порты имеют ширину полосы пропускания 10 Мбит/с или 100 Мбит/с.

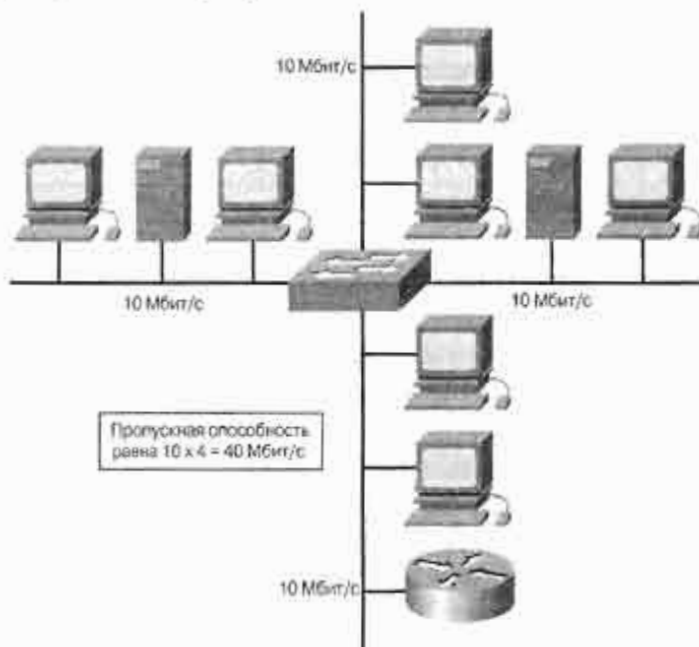


Рис. 5.24. Симметричная коммутация

Как показано на рис. 5.25, асимметричный LAN-коммутатор обеспечивает коммутируемые соединения между портами с различной шириной полосы пропускания, например, в случаях комбинации портов с шириной полосы пропускания 10 Мбит/с и 100 Мбит/с или 100 Мбит/с и 1000 Мбит/с.

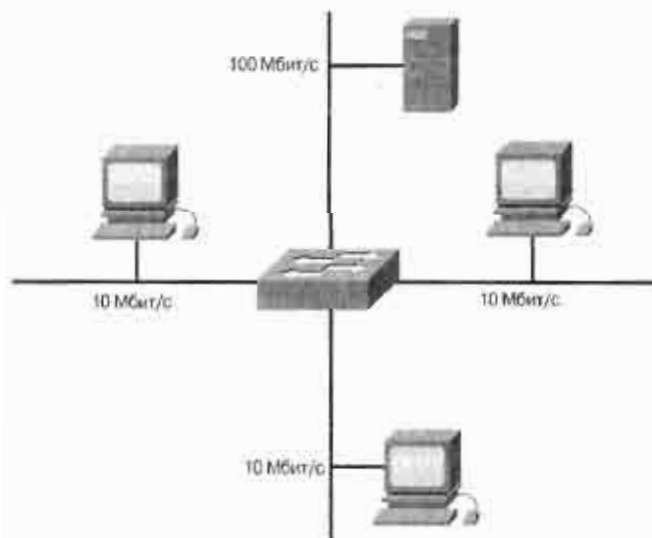


Рис. 5.25. Асимметричная коммутация

Асимметричная коммутация используется в случае наличия больших сетевых потоков типа клиент/сервер, когда многочисленные пользователи обмениваются информацией с сервером одновременно, что требует большей ширины пропускания для того порта коммутатора, к которому подсоединен сервер, с целью предотвращения переполнения на этом порте. Как будет описано в следующем разделе, для того чтобы направить поток данных с порта 100 Мбит/с на порт 10 Мбит/с без опасности переполнения на последнем, асимметричный коммутатор должен иметь буфер памяти. Асимметричный коммутатор также необходим для обеспечения большой ширины полосы пропускания каналов между коммутаторами, осуществляемых через вертикальные кросс-соединения или каналов между сегментами магистрали.

Буфер памяти

Для временного хранения пакетов и последующей их отправки по нужному адресу коммутатор может использовать буферизацию. Буферизация может быть также использована в том случае, когда порт пункта назначения занят. Буфером называется область памяти, в которой коммутатор хранит передаваемые данные.

Буфер памяти может использовать два метода хранения и отправки пакетов — буферизация по портам и буферизация с общей памятью.

При буферизации по портам пакеты хранятся в очередях (queues), которые связаны с отдельными входными портами. Пакет передается на выходной порт только тогда, когда все пакеты, находившиеся впереди него в очереди, были успешно переданы. При этом возможна ситуация, когда один пакет задерживает всю очередь из-за занятости порта его пункта назначения. Эта задержка может происходить даже в том случае, когда остальные пакеты могут быть переданы на открытые порты их пунктов назначения.

При буферизации в общей памяти все пакеты хранятся в общем буфере памяти, который используется всеми портами коммутатора. Количество памяти, отводимой порту, определяется требуемым ему количеством. Такой метод называется динамическим распределением буферной памяти. После этого пакеты, находящиеся в буфере динамически распределяются по выходным портам. Это позволяет получить пакет на одном порте и отправить его с другого порта, не устанавливая его в очередь.

Коммутатор поддерживает карту портов, в которые требуется отправить пакеты. Очистка этой карты происходит только после того, как пакет успешно отправлен. Поскольку память буфера является общей, размер пакета ограничивается всем размером буфера, а не долей, предназначенной для конкретного порта. Это означает, что крупные пакеты могут быть переданы с меньшими потерями, что особенно важно при асимметричной коммутации, т.е. когда порт с шириной полосы пропускания 100 Мбит/с должен отправлять пакеты на порт 10 Мбит/с или когда порт с шириной полосы пропускания 100 Мбит/с должен отправлять пакеты на порт 10 Мбит/с или 100 Мбит/с.

Проектирование локальных сетей

Несмотря на усовершенствования в области эффективности оборудования и повышение возможностей передающих сред, процесс проектирования сетей становится все более сложным. Намечается тенденция к использованию более сложных сред, включая различные носители и межсетевые соединения за пределами управляемой се-

ти, контролируемой одной организацией. В процессе проектирования важно постоянно помнить о совокупности этих факторов, поскольку тщательное проектирование сети может уменьшить трудности, связанные с ростом и развитием сетевой среды.

Тщательное проектирование сети является важнейшей предпосылкой ее быстрой и устойчивой работы. Если при проектировании сети допущены ошибки, то может возникнуть множество непредвиденных проблем и возможность ее роста окажется под угрозой. Процесс проектирования требует глубокого анализа конкретной ситуации. В настоящей главе приведен обзор процесса проектирования локальных сетей. Кроме того, в ней описаны цели, проблемы и методология проектирования, а также процесс разработки топологии локальных сетей.

Цели проекта локальной сети

Проектирование сети может оказаться сложной задачей. Оно включает в себя нечто большее, чем просто создание связи между компьютерами. Для того, чтобы сеть была управляемой и расширяемой, требуется учесть множество особенностей. Чтобы спланировать надежную и расширяемую сеть, проектировщик должен осознавать, что каждый из основных компонентов сети предъявляет к ней свои особые требования. Даже сеть, содержащая всего 50 узлов маршрутизации, может создать целый комплекс проблем, которые ведут к непредсказуемым результатам. А попытка разработать и построить сеть, включающую тысячи узлов, может вызвать еще более сложные проблемы.

Первым шагом в планировании сети является определение и документирование целей проекта. Названные цели являются специфическими для каждой организации или конкретной ситуации. Однако следующие требования характерны для большинства проектов.

- **Функциональность.** Прежде всего, сеть должна работать. Это означает, что она должна предоставить пользователям возможность удовлетворения их производственных потребностей. Сеть должна обеспечить связь пользователей друг с другом и с приложениями с соответствующей требованиям скоростью и надежностью.
- **Расширяемость.** Сеть должна обладать способностью к росту. Это означает, что первоначально реализованная сеть должна увеличиваться без каких-либо существенных изменений общего устройства.
- **Адаптируемость.** Сеть должна быть разработана с учетом технологий будущего и не должна включать элементы, которые в дальнейшем ограничивали бы внедрение технологических новшеств.
- **Управляемость.** Сеть нужно сконструировать так, чтобы облегчить текущий контроль и управление для обеспечения стабильности ее работы.

Аспекты, указанные выше, являются специфическими для одних типов сетей и более общими для других типов. В настоящей главе рассказывается как учесть эти требования в процессе проектирования.

Компоненты сетевого проекта

С появлением в последние годы высокоскоростных технологий, таких как АТМ (режим асинхронной передачи) и более сложных архитектур локальных сетей, использующих коммутацию и виртуальные локальные сети, многие организации стали обновлять свои локальные сети, планировать и внедрять новые.

Для конструирования локальных сетей под высокоскоростные технологии и мультимедийные приложения проектировщику необходимо учитывать следующие важнейшие аспекты общего проектирования сетей.

- Функции и размещение серверов.
- Определение коллизий.
- Сегментация.
- Соответствие широкополосных и широковещательных доменов.

Эти вопросы обсуждаются в следующих разделах.

Функции и размещение серверов

Одним из ключевых моментов успешного проектирования является правильное понимание функций серверов и особенностей их размещения в сети. Серверы предоставляют доступ к файлам, печать, связь и службы приложений, таких как обработка текстов. Серверы чаще используются не в качестве рабочих станций, а работают под управлением специализированных операционных систем, таких как NetWare, Windows NT/2000/XP, UNIX и Linux. В настоящее время каждый сервер обычно выделяется для выполнения одной функции, например, функции почтового или файлового сервера.

Серверы можно разделить на два отдельных класса: **серверы предприятия (enterprise servers)** и **серверы рабочих групп (workgroup servers)**. Сервер предприятия поддерживает всех пользователей сети, предоставляя им различные службы, такие как электронная почта или служба доменных имен (DNS). Поскольку серверы электронной почты и DNS выполняют централизованные функции, они могут понадобиться каждому члену организации. С другой стороны, сервер рабочей группы обслуживает определенную группу пользователей и предлагает им такие службы, как обработка текстов или совместный доступ к файлам, то есть функции, которые могут понадобиться только некоторым группам пользователей.

Серверы предприятия должны размещаться в **главной распределительной станции (main distribution facility — MDF)**. В этом случае поток данных на серверы предприятия будет идти только к MDF, не проходя через остальные сети. В идеальном случае серверы рабочих групп следует размещать в **промежуточных распределительных станциях (intermediate distribution facilities — IDF)**, по возможности ближе к пользователям, использующим приложения этих серверов. Если расположить серверы рабочих групп близко к пользователям, то поток данных будет проходить по инфраструктуре сети прямо к IDF, не затрагивая других пользователей в этом сегменте. Внутри MDF и IDF коммутаторы 2-го уровня должны иметь для этих серверов ширину полосы пропускания не менее 100 Мбит/с.

Сегментация

Под сегментацией (segmentation) понимается процесс разделения одного коллизийного домена на два или более, как показано на рис. 5.26. Мосты и коммутаторы 2-го (канального) уровня можно использовать для сегментации сети с логической *шинной топологией* и для создания разделенных коллизийных доменов. В результате увеличивается доступная полоса пропускания для отдельных станций. Следует обратить внимание на то, что вся показанная на рис. 5.27 сеть с шинной топологией по-прежнему представляет собой широковещательный домен, поскольку мосты и коммутаторы пересылают широковещательные пакеты, хотя и не распространяют коллизии.



Рис. 5.26. Процесс проектирования локальной сети

Для сегментации используются как мосты, так и коммутаторы

- Приводит к созданию нескольких коллизийных доменов
- Остается один широковещательный домен
- Станции могут получить выделенную полосу пропускания



Рис. 5.27. Использование сегментации

Все широковещательные рассылки от любого узла видны остальным узлам в том же широковещательном домене, что необходимо для обеспечения возможности установления соединения. Расширяемость широкополосного домена зависит от общего потока данных, а расширяемость широковещательного домена — от общего широковещательного потока. Важно помнить, что мосты и коммутаторы пересылают широковещательный (FF-FF-FF-FF-FF) поток, в то время как маршрутизаторы обычно этого не делают.

Широковещательные домены

Под широкополосным доменом понимаются все устройства, связанные с одним портом моста или коммутатора. В случае Ethernet-коммутатора широкополосный домен называется также коллизийным доменом. Как показано на рис. 5.28, коммутатор может создать по одному широкополосному домену на каждом порте. Все рабочие станции одного широкополосного домена конкурируют за полосу пропускания своей локальной сети. Весь поток данных с любого узла широкополосного домена виден всем остальным узлам. В коллизийном домене сети Ethernet две станции могут начать передачу одновременно, что вызывает коллизию.

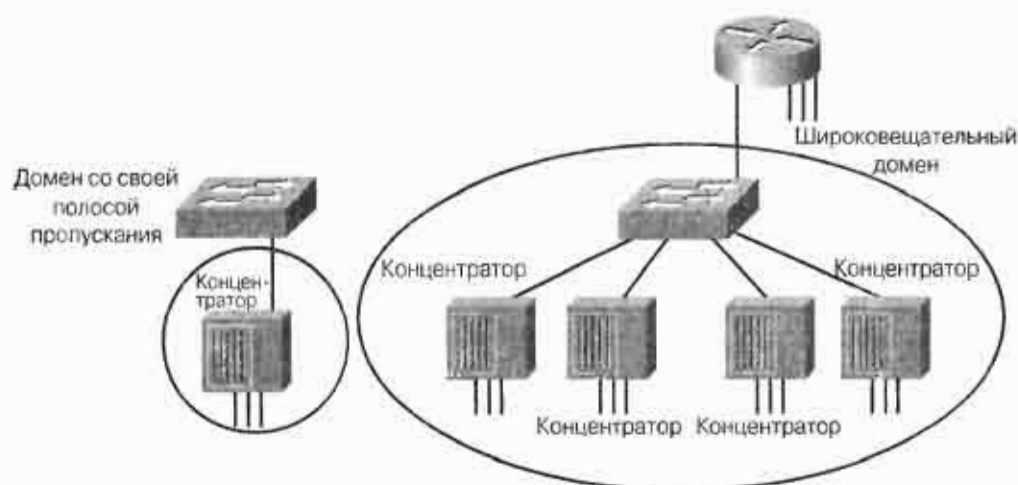


Рис. 5.28. Широкополосный и широковещательный домены

Методология проектирования сети

Чтобы локальная сеть была эффективной и удовлетворяла потребностям пользователей, она должна быть спроектирована и реализована в результате тщательно спланированной последовательности действий, включающих следующее.

- Сбор требований и ожиданий пользователей.
- Анализ собранных требований.
- Проектирование структуры 1-го, 2-го и 3-го уровней локальной сети (т. е. топологии сети).
- Документирование логической и физической реализации сети.

Эти действия описываются в приведенных ниже разделах.



На первом этапе проектирования сети следует собрать данные о структуре организации. Эта информация должна включать в себя данные об истории и текущем состоянии организации, о планируемом росте, о методах управления, офисных системах, а также мнения членов персонала, которые будут использовать локальную сеть. При этом необходимо ответить на следующие вопросы: кто будет пользователем локальной сети? Каков уровень ее навыков, и как он относится к компьютерам и компьютерным приложениям? Ответы на эти и подобные вопросы помогут определить требования к дополнительному обучению и количество специалистов, необходимое для поддержки данной локальной сети.

В идеальном случае процесс сбора информации помогает определить и прояснить проблемы, стоящие перед проектировщиком. Следует также определить, существуют ли в организации уже установленные правила. Объявлены ли какие-либо данные как критичные? Объявлены ли какие-либо операции как критичные? (Критичные данные и операции рассматриваются в качестве ключевых для бизнеса, а доступ к ним является критически важным для ежедневно выполняемых дел.) Какие протоколы можно использовать в сети? Существуют ли ограничения на типы рабочих станций?

Далее следует определить, кто в данной организации обладает полномочиями на установление адресации, назначение имен, на установку конфигурации и планирование топологии. В некоторых компаниях имеется центральный департамент управления информационными системами (Management Information Systems — MIS) который отвечает за решение этих вопросов. В других компаниях департамент MIS очень мал и поэтому полномочия передаются отделам. При этом также следует уделить особое внимание оценке ресурсов предприятия и имеющихся ограничений. Ресурсы организации, которые могут повлиять на реализацию новой локальной сети, подразделяются на две основные категории: компьютерное программное и аппаратное обеспечение и человеческие ресурсы. Нужно документально зафиксировать существующее программное и аппаратное обеспечение организации и то, которое потребуется в будущем. Каким образом в настоящее время эти ресурсы связаны и предоставляются ли они для совместного доступа? Какими финансовыми ресурсами обладает данная организация? Ответ на эти вопросы поможет оценить издержки и рассчитать бюджет локальной сети. Проектировщику следует также убедиться в правильном понимании им того, насколько эффективны сети, уже существующие на предприятии.

Следующий шаг при конструировании сети — анализ собранных на предыдущем этапе требований пользователей к будущей сети. С течением времени пользователи сети, как правило, повышают свои требования. Например, чем больше появляется доступных голосовых и видеоприложений, тем большими становятся требования *к увеличению пропускной способности сети*.

Еще одной задачей данного этапа является оценка требований пользователей. Конечно, мало пригодна сеть, которая не способна предоставить своим пользователям необходимую и точную информацию. Поэтому необходимо предпринять соответствующие действия для удовлетворения информационных требований организации и ее работников.

Доступность и поток данных в сети

Полезность сети определяется ее доступностью. На доступность влияют многие факторы, включая следующие.

- Пропускная способность.
- Время отклика.
- Доступ к ресурсам.

У каждого заказчика есть свое определение **доступности**. Например, может возникнуть необходимость передавать голосовые или видеоданные по сети. Однако подобные службы требуют полосы пропускания большей, чем имеющаяся в сети или магистрали. В этом случае доступность можно увеличить путем добавления ресурсов, но такой путь значительно увеличивает стоимость. В процессе сетевого проектирования необходимо искать способы обеспечения большей доступности с наименьшими затратами.

Проектирование сетевой топологии

Следующий шаг после определения всех требований к сети — принятие решения по выбору удовлетворяющей нужды пользователей, топологии локальной сети. В этой книге рассматриваются *звездообразная (star topology)* и расширенная звездообразная топологии. Как показано на рис. 5.29, звездообразная и расширенная звездообразная топологии используют технологию сетей Ethernet 802.3 — метод множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD). В этой книге рассматривается звездообразная топология CSMA/CD по причине ее доминирующего положения в индустрии.

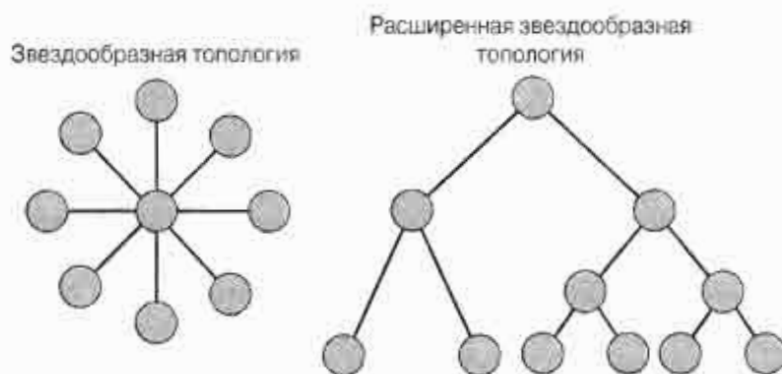


Рис. 5.29. Типы сетевых топологий

Проектирование на 1-м уровне

В настоящем разделе рассматриваются звездообразная и расширенная звездообразная топологии, показанные на рис. 5.26.

Физические кабели — один из наиболее важных компонентов, выбираемых при проектировании сети. Решение этой задачи включает в себя выбор типа используемого кабеля (обычно медный или оптоволоконный) и его общей структуры. Кабельная среда физического уровня включает в себя такие типы, как неэкранированная

витая пара пятой категории (Category 5 UTP) и оптоволоконный кабель (fiber-optic cable). Как показано на рис. 5.30, при прокладке кабеля следует руководствоваться стандартом TIA/EIA 568 для размещения и соединения проводных схем.

В дополнение к ограничениям на протяженность кабеля, необходимо тщательно оценить сильные и слабые стороны различных кабельных топологий, поскольку эффективность сети прежде всего зависит от качества ее основного кабеля. Большая часть проблем, возникающих в сети, связана с проблемами физического уровня. Если планируются какие-либо значительные изменения в сети, то следует сделать полный анализ состояния кабеля для определения зон, в которых требуется обновление и замена кабеля.

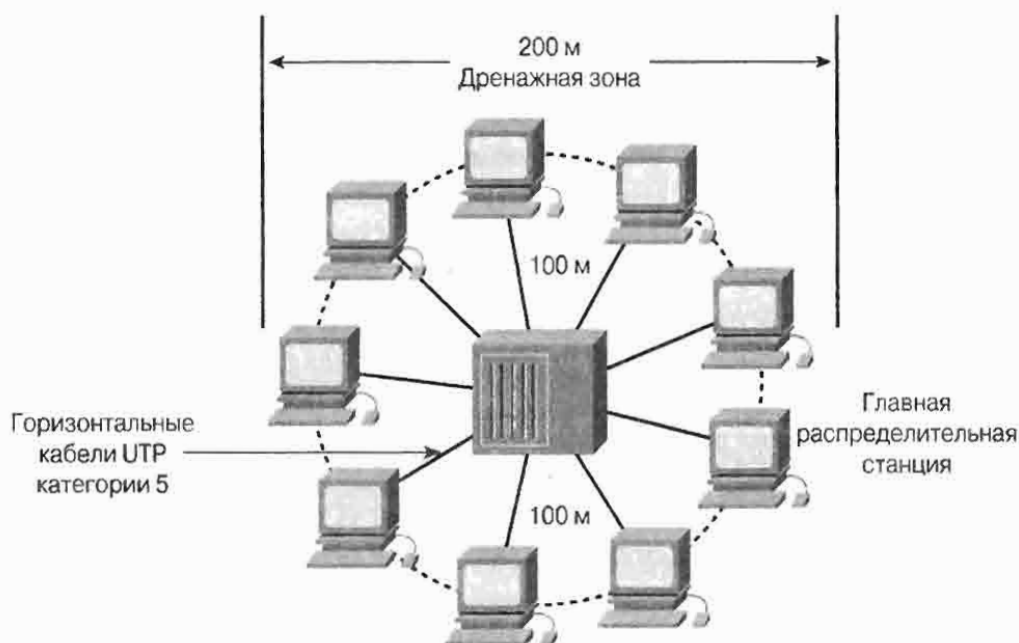


Рис. 5.30. Звездообразная топология

При проектировании новой сети или повторной прокладке кабеля, необходимо использовать, как минимум, оптоволоконный кабель в качестве магистрали и вертикальных соединений и кабель UTP пятой категории (Category 5 UTP) для горизонтальных соединений. Необходимо также учесть самые последние стандарты UTP категорий Category 5e и Category 6. Обновление кабеля должно иметь приоритет перед другими необходимыми изменениями и предприятие должно обеспечить полное и безусловное соответствие этих систем общепринятым промышленным стандартам, таким как спецификации TIA/EIA 568-B.

Стандартом TIA/EIA 568 определяется, что каждое устройство, подключенное к сети, должно быть соединено горизонтальным кабелем с центральной точкой. Это требование должно выполняться в том случае, когда все станции, которым необходим доступ в сеть, находятся в радиусе 100 метров для кабеля пятой категории Category 5 UTP Ethernet, как указывается в стандарте TIA/EIA 568-B. В табл. 5.1 перечислены типы кабелей и их характеристики.

В простой звездообразной топологии с только одним монтажным шкафом MDF включает в себя одну или более patch-панелей горизонтальных кросс-соединений (horizontal cross connect — HCC), как показано на рис. 5.31 patch-кабели HCC используются для соединения горизонтальных кабелей 1-го уровня с портами LAN-коммутаторов 2-го уровня. Восходящий порт LAN-коммутатора, в зависимости от модели, отличающийся от других портов тем что он не cross over, подсоединен к Ethernet-порту маршрутизатора 3-го уровня с использованием patch-кабеля. После выполнения этого этапа конечная станция имеет полное физическое соединение с портом маршрутизатора.

Таблица 5.1. Типы и характеристики кабелей IEEE 802.3

Характеристики	10BASE-T	10BASE-FL	100BASE-TX	100BASE-FX
Скорость передачи данных	10 Мбит/с	10 Мбит/с	100 Мбит/с	100 Мбит/с
Метод сигнализации	Внутриполосная	Внутриполосная	Внутриполосная	Внутриполосная
Передающая среда	Категория 5 UTP	Оптоволоконный кабель	Категория 5 UTP	Многомодовый оптоволоконный кабель (два strands)
Максимальная длина	100 метров	2000 метров	100 метров	2000 метров

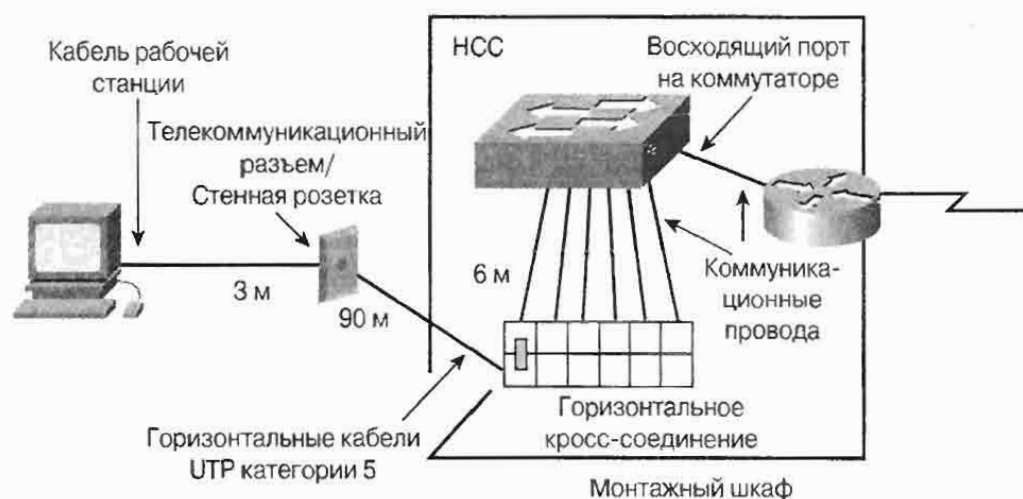


Рис. 5.31. Типичный MDF в звездообразной топологии

В тех случаях, когда в больших сетях станции выходят за 100-метровое ограничение для Category 5 UTP, часто используется более одного монтажного шкафа. При использовании нескольких монтажных шкафов создается несколько дренажных областей. Вторичные монтажные шкафы называются IDF-шкафами. Как показано на рис. 5.32, стандарты TIA/EIA 568-B определяют, что IDF должны быть подсоединены к MDF.

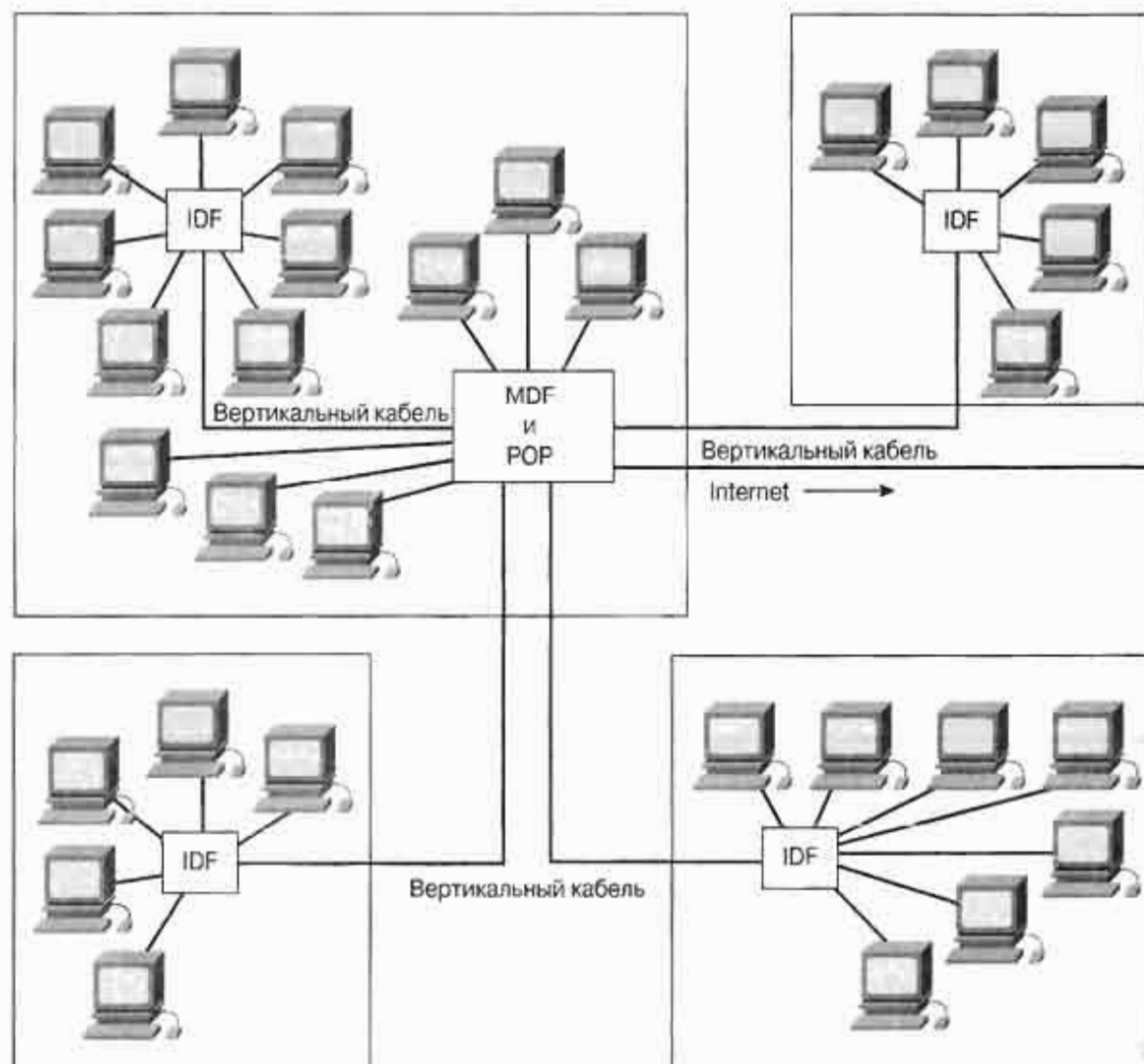


Рис. 5.32. Расширенная звездообразная топология в кампусе, состоящем из нескольких зданий

Как показано на рис. 5.33, вертикальные кросс-соединения (vertical cross connect — VCC) используется для соединения различных IDF с центральной MDF. Поскольку длина вертикального кабеля обычно превышает 100-метровое ограничение для кабеля 5-й категории UTP, для этой цели обычно используется оптоволоконный кабель, как показано на рис. 5.34.

Fast Ethernet представляет собой Ethernet, улучшенный до пропускной способности 100 Мбит/с. Этот тип сети использует ориентированную на широковещание логическую шинную топологию 10BASE-T, наряду с известным методом доступа CSMA/CD для управления доступом к передающей среде (MAC). В настоящее время стандарт Fast Ethernet включает в себя целый ряд различных стандартов, основанных на медной паре (100BASE-TX) и оптоволоконном кабеле (100BASE-FX). Он исполь-

зуются для соединения ГРС и ПРС, как показано на рис. 5.35. Во многих случаях требования к полосе пропускания сети могут быть удовлетворены путем использования коммутируемого 10BASE-TX Ethernet для настольных систем и магистралей Fast Ethernet.

В новых сетях выбор может быть сделан в пользу Gigabit Ethernet, использующей оптоволоконный кабель для вертикальных (магистральных) соединений и Fast Ethernet, использующей горизонтальные соединения CAT 5e, для настольных систем, в зависимости от финансовых возможностей организации.

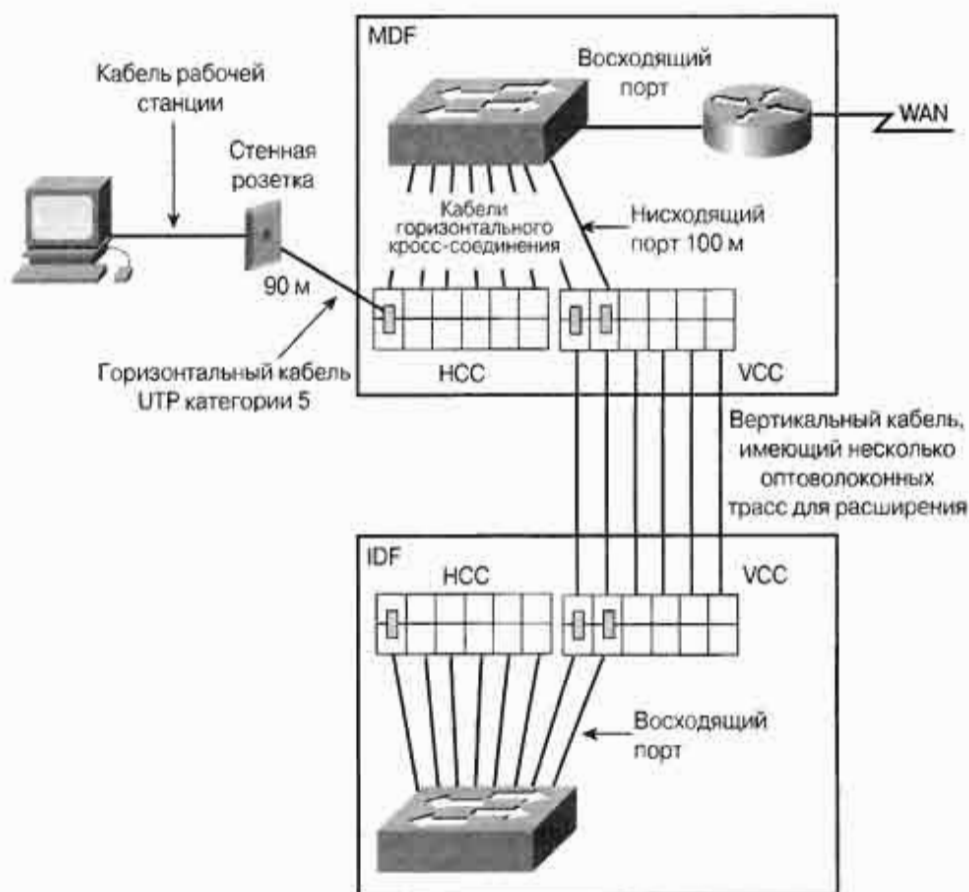


Рис. 5.33. Расширенная звездообразная топология

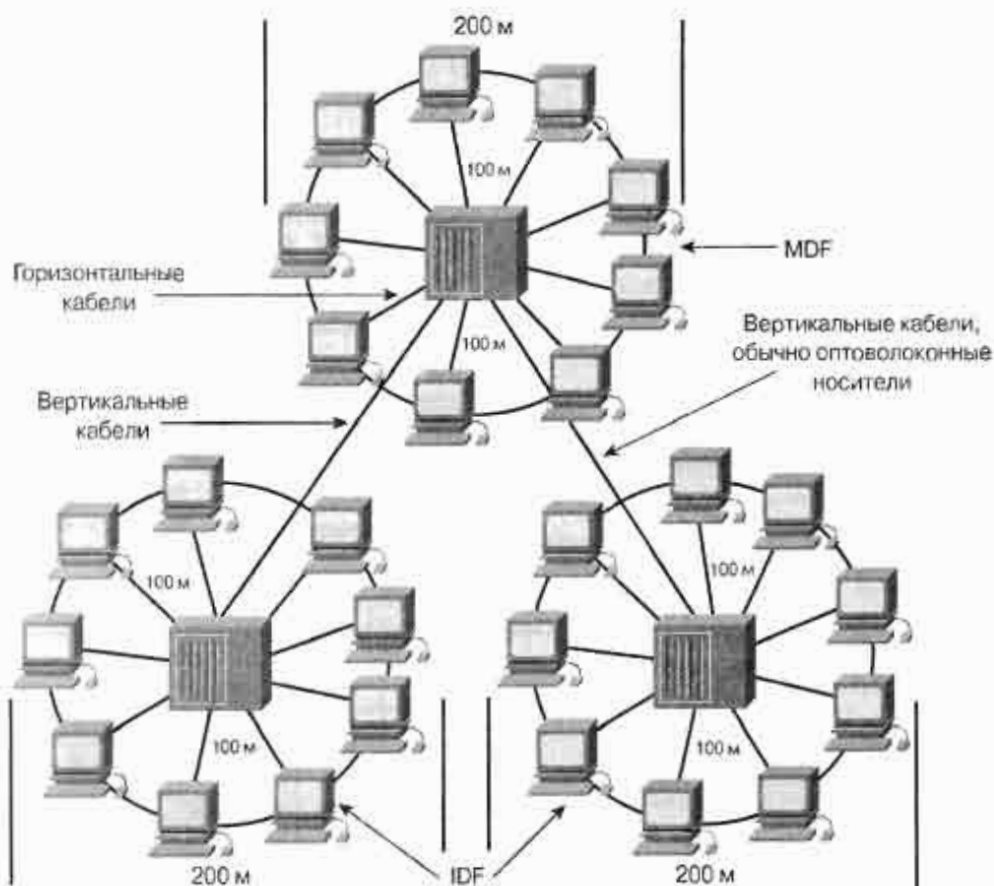


Рис. 5.34. Расширенная звездообразная топология. Вертикальные кабели

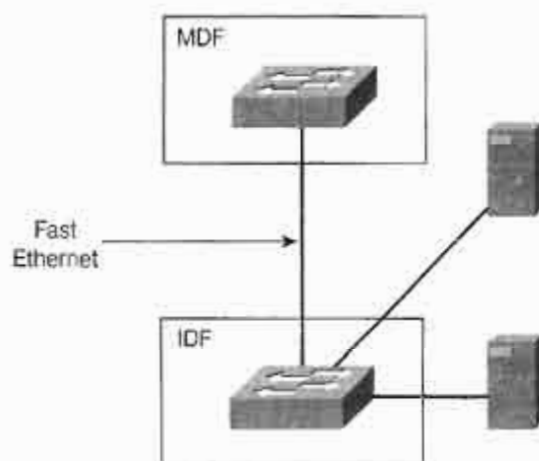


Рис. 5.35. Вертикальные кабели от MDF к IDF

Как показано на рис. 5.36, логическая диаграмма представляет собой модель сетевой топологии без точного указания всех деталей прокладки кабеля. Логическая диаграмма — это основная карта локальной сети. Элементы логической диаграммы включают в себя следующее.

- Точное расположение монтажных шкафов ГРС и ПРС.
- Тип и количество кабеля для соединения ГРС и ПРС, включая количество запасного кабеля для увеличения полосы пропускания между монтажными шкафами. Например, если вертикальный кабель между ПРС1 и ГРС используется на 80%, то можно применить две дополнительные пары для удвоения полосы пропускания.
- Подробную документацию на все кабельные трассы, как показано на рис. 5.37, идентификационные номера и порт на вертикальном или горизонтальном кросс-соединении, на котором заканчивается трасса. Например, предположим, что 203-я комната потеряла связь с сетью. Изучая врезку, можно выяснить, что эта комната использует трассу 203-1, которая заканчивается на 13-м порте горизонтального кросс-соединения. Теперь можно проверить трассу кабельным тестером, чтобы определить, вызвана ли проблема отказом на 1-ом уровне. Если это так, то для восстановления соединения можно просто использовать одну из двух других трасс, а затем заняться устранением неисправности трассы 203-1.



Рис. 5.36. Логическая диаграмма сети

IDF1- Расположение-комната XXX				
Соединение	Идентификатор кабеля	Кросс-соединения Номер пары/ Номер порта	Тип кабеля	Состояние
От IDF1 к комнате 203	203-1	НСС/Порт 13	Кабель UTP 5 категории	Используется
От IDF1 к комнате 203	203-2	НСС1/Порт14	Кабель UTP 5 категории	Не используется
От IDF1 к комнате 203	203-3	НСС2/Порт 3	Кабель UTP 5 категории	Не используется
От IDF1 к MDF	IDF1-1	VCC1/Порт 1	Многомодовый оптоволоконный кабель	Используется
От IDF1 к MDF	IDF1-2	VCC1/Порт 2	Многомодовый оптоволоконный кабель	Используется

Рис. 5.37. Пример описания кабельных трасс

Проектирование 2-го уровня топологии локальной сети

Наиболее типичным устройством 2-го уровня (за исключением карты сетевого интерфейса, которую должна иметь каждая рабочая станция) является LAN-коммутатор. Устройства этого уровня определяют размеры коллизийных и широковещательных доменов. В настоящем разделе рассматривается реализация коммутации локальных сетей на 2-ом уровне.

Коллизии и размер коллизийного домена представляют собой два фактора, негативно влияющих на эффективность работы сети. Используя коммутацию, можно микросегментировать сеть, устранив таким образом коллизии, и уменьшить размеры коллизийных доменов. Как показано на рис. 5.38, еще одна важная черта коммутатора локальной сети состоит в его способности распределять полосу пропускания по портам и предоставлять, таким образом, большую полосу вертикальным и восходящим кабелям, а также серверам. Такой тип коммутации называется асимметричным. Он обеспечивает коммутацию портов с разными полосами пропускания, например, сочетание портов со скоростями 10 и 100 Мбит/с.

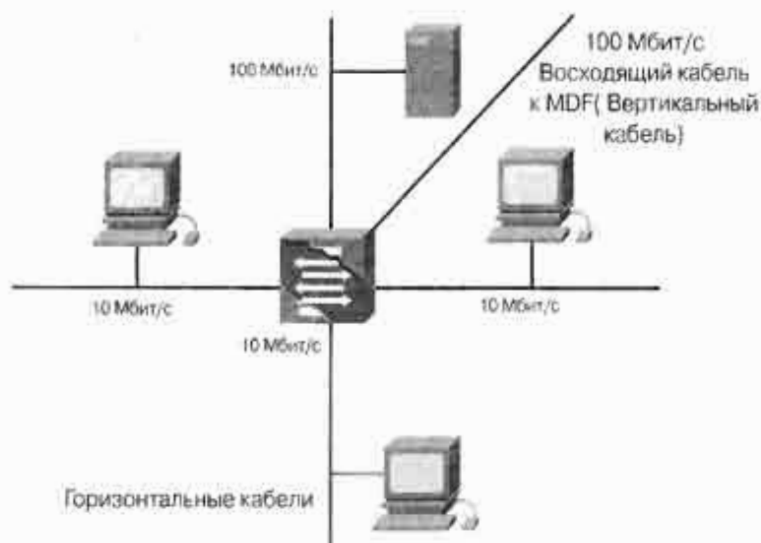


Рис. 5.38. Асимметричная коммутация

Как было сказано ранее, микросегментация означает использование мостов и коммутаторов для повышения эффективности рабочей группы или магистрали. Обычно повышение эффективности таким способом включает в себя Ethernet-коммутацию. Коммутаторы могут использоваться вместе с концентраторами для обеспечения соответствующего уровня эффективности для разных пользователей и серверов, как показано на рис. 5.39. Вследствие своей невысокой относительной стоимости (с учетом количества портов) все чаще новые сети строятся исключительно на использовании коммутаторов.

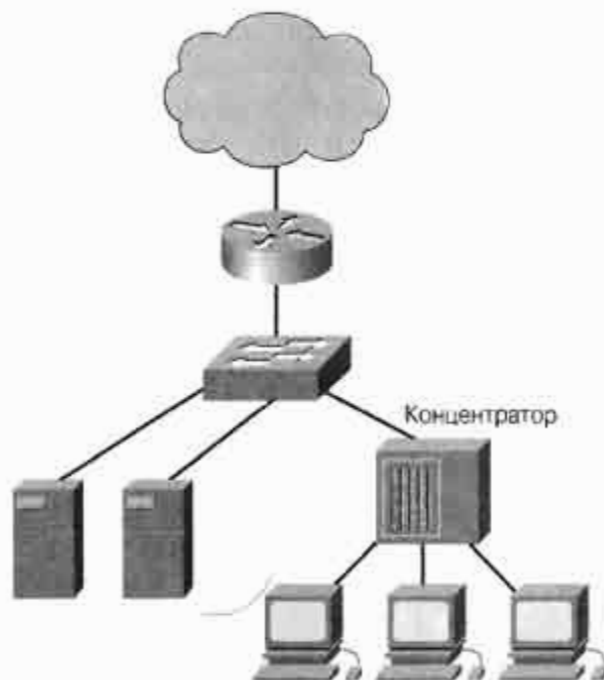


Рис. 5.39. Уменьшение вероятности перегрузки сети

Если коммутирующее оборудование локальной сети установлено в ГРС и ПРС и между ними пролегает вертикальный кабель, то по этому кабелю передаются все данные между ГРС и ПРС. Следовательно, пропускная способность этой трассы должна быть больше, чем у трасс между ПРС и рабочими станциями.

Трассы горизонтального кабеля используют пятую категорию UTP (рис. 5.40), поэтому ни одно кабельное снижение не должно превышать 100 метров. Это позволяет использовать каналы 10 или 100 Мбит/с. В обычных условиях 10 Мбит/с соответствуют горизонтальному кабельному снижению. Поскольку коммутаторы асимметричных локальных сетей позволяют совместное использование портов с полосой пропускания 10 и 100 Мбит/с на одном коммутаторе, следующей задачей является определение числа таких портов, необходимых ГРС и каждой ПРС. Эта задача может быть решена путем повторного изучения требований пользователей, касающихся числа снижений горизонтального кабеля в одной комнате и общего числа снижений в дренажной области, а также числа вертикальных кабельных трасс.

Например, предположим, что в соответствии с требованиями пользователей в каждой комнате должно быть установлено по четыре горизонтальных кабельных трассы. ПРС, обслуживающая дренажную зону, охватывает восемнадцать комнат. Путем несложных арифметических расчетов получаем число портов, равное семи-десяти двум.

Для определения размеров коллизийного домена необходимо знать, сколько хостов физически подключены к одному порту коммутатора. Этот фактор также влияет на полосу пропускания, доступную каждому отдельно взятому хосту. В идеальном случае только один хост подключен к порту коммутатора. Это означает,

что размер коллизийного домена равен двум (хост-отправитель и хост-получатель). Поскольку такой домен имеет небольшой размер, то в нем практически не должно быть коллизий при обмене данными между двумя хостами. Другой способ реализации коммутации локальной сети – это установка на порты коммутатора совместно используемых концентраторов. Таким образом, несколько хостов подключаются к одному порту коммутатора, как показано на рис. 5.41. Как показано на рис. 5.42, все хосты, подключенные к совместно используемому концентратору, используют один и тот же коллизийный домен и одну и ту же полосу пропускания. На рис. 5.43 приведен пример расчета полосы пропускания для одного пользователя в среде Ethernet совместного пользования. В современных проектах сетей не рекомендуется подсоединять 24 пользователей к одному концентратору с полосой пропускания 10 Мбит/с с последующим подключением к одному порту коммутатора.

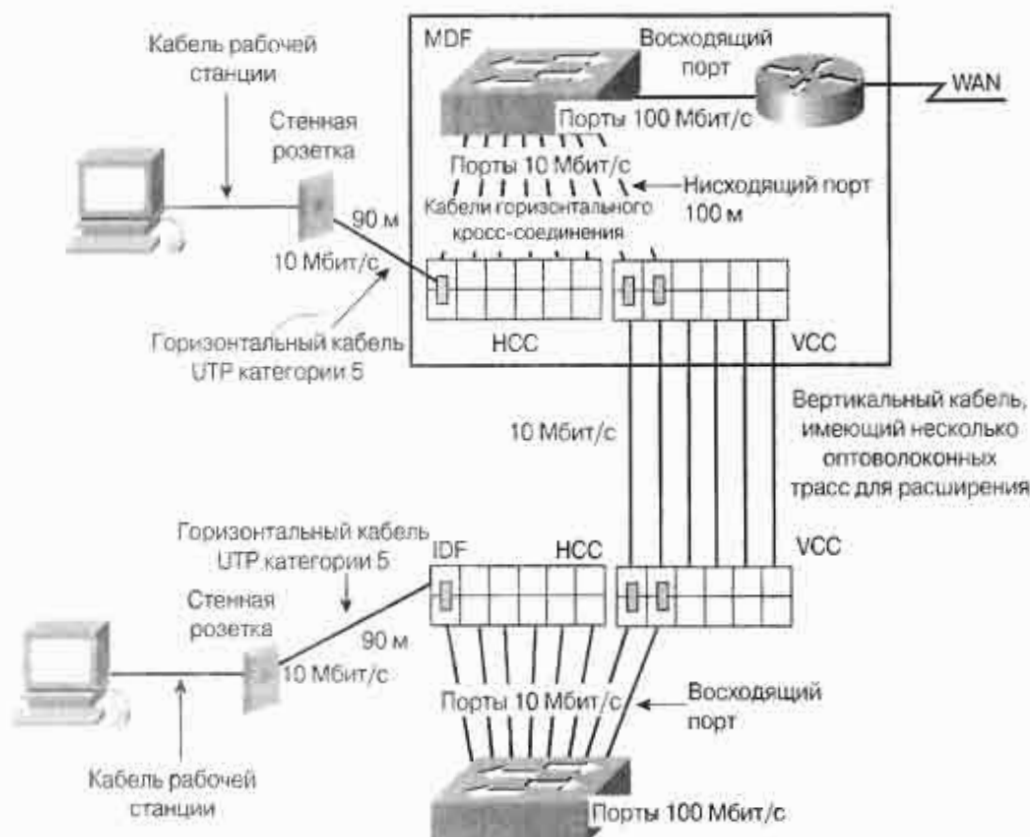
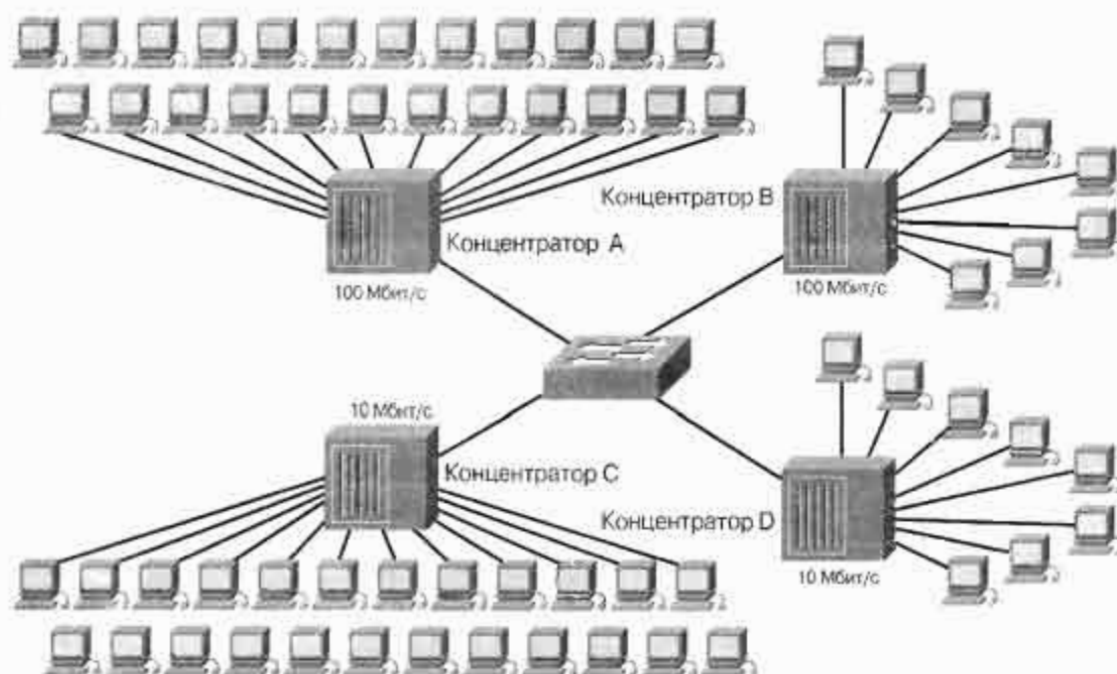
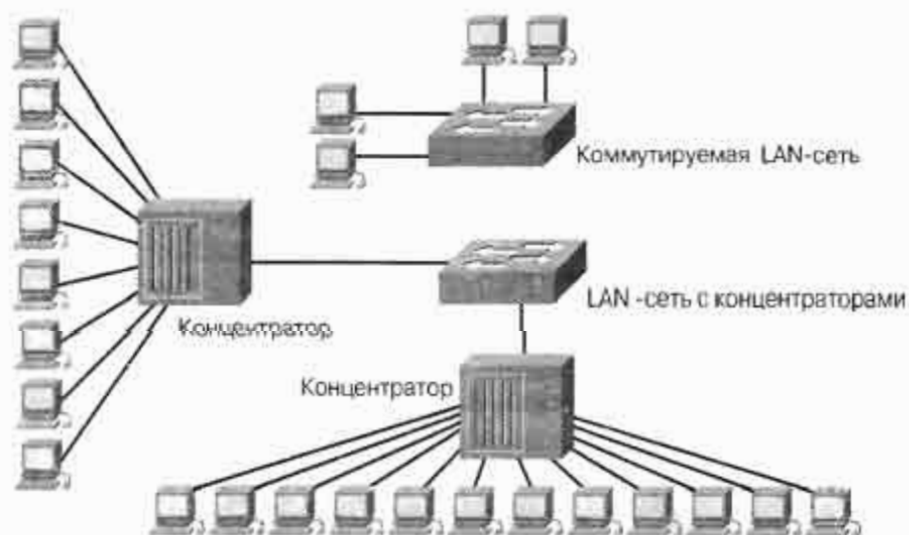


Рис. 5.40. Коммутация 2-го уровня



Концентратор А: Коллизийный домен = 24 узла
 Средняя полоса пропускания = $100 \text{ Мбит/с} / 24 \text{ узла} = 4,167 \text{ Мбит/с}$ на один узел
 Концентратор В: Коллизийный домен = 8 узлов
 Средняя полоса пропускания = $100 \text{ Мбит/с} / 8 \text{ узлов} = 12,5 \text{ Мбит/с}$ на один узел
 Концентратор С: Коллизийный домен = 24 узла
 Средняя полоса пропускания = $10 \text{ Мбит/с} / 24 \text{ узла} = 0,4167 \text{ Мбит/с}$ на один узел
 Концентратор D: Коллизийный домен = 8 узлов
 Средняя полоса пропускания = $10 \text{ Мбит/с} / 8 \text{ узлов} = 1,25 \text{ Мбит/с}$ на один узел

Рис. 5.41. Размер коллизийного домена при использовании концентраторов



- В простой среде коммутируемой LAN-сети размер коллизийного домена равен двум узлам
- При использовании концентраторов размер коллизийного домена возрастает, а полоса пропускания совместно используется многими узлами

Рис. 5.42. Коллизийные домены коммутатора 2-го уровня

Следует заметить, что некоторые ранние модели коммутаторов, такие как Catalyst 1700, в действительности не могут делить коллизионный домен и полосу пропускания, поскольку не поддерживают множественное назначение MAC-адресов каждому порту. В этом случае число ARP-запросов и широковещательных рассылок становится большим.

В большинстве случаев концентраторы среды с общим доступом используются в коммутируемой среде локальных сетей для увеличения количества точек подключения на концах горизонтальных кабельных трасс, как показано на рис. 5.43. Такой подход является приемлемым, однако нужно гарантировать, что размеры коллизионных доменов не будут увеличиваться и требования, касающиеся полосы пропускания к хосту, будут выполнены согласно спецификациям, собранным на соответствующем этапе проектирования сети.

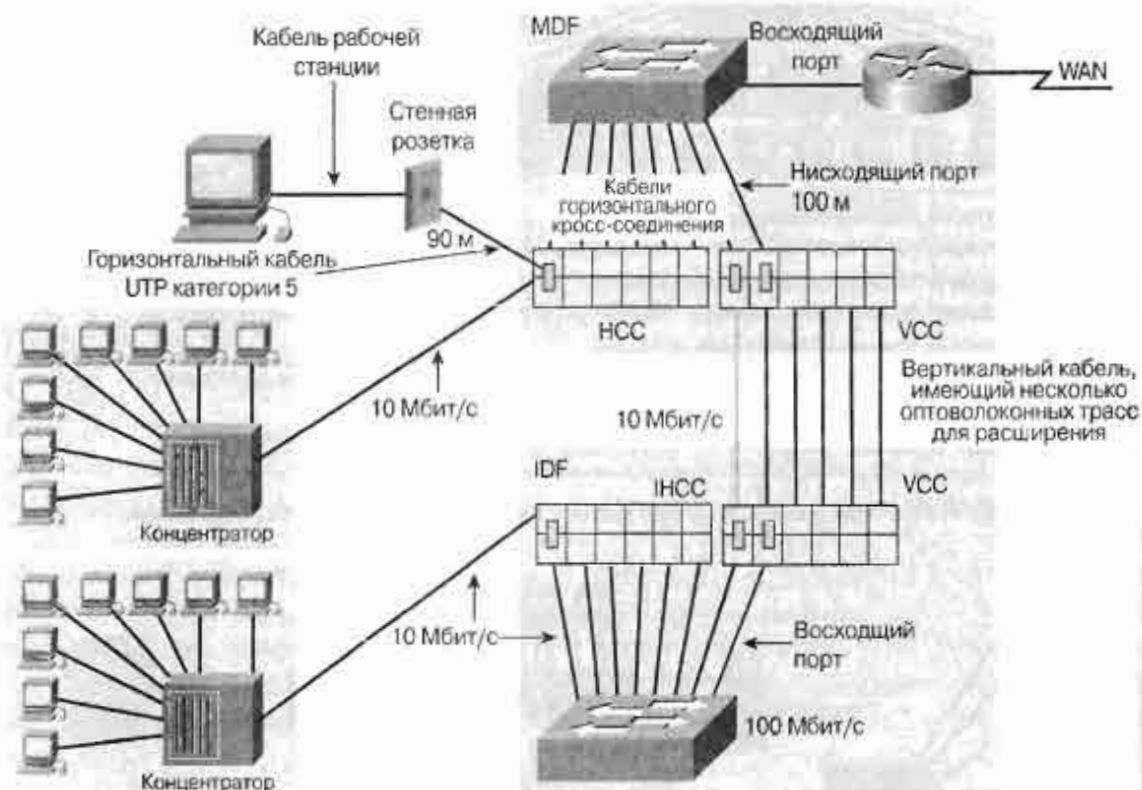


Рис. 5.43. Концентраторы можно использовать с целью создания большего количества точек подключения для хоста.

Переход на большую полосу пропускания на 2-ом уровне

При росте сети растет и потребность в большей полосе пропускания. В вертикальных соединениях неиспользуемое оптоволокно можно применить для связи с портом коммутатора, имеющим полосу пропускания 100 Мбит/с. Полоса пропускания сети, показанной на рис. 5.44, удвоена по сравнению с полосой пропускания вертикального кабеля сети, представленной на рис. 5.43. Это происходит за счет внедрения еще одной линии.

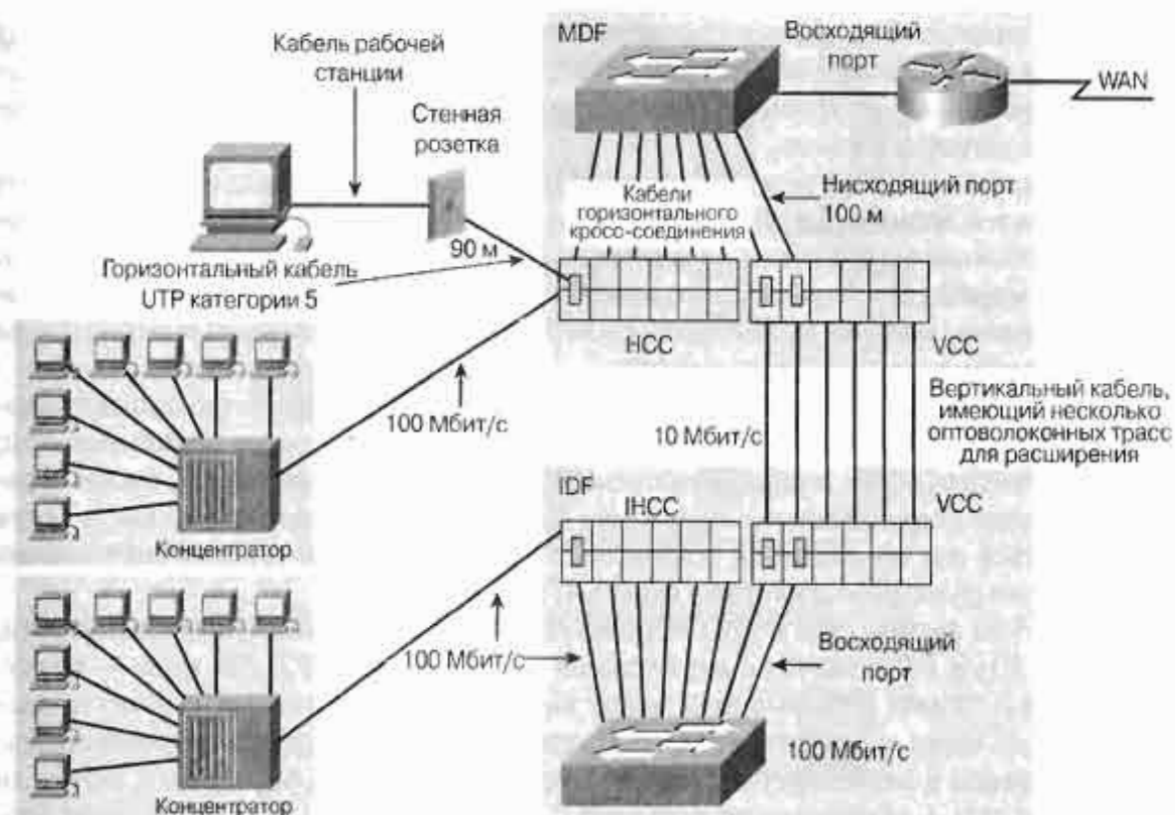


Рис. 5.44. Уровень 2: увеличение полосы пропускания сети

Проектирование 3-го уровня топологии локальной сети

Устройства 3-го (сетевого) уровня (рис. 5.45), такие как маршрутизаторы, могут использоваться для создания отдельных сегментов локальной сети и обеспечения обмена информацией между сегментами, основываясь на адресации 3-го уровня, т.е. на IP-адресах. Внедрение устройств 3-го уровня, например маршрутизаторов, позволяет осуществить сегментацию локальной сети на обособленные физические и логические сети. Маршрутизаторы также позволяют подключаться к распределенным сетям (wide-area network — WAN), таким как Internet.

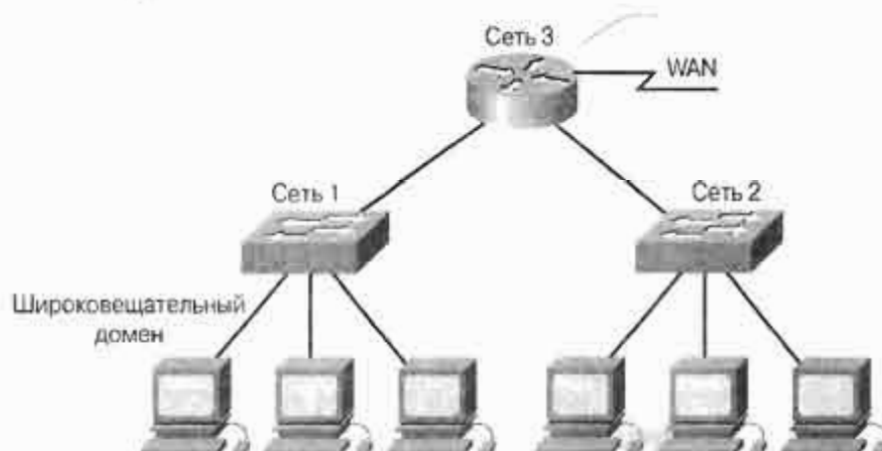


Рис. 5.45. Установка в сети маршрутизатора 3-го уровня

Маршрутизация 3-го уровня определяет транспортировку потока данных между отдельными физическими сегментами сети такими, как IP-сеть и подсеть, основываясь на адресации 3-го уровня. Маршрутизатор представляет собой одно из наиболее мощных устройств в сети.

Как известно, маршрутизатор перенаправляет пакеты данных, основываясь на адресах пунктов назначения. Вместе с тем, маршрутизатор не перенаправляет широковещательные рассылки локальных сетей, такие как ARP-запросы. Следовательно, интерфейс маршрутизатора рассматривается как точка входа-выхода широковещательного домена, которая предотвращает переход широковещательных рассылок из одних сегментов локальной сети в другие.

Одной из важнейших характеристик сети является общее количество широковещательных рассылок, таких как ARP-запросы. Используя виртуальные локальные сети, можно ограничить поток широковещательных сообщений внутри сети и, таким образом, уменьшить широковещательный домен (рис. 5.46). Виртуальные сети могут также использоваться для обеспечения безопасности, путем создания групп в виртуальных сетях согласно функциям этих групп (рис. 5.47).

На рис. 5.46 физические порты используются для назначения виртуальной сети. Порты P0, P1, и P4 назначены виртуальной сети 1, а порты P2, P3, и P5 — виртуальной сети 2. Обмен информацией между виртуальными сетями 1 и 2 может происходить только через маршрутизатор. Эта схема ограничивает размеры широковещательных доменов и использует маршрутизатор для того, чтобы определить, может ли виртуальная сеть 1 обмениваться данными с виртуальной сетью 2. Это создает возможность увеличения безопасности, основанную на назначениях виртуальной сети.

Маршрутизаторы обеспечивают расширяемость, так как они могут служить в качестве брандмауэров для широковещательных рассылок, как показано на рис. 5.48. Кроме того, поскольку адреса 3-го уровня обычно являются структурированными, маршрутизаторы могут обеспечивать большую расширяемость путем разделения сетей и подсетей, и, следовательно, структурируя эти адреса. Способы, которыми можно достичь большей расширяемости сетей, показаны на рис. 5.48. Способы достижения большей структурированности и масштабируемости сети показаны на рис. 5.49.

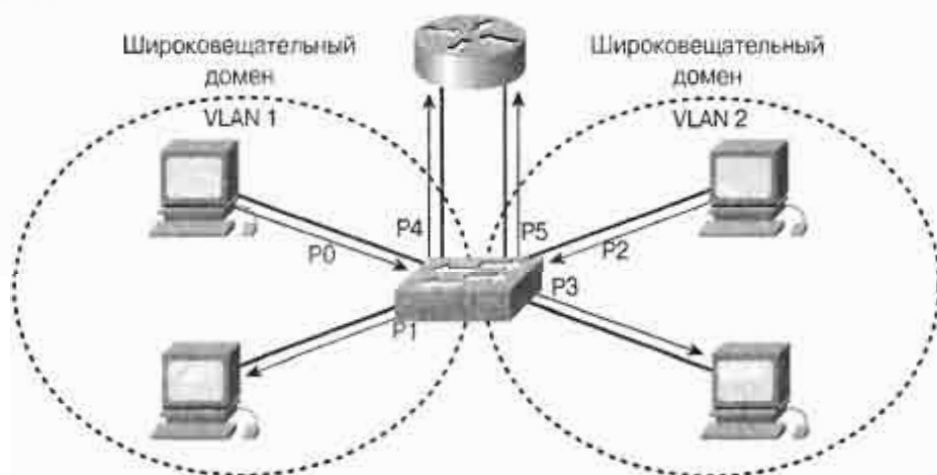


Рис. 5.46. Взаимодействие между виртуальными локальными сетями

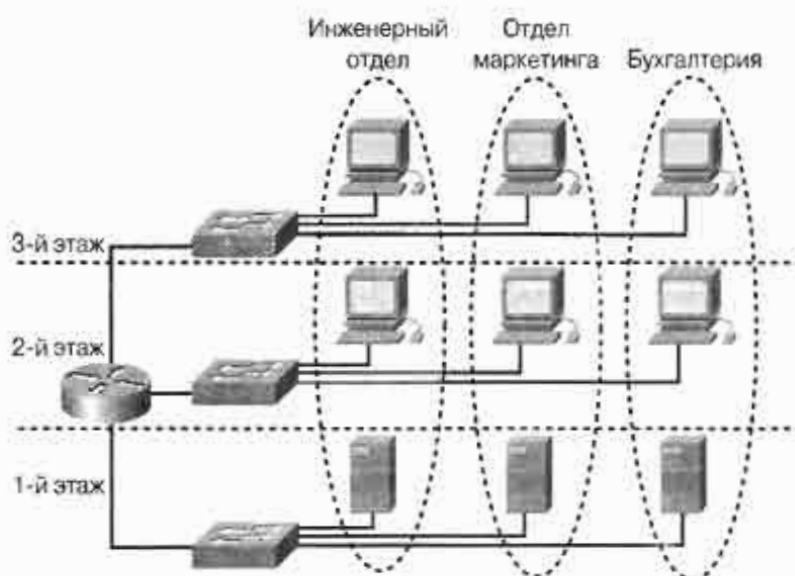


Рис. 5.47. Реализация виртуальных локальных сетей

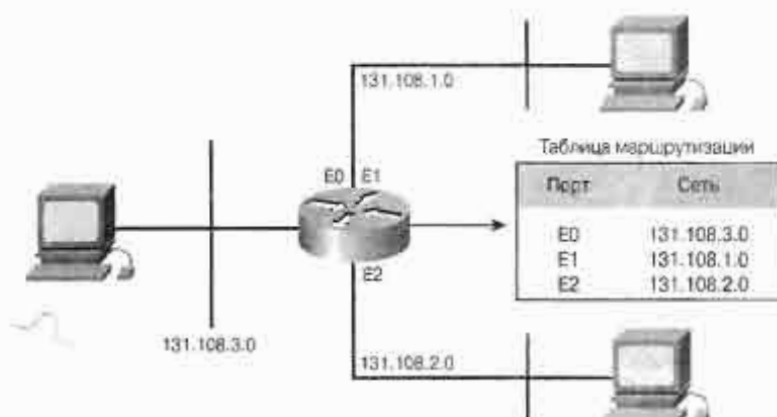


Рис. 5.48. Маршрутизаторы создают логическую структуру сети

Логический адрес	Физические устройства сети
x.x.x.1-x.x.x.10	Порты маршрутизатора, LAN-сети и WAN-сети
x.x.x.11-x.x.x.20	Коммутаторы LAN-сети
x.x.x.21-x.x.x.30	Серверы предприятия
x.x.x.31-x.x.x.60	Серверы рабочих групп
x.x.x.61-x.x.x.254	Узлы

Рис. 5.49. Преобразование логической адресации в прямую адресацию физических сетей

Технология маршрутизации обеспечивает фильтрацию широковещательных и многоадресных рассылок канального уровня. Добавляя порты маршрутизатора с дополнительными адресами сети (network address) или подсети, можно сегментировать сеть в соответствии с текущими требованиями. Адресация и маршрутизация, используемые сетевыми протоколами, обеспечивают встроенное расширение. При решении вопроса о том, что использовать — маршрутизатор или коммутатор, необходимо ответить на вопрос:

"Какую проблему необходимо решить?" Если проблема связана скорее с протоколом, чем с конкуренцией в сети, то следует использовать маршрутизатор. Маршрутизаторы решают проблемы, связанные с чрезмерным широковещанием, плохо масштабируемыми протоколами, аспектами безопасности и адресацией сетевого уровня. В то же время, маршрутизаторы стоят дороже и сложнее в настройке, чем коммутаторы.

В структурированной кабельной схеме 1-го уровня легко создавать многочисленные физические сети путем простого соединения вертикальных и горизонтальных кабелей с соответствующим коммутатором 2-го уровня. В следующих главах рассказывается, как подобный подход обеспечивает надежную реализацию защиты. И, наконец, следует напомнить, что маршрутизатор в локальной сети является центральной точкой прохождения потока данных.

Использование маршрутизаторов для логического структурирования

Как показано на рис. 5.50, маршрутизаторы можно использовать для реализации IP-подсетей путем структурирования адресов. Мосты и маршрутизаторы должны отбрасывать все неизвестные адреса с каждого порта. Маршрутизаторы помогают хостам, использующим протоколы адресации сетевого уровня, отыскать другие хосты, без использования лавинной передачи. Если адрес пункта назначения является локальным, то посылающий хост может инкапсулировать данные в заголовок канального уровня и отправить фрейм непосредственно адресату. Маршрутизатор не видит этот фрейм и, естественно, не нуждается в лавинной передаче. Есть вероятность, что передающему хосту придется использовать ARP, что повлечет за собой широковещание. Однако, широковещание — локальное явление и не распространяется маршрутизатором. В случае, когда адресат не является локальным, посылающая станция передает пакеты маршрутизатору. Маршрутизатор отправляет фреймы по назначению или к следующему переходу, основывая свой выбор на собственной таблице маршрутизации. Исходя из приведенной выше функциональности, можно сделать вывод, что в крупных, расширяемых сетях необходимо использовать маршрутизаторы.

На рис. 5.51 приведен пример реализации системы, в которой есть несколько физических сетей. Весь поток данных из сети 1, предназначенный для сети 2, должен пройти через маршрутизатор. В приведенной реализации сети 1 и 2 представляют собой два широковещательных домена. Эти две сети имеют уникальные IP-адресации (адресные схемы сеть/подсеть). В структурированной кабельной схеме 1-го уровня легко создать несколько физических сетей путем добавления отрезков горизонтальных и вертикальных кабелей к коммутатору 2-го уровня. Такая реализация обеспечивает высокую степень надежности. Кроме того, маршрутизатор является центральной точкой сети LAN для потоков данных, пересылаемых в пункты назначения.

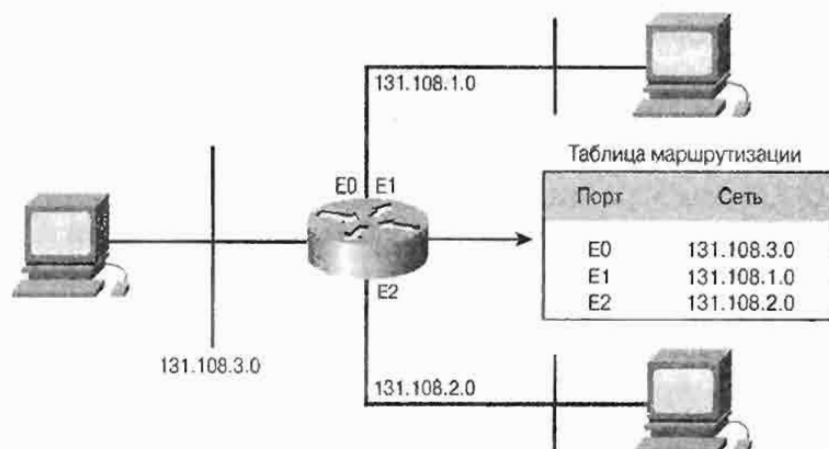


Рис. 5.50. Использование маршрутизаторов для создания логической структуры

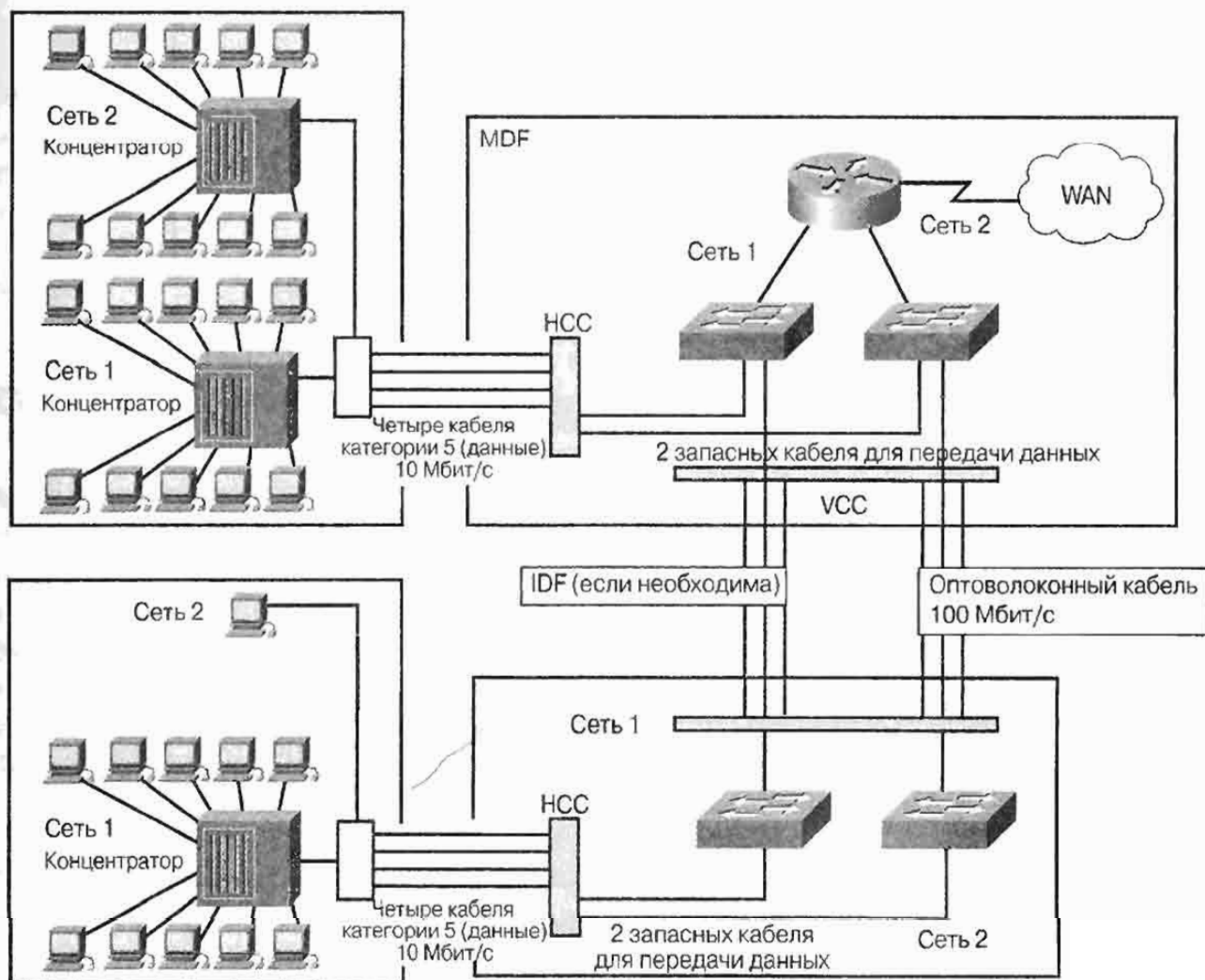


Рис. 5.51. Сегментация на уровне 3

После разработки схемы IP-адресации для заказчика следует составить соответствующие документы для каждого ее участка и для сети внутри этого участка. Следует установить стандартное соглашение для адресации важнейших хостов в сети, как показано на рис. 5.52. Эта схема не должна содержать противоречий внутри всей сети. После создания карты адресации проектировщик получает снимок сети, как показано на рис. 5.53, а создание физической карты, изображенной на рис. 5.54 поможет при устранении сетевых неисправностей.

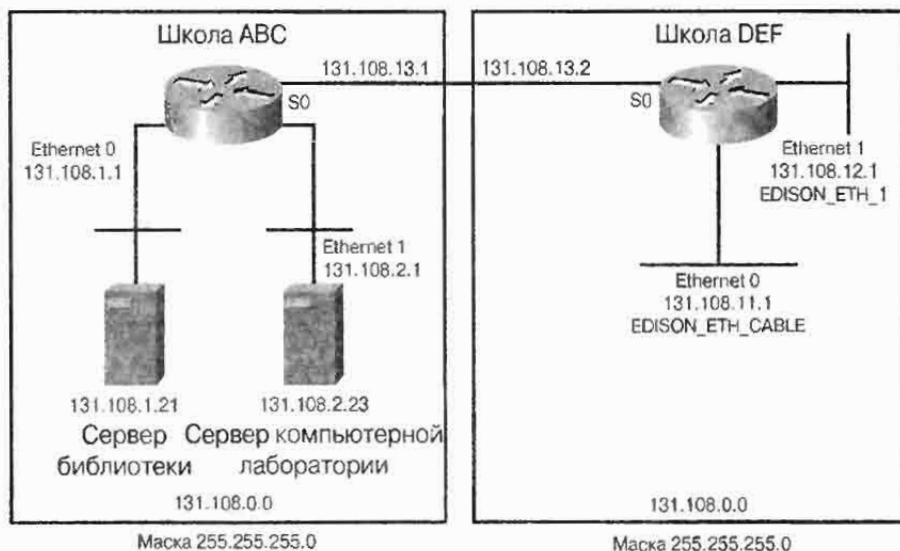


Рис. 5.52. Карта адресации

IP-сеть 131.108.0.0
Маска подсети= 255.255.255.0

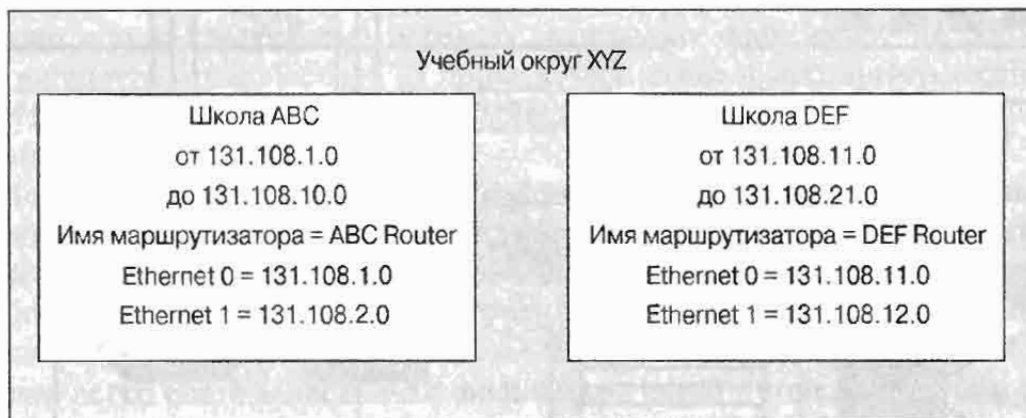


Рис. 5.53. Логическая карта сети

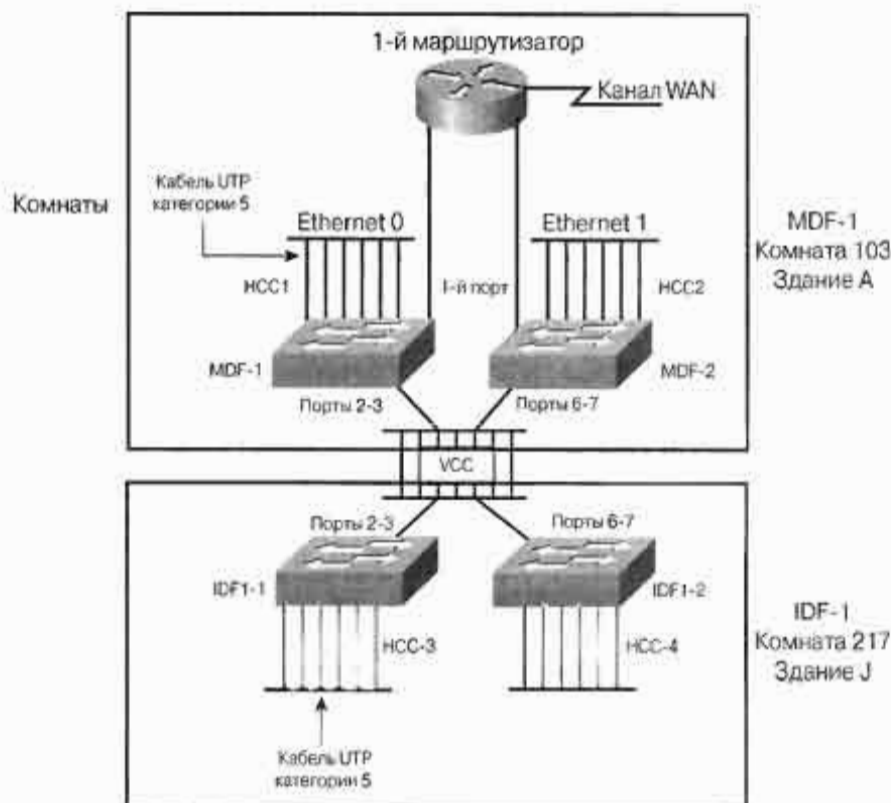


Рис. 5.54. Физическая карта сети

Основы применения мостов и коммутаторов на 2-м уровне

В настоящем разделе рассматриваются функции коммутаторов и мостов, которые в эталонной модели OSI рассматриваются как устройства 2-го уровня. В ней обсуждаются методы, используемые коммутаторами для передачи фреймов и способы фильтрации фреймов. Взаимодействие с коммутаторами и мостами помогает понять, каким образом мосты и коммутаторы узнают адреса подсоединенных к ним устройств. Необходимо понять принципы сегментации в локальных сетях и сущность коллизионных доменов, поскольку не все сети LAN могут быть сегментированы. Сегментация представляет собой метод, использование которого позволяет предотвратить падение производительности сети LAN при увеличении ее размера.

По мере роста сети и увеличения количества ее пользователей возрастает потребность в полосе пропускания, необходимой для работы приложений пользователей. Возникающие в сети переполнения могут существенно замедлить работу сети и достичь того уровня, при котором она становится практически неработоспособной. Пользователи склонны проявлять нетерпение и раздражение когда приложение работает слишком медленно. Одним из наиболее эффективных средств решить проблему заторов является разбиение сети на области меньшего размера, называемые сегментами. Такие сегменты могут быть созданы, например, с помощью мостов или коммутаторов, которые ограничивают количество устройств, приходящихся на один сетевой сегмент.

Коммутатор концентрирует соединения в одной точке, что делает более эффективной передачу данных. Фреймы коммутируются (передаются) с входных портов (интерфейсов) на выходные порты. Каждый порт обеспечивает всю доступную полосу пропускания каждому соединению с рабочей станцией.

В типичном концентраторе Ethernet все порты подсоединены к общей задней панели, которая осуществляет физическое соединение с концентратором, а все устройства, подсоединенные к концентратору, совместно используют полосу пропускания сети. Если две станции устанавливают между собой сеанс связи, использующий значительную часть полосы пропускания, то производительность работы всех других станций, подсоединенных к концентратору, значительно уменьшается. Для уменьшения такого отрицательного воздействия коммутатор рассматривает каждый свой интерфейс как индивидуальный сегмент. Когда станциям, подсоединенным к различным интерфейсам, требуется осуществить сеанс связи, коммутатор пересылает фреймы с одного интерфейса на другой практически со скоростью света, в результате чего каждый сеанс связи получает полностью всю полосу пропускания.

Для осуществления эффективной коммутации фреймов между интерфейсами коммутатор поддерживает адресную таблицу. При поступлении каждого нового фрейма коммутатор логически связывает MAC-адрес станции, отправившей этот фрейм (станции-отправителя), с интерфейсом, на котором он был принят. Ниже приведены основные функции Ethernet-коммутатора.

- Изоляция перемещения данных в каждом сегменте от других сегментов.
- Увеличение полосы пропускания, приходящейся на каждого пользователя за счет создания коллизионных доменов меньшего размера.

Первая функция коммутатора состоит в изоляции перемещения данных в разных сегментах сети, под которыми понимаются области сети меньшего размера, образующиеся вследствие использования таких Ethernet-коммутаторов. Каждый сегмент использует метод доступа CSMA/CD для поддержки передачи данных между пользователями этого сегмента. Такая сегментация позволяет нескольким пользователям, находящимся в разных сегментах, одновременно осуществлять передачу, не замедляя работу сети. Коммутаторы Ethernet фильтруют потоки данных, перенаправляя дейтаграммы на соответствующий порт или порты на основе MAC-адреса 2-го уровня. Вторая функция коммутатора Ethernet состоит в увеличении полосы пропускания, приходящейся на каждого пользователя, за счет создания коллизионных доменов меньшего размера.

Коммутатор Fast Ethernet позволяет осуществлять сегментацию сети LAN (разбиение сети на коллизионные домены меньшего размера), предоставляя каждому сегменту выделенный канал (аналогичный полосе движения на автотрассе) с полосой пропускания до 100 Мбит/с. Серверы с большой нагрузкой могут иметь свои единоличные каналы с полосой пропускания 100 Мбит/с или даже 1000 Мбит/с. В современных сетях коммутаторы Fast Ethernet и Gigabit Ethernet используются в качестве «магистралей» сети LAN, а коммутаторы Ethernet с портами 10 Мбит/с и 100 Мбит/с используются для соединения настольных компьютерных систем в рабочих группах. По мере того, как становятся все более популярными новые приложения в настольных системах, такие как мультимедийные приложения и видеоконференции, которым требуется большая полоса пропускания, индивидуальным настольным компьютерам для связи с сетью могут выделяться свои собственные выделенные каналы 100 Мбит/с. современные локальные сети, как правило полностью строятся на использовании коммутаторов и используют для магистралей каналы 100 Мбит/с или 1000 Мбит/с, а для настольных рабочих станций каналы 10/100 Мбит/с.

Фильтрация фреймов коммутаторами и мостами

Мосты могут фильтровать фреймы на основе любых полей заголовка 2-го уровня. Например, мост может быть запрограммирован на отбрасывание всех фреймов, которые поступают из определенной сети. Поскольку информация канального уровня часто включает в себя ссылку на протокол более высокого уровня, фильтрация может производиться и по этому параметру. Кроме того, фильтры могут оказаться полезными при обработке ненужных широковещательных пакетов и пакетов многоадресной рассылки. Часто функции моста часто выполняются не отдельным устройством, а встраиваются в аппаратное обеспечение маршрутизатора.

После того, как мост построил свою адресную таблицу, он готов к работе. При получении мостом фрейма просматривается адрес отправителя. Если адрес фрейма указывает на локальное устройство, то фрейм игнорируется. Если фрейм адресован другой сети LAN, то мост копирует его для передачи в эту сеть. Игнорирование фрейма называется фильтрацией. Копирование фрейма для передачи на другой порт называется пересылкой.

Типы фильтрации

При типовой фильтрации выполняются следующие операции:

- локальные фреймы сохраняют локальный характер и не пересылаются;
- фреймы, адресованные удаленным сегментам, пересылаются в эти сегменты.

При использовании фильтрации по адресу отправителя или получателя могут быть выполнены следующие действия:

- определенной станции может быть запрещена отправка фреймов за пределы ее собственной локальной сети;
- заблокировать получение определенной станцией получение всех “внешних” фреймов, ограничивая тем самым круг станций с которыми она может осуществлять связь.

Оба типа фильтрации предоставляют некоторый уровень контроля межсетевого обмена данными и позволяют повысить уровень безопасности в сети.

Большинство мостов Ethernet могут фильтровать широковещательные фреймы и фреймы многоадресной рассылки. Бывают случаи, когда какое-либо устройство функционирует неправильно и непрерывно рассылает широковещательные фреймы, которые в принципе бесконечное число раз копируются в сети. Это явление, называемое *широковещательной лавиной (broadcast storm)* или *широковещательным штормом*, способно свести производительность работы сети к нулю. Если мост может фильтровать широковещательные фреймы, то вероятность широковещательной лавины значительно уменьшается.

В настоящее время мосты могут также осуществлять фильтрацию по типу протокола сетевого уровня. Это в значительной степени стирает различие между мостами и маршрутизаторами. Маршрутизатор функционирует на сетевом уровне и использует протокол маршрутизации для выбора маршрута передачи данных по сети. Мост, осуществляющий расширенную фильтрацию обычно называют “брутером” (калька с англ. Brouter, образованного, в свою очередь из слов bridge — мост, и router — маршрутизатор). Такое устройство осуществляет фильтрацию с использованием информации сетевого уровня, однако не использует протокол маршрутизации для выбора маршрута. Функции моста часто выполняются не отдельным устройством, а встраиваются в аппаратное обеспечение маршрутизатора.

Резюме

Ниже приводятся основные положения, которые были обсуждены в настоящей главе.

- Сочетание более мощных компьютеров/рабочих станций и интенсивно использующих сеть приложений вызвало необходимость в полосе пропускания, значительно большей, чем 10 Мбит/с, доступной в сетях LAN общего (совместного доступа) Ethernet/802.3.
- В связи с тем, что все большее количество пользователей используют сеть для совместной работы с большими файлами, для доступа к файловым серверам и для выхода в Internet, в локальных сетях все чаще возникает переполнение.
- В сегментированной локальной сети Ethernet передаваемые между сегментами данные проходят через мосты, коммутаторы и маршрутизаторы. Коммутатор делит сеть LAN на микросегменты, создавая из одного большого коллизийного домена несколько доменов, свободных от коллизий.
- Сеть LAN, использующая топологию коммутируемого Ethernet, превращается в сеть, которая ведет себя так, как если бы она имела только два узла — передающий и принимающий.
- Коммутаторы осуществляют высокоскоростную передачу, просматривая в пакете MAC-адрес 2-го уровня, во многом аналогично тому как это делают мосты.
- Ethernet-коммутация увеличивает доступную в сети ширину полосы пропускания за счет создания выделенных сетевых сегментов (соединений типа “точка-точка”) и соединяя их внутри коммутатора в виртуальную сеть.
- Симметричной называется коммутация, при которой все порты коммутатора имеют одну и ту же полосу пропускания.
- Под виртуальной локальной сетью VLAN понимается объединение сетевых устройств или пользователей, не ограниченное физическим сегментом коммутатора.
- Главная функция протокола связующего дерева (Spanning Tree Protocol — STP) состоит в создании возможности существования в сети нескольких проходящих через коммутаторы или мосты маршрутов между отправителем и получателем, предотвращая вместе с тем увеличение задержки из-за возникновения петель.
- Одним из наиболее важных факторов, определяющих быструю и устойчивую работу сети является ее проектирование.
- Если при проектировании сети были допущены ошибки, то возможно возникновение непредвиденных проблем, ставящих под угрозу само функционирование сети.
- Целью проектирования локальной сети LAN является обеспечение функциональности, масштабируемости, адаптируемости и управляемости сети.

Процесс проектирования сети включает в себя:

- Сбор требований и пожеланий пользователей;
- Определение типовых режимов передачи данных в настоящее время и в будущем с учетом роста сети и размещения серверов

- Выбор устройств 1-го, 2-го и 3-го уровней, а также топологии локальной (LAN) и распределенной (WAN) сетей;
- Документирование физической и логической реализации сети.

В дополнение к материалу, изложенному в настоящей главе, рекомендуется ознакомиться с лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Ключевые термины

IEEE 802.3 Протокол локальных сетей института IEEE, определяющий реализацию физического уровня локальных сетей LAN и MAC-подуровня канального уровня. IEEE 802.3 использует метод доступа CSMA/CD и поддерживает ряд скоростей передачи в различных физических передающих средах. Расширения стандарта IEEE 802.3 определяют реализацию сетей Fast Ethernet. Физические варианты первоначальной спецификации IEEE 802.3 включают в себя 10BASE-2, 10BASE-5, 10BASE-F, 10BASE-T и 10BROAD-36. Физические варианты спецификации Fast Ethernet включают в себя 100BASE-TX and 100BASE-FX. Вариантами Gigabit Ethernet являются спецификации 1000BASE-T, 1000BASE-LX, and 1000BASE-SX.

MAC-адрес (MAC (Media Access Control) address). Стандартизованный адрес канального уровня, требуемый каждому порту или устройству, подсоединенному к сети LAN. Другие устройства сети используют эти адреса для нахождения конкретных портов в сети и для обновления таблиц маршрутизации и иных структур данных. MAC-адреса имеют длину 6 байтов и устанавливаются институтом IEEE. Их также называют аппаратными адресами, адресами MAC-уровня или физическими адресами.

Быстрый Ethernet (fast ethernet). Любая из многочисленных спецификаций Ethernet с полосой пропускания 100 Мбит/с. Fast Ethernet обеспечивает скорость в 10 раз большую, чем спецификация Ethernet 10BASE-T, сохраняя при этом такие характеристики, как формат фрейма, MAC-механизмы и величину максимального блока передачи (maximum transmission unit — MTU). Это позволяет использовать существующие приложения и средства управления спецификации 10BASE-T в сетях Fast Ethernet. Спецификация Fast Ethernet является расширением спецификации IEEE 802.3. См. также спецификация Ethernet.

Гигабитовый Ethernet (gigabit Ethernet). Любая из многочисленных спецификаций Ethernet со скоростью передачи 1000 Мбит/с. Гигабитовый Ethernet обеспечивает скорость передачи, в 10 большую, чем Fast Ethernet.

Задержка (latency). Промежуток времени между моментом, когда устройство запрашивает доступ к сети и моментом, когда оно получает разрешение на передачу.

Звездообразная топология (star topology). Топология локальной сети, в которой конечные точки сети соединяются с общим центральным коммутатором каналами типа “точка-точка”. В кольцевой звездообразной топологии вместо каналов типа “точка-точка” используются односторонние замкнутые петли. Ср. с шинной топологией.

Институт инженеров по электротехнике и электронике (Institute of Electrical and Electronics Engineers — IEEE). Профессиональная организация, занимающаяся разработкой средств коммуникации и сетевых стандартов. Стандарты локальных сетей, разработанные IEEE, в настоящее время являются общепризнанными.

Коллизионный домен (collision domain). В сетях Ethernet область сети в которой распространяются фреймы, поврежденные в результате коллизии. Повторители и концентраторы позволяют распространяться коллизиям, в то время как LAN-коммутаторы, мосты и маршрутизаторы их задерживают. Также называется доменом полосы пропускания.

Коллизия (collision). В сетях Ethernet столкновение, возникающее при одновременной передаче пакетов двумя узлами. При встрече в физической передающей среде фреймы сталкиваются и повреждаются.

Коммутатор (switch). Сетевое устройство, которое выполняет фильтрацию, пересылку или лавинную рассылку фреймов на основе адреса получателя, содержащегося в каждом фрейме. Коммутаторы функционируют на канальном уровне эталонной модели OSI.

Коммутатор локальной сети LAN (LAN switch). Высокоскоростной коммутатор, осуществляющий пересылку пакетов между сегментами сети на основе данных канального уровня. Большинство LAN-коммутаторов используют для этого MAC-адреса. Эти коммутаторы часто делятся на две категории: использующие сквозную коммутацию или коммутацию с промежуточным хранением. Примером LAN-коммутатора может служить Cisco Catalyst 5000.

Коммутация (switching). Процесс получения фрейма на одном интерфейсе устройства и отправки его с другого интерфейса.

Коммутация без буферизации пакетов (cut-through). Метод коммутации пакетов, при котором прохождение потока данных через коммутатор осуществляется таким образом, что начало пакета начинает покидать выходной порт до того, как конец пакета полностью пройдет входной порт. Устройство, осуществляющее сквозную коммутацию, начинает чтение, обработку и пересылку пакета сразу после того, как стал известен адрес получателя и определен выходной порт. Такой метод коммутации также известен как "коммутация-на-лету".

Коммутация с быстрой пересылкой или быстрая коммутация (fast-forward switching). Метод коммутации с минимальной задержкой, достигаемой благодаря тому, что пересылка пакета начинается сразу после получения адреса получателя.

Локальная сеть (local-area network — LAN). Высокоскоростная сеть передачи данных с низким уровнем ошибок, охватывающая относительно небольшую географическую область (до нескольких километров). Сети LAN включают в себя рабочие станции, периферийные устройства, терминалы и другие устройства, находящиеся в одном здании или в другой географически ограниченной области. Стандарты LAN-сетей определяют характеристики кабельных соединений и методы сигнализации на физическом и канальном уровнях эталонной модели OSI. Широкое распространение получили LAN-технологии Ethernet, FDDI и Token Ring.

Маршрутизатор (router). Устройство сетевого уровня, использующее одну или более метрик для определения оптимального маршрута для пересылки данных. Маршрутизаторы пересылают потоки данных из одной сети в другую на основе информации сетевого уровня. Иногда называются шлюзами, хотя это название все более устаревает.

Метод множественного доступа с контролем несущей и обнаружением коллизий (carrier sense multiple access collision detect — CSMA/CD). Способ доступа к передающей среде, при котором устройство перед передачей данных проверяет, не идет ли в это момент по ней передача данных других устройств. Если в течение определенного

промежутка времени носитель остается свободным, то начинается передача. Если два устройства начинают передачу одновременно, то происходит коллизия, о которой уведомляются все передающие устройства. В этом случае выполнявшие передачу устройства прекращают ее на некоторый промежуток времени, определяемый случайным образом. Доступ типа CSMA/CD применяется в сетях Ethernet и IEEE 802.3.

Микросегментация (microsegmentation). Разделение сети на сегменты меньшего размера, обычно для увеличения общей полосы пропускания к отдельным сетевым устройствам.

Мост (bridge). Устройство, соединяющее два сетевых сегмента, использующих один и тот же коммуникационный протокол и передающее между ними пакеты. Мосты функционируют на 2-м (канальном) уровне эталонной модели OSI. В целом мосты фильтруют, пересылают или выполняют лавинную рассылку фреймов на основе их MAC-адресов.

Мостовая технология (bridging). Технология, в которой мост соединяет два или более сегментов LAN.

Переполнение (congestion). Попытка передачи объема данных, превышающего пропускную способность сети.

Пересылка с промежуточным хранением (store-and-forward). Метод коммутации при использовании которого фреймы должны быть полностью обработаны перед тем как будут отправлены на соответствующий порт. Эта обработка включает в себя выполнение проверки с циклической избыточностью (cyclic redundancy check — CRC) и проверки адреса получателя. Кроме того, фреймы временно хранятся до тех пор, пока станут доступными сетевые ресурсы для отправки сообщения (такие, например, как свободный канал).

Повторитель (repeater). Устройство, осуществляющее регенерацию и дальнейшее распространение электрических сигналов, передаваемых между двумя сетевыми сегментами.

Протокол связующего дерева (spanning tree protocol). Мостовой протокол, использующий алгоритм связующего дерева, позволяющий мосту динамически обходить петли в сетевой топологии путем создания связующего дерева. Для обнаружения петель мосты обмениваются друг с другом модулями данных мостового протокола (bridge protocol data unit — BPDU); после этого петли ликвидируются путем отсечения выбранных мостовых интерфейсов. Рассматриваемый термин относится как к протоколу IEEE 802.1 “Spanning Tree Protocol”, так и более раннему одноименному протоколу корпорации Digital Equipment, на котором он основан. Версия IEEE поддерживает мостовые домены и позволяет мостам создавать свободную от петель топологию в расширенных локальных сетях LAN. Версии IEEE чаще отдается предпочтение чем версии Digital.

Сервер предприятия (enterprise server). Сервер, предлагающий службы всем пользователям некоторой сети. Примером таких серверов могут служить серверы электронной почты или DNS-серверы.

Сетевой уровень (network layer). 3-й уровень эталонной модели OSI. На этом уровне обеспечиваются соединения и происходит выбор маршрута между двумя конечными системами. На этом уровне также осуществляется маршрутизация. Примерно соответствует уровню контроля маршрута в модели SNA.

Спецификация Ethernet. Спецификация локальных сетей, созданная корпорацией Xerox и далее совместно разработанная корпорациями Xerox, Intel и Digital Equipment. Сети Ethernet используют метод доступа CSMA/CD и разнообразные типы кабелей с пропускной способностью 10 Мбит/с. Спецификация Ethernet во многом аналогична серии стандартов IEEE 802.3.

Схема каблирования (cut sheet). Схема, на которой показано расположение отрезков кабелей и номера помещений, к которым они ведут.

Таблица маршрутизации (routing table). Таблица, которая хранится на маршрутизаторе или другом устройстве межсетевого обмена и в которой регистрируются маршруты к отдельным сетям-получателям и, в некоторых случаях, значения метрик, связанные с этими маршрутами.

Шинная топология (bus topology). Линейная структура LAN, при которой передаваемые данные от сетевых станций распространяются по всей передающей среде и принимаются всеми станциями. Ср. со звездообразной топологией.

Широковещательная лавина (broadcast storm). Нежелательное событие в сети, при котором большое количество широковещательных сообщений рассылаются одновременно по всем сетевым сегментам. Широковещательная лавина занимает значительную часть полосы пропускания сети и, как правило, вызывает простой сети.

Широковещательный адрес (broadcast address). Специальный адрес, зарезервированный для рассылки сообщений всем станциям сети. Как правило, широковещательный адрес представляет собой MAC-адрес пункта назначения состоящий только из единиц. См. также широковещание.

Широковещательный домен (broadcast domain). Совокупность сетевых устройств, получающих широковещательные фреймы, отправленные любым устройством из этой совокупности. Границы широковещательного домена часто определяются маршрутизаторами, которые не передают далее широковещательные фреймы. См. также широковещание.

Широковещательный пакет (broadcast). Пакет данных, который рассылается всем узлам сети. Широковещательные пакеты идентифицируются специальным широковещательным адресом. См. также широковещательный адрес, широковещательный домен и широковещательная лавина.

Контрольные вопросы

1. Какой из приведенных ниже методов широковещания использует среда Ethernet для передачи данных всем узлам сети и получения данных от всех узлов?
 - A. Пакет
 - B. Фрейм данных
 - C. Сегмент
 - D. По одному байту
2. Что из нижеперечисленного является характеристикой микросегментации?
 - A. Виртуальные маршруты между станциями отправителя и получателя
 - B. Наличие нескольких маршрутов перемещения данных в коммутаторе
 - C. Видны сразу все потоки данных в сетевом сегменте
 - D. А и B

3. Какие из приведенных ниже устройств рассматриваются как коммутаторы LAN?
 - А. Многопортовые повторители, функционирующие на 1-м уровне
 - В. Многопортовые концентраторы, функционирующие на 2-м уровне
 - С. Многопортовые маршрутизаторы, функционирующие на 3-м уровне
 - Д. Многопортовые мосты, функционирующие на 2-м уровне
4. Для какой из перечисленных ниже целей оптимизируется асимметричная коммутация?
 - А. Для обработки потоков данных в системах типа "клиент/сервер", в которых "быстрый порт" коммутатора подсоединен к серверу
 - В. Для равномерного распределения потоков данных в сети
 - С. Для коммутаторов, у которых отсутствует буфер памяти
 - Д. А и В
5. Опишите работу дуплексных и полудуплексных сетей Ethernet.
6. Опишите главную функцию протокола связующего дерева.
7. В качестве чего рассматривается каждый сегмент сети, которая сегментирована с помощью коммутаторов?
 - А. В качестве сети
 - В. В качестве сети кампуса
 - С. В качестве коллизийного домена
 - Д. В качестве распределенной сети WAN
8. Какое из приведенных ниже утверждений справедливо для дуплексного коммутатора Ethernet?
 - А. Фактически устраняются коллизии.
 - В. Для каждого узла используются две пары кабелей и коммутируемое соединение.
 - С. Соединения между узлами рассматриваются как соединения типа "точка-точка".
 - Д. Все вышеперечисленные утверждения.
9. Какие из ниже перечисленных эффектов вызываются переполнением?
 - А. Низкая надежность и незначительный объем передачи данных
 - В. Высокий уровень коллизий
 - С. Непредсказуемость поведения сети и высокий уровень ошибок
 - Д. Длительное ожидание отклика сети на запрос, большое время, требуемое для передачи файлов и большая величина задержки в сети
 - Е. Все вышеперечисленные
10. Станция А осуществляет передачу данных другой станции, станции В. Связь происходит таким образом, что станция А прекращает передачу содержательных пакетов и тогда начинает передачу станция В. Аналогичным образом, станция В прекращает передачу, когда ее снова начинает станция А. К какому из перечисленных ниже относится такой тип передачи?
 - А. Дуплексная передача

- B. Полудуплексная передача
 - C. Симлекс
 - D. Никакой из вышеперечисленных
11. Какое из приведенных ниже утверждений, относящихся к пересылке пакетов в сети LAN, ошибочно?
- A. При использовании коммутации с промежуточным хранением фреймы полностью обрабатываются перед отправкой его на соответствующий выходной порт.
 - B. Коммутация с промежуточным хранением осуществляется медленнее чем сквозная коммутация.
 - C. Сквозная коммутация также называется коммутацией "на лету".
 - D. Если сетевое соединение или канал имеет невысокую скорость передачи, то при использовании сквозной коммутации требуется буферизация.
12. Какое из приведенных ниже утверждений справедливо для коммутатора LAN-сети?
- A. Коммутатор восстанавливает сетевые фрагменты, известные как микро-сегменты.
 - B. Коммутатор LAN-сети представляет собой высокоскоростной многопортовый мост.
 - C. Большая величина задержки вызывается узкой полосой пропускания.
 - D. Коммутатору LAN требуются новые сетевые интерфейсы на подключаемых станциях.
13. Сколько коллизийных доменов создает 16-портовый коммутатор LAN?
- A. 1
 - B. 2
 - C. 14
 - D. 16
14. Что происходит при создании для сегмента виртуального канала с использованием LAN-коммутации?
- A. Возрастает количество коллизий
 - B. Уменьшается доступная полоса пропускания
 - C. Возрастает объем широковещания
 - D. Увеличивается доступная полоса пропускания
15. Каким образом коммутатор узнает адреса устройств, подсоединенных к его портам?
- A. Коммутаторы получают адресные таблицы от маршрутизаторов.
 - B. Коммутаторы считывают адреса отправителей в пакетах, поступающих на их порты.
 - C. Коммутаторы обмениваются адресными таблицами с другими коммутаторами.
 - D. Коммутаторы не могут строить адресные таблицы.
16. В чем состоит цель симметричной коммутации?

- A. Она обеспечивает соединение на коммутаторе портов с одной и той же полосой пропускания.
 - B. Она обеспечивает симметричность сетевых таблиц.
 - C. Она обеспечивает соединение на коммутаторе портов с различной полосой пропускания.
 - D. Коммутаторы обеспечивают только асимметричную коммутацию.
17. Какие устройства выполняют логическую сегментацию локальной сети LAN?
- A. Маршрутизаторы
 - B. Мосты
 - C. Коммутаторы
 - D. Концентраторы
18. Каким образом маршрутизатор сегментирует локальную сеть LAN?
- A. Он уменьшает широковещательные домены.
 - B. Он увеличивает количество логических сегментов.
 - C. Он уменьшает величину полосы пропускания.
 - D. А и B.
19. Что из перечисленного ниже *не* является преимуществом использования устройств 3-го уровня в локальной сети LAN?
- A. Оно позволяет сегментировать сеть LAN на уникальные физические и логические подсети.
 - B. Оно позволяет осуществлять соединения с распределенными сетями WAN.
 - C. Оно обеспечивает логическое структурирование сети.
 - D. Оно увеличивает размер сети LAN.
20. Какое из нижеперечисленных устройств может служить примером сервера предприятия?
- A. Сервер CAD крупной компании
 - B. DNS-сервер учебного округа
 - C. Сервер административного журнала (оценок) в школе
 - D. Сервер статистики и учета денег



В этой главе...

- Приводятся начальные сведения о коммутаторах
- Описаны компоненты коммутатора
- Рассмотрено, где располагаются коммутаторы уровня доступа
- Описано расположение коммутаторов уровня распределения
- Рассмотрено, где располагаются коммутаторы базового уровня

Коммутаторы

В настоящей главе приводится краткий сравнительный анализ концентраторов и современной технологии коммутации. В ней описаны физические компоненты и характеристики *коммутаторов*, светодиодные индикаторы (LED) и их назначение. Также рассмотрен процесс инициализации коммутатора, подсоединение консоли и справочная система, вызываемая из командной строки. Основное внимание уделяется различным типам и моделям коммутаторов, иерархическому проектированию сети и использованию коммутаторов на уровнях доступа, распределения и на базовом уровне.

Рекомендуется также выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Обзор коммутаторов

Коммутатор представляет собой сетевое устройство 2-го уровня, которое выполняет функции точки концентрации для соединения между собой рабочих станций, серверов, маршрутизаторов, концентраторов и других коммутаторов.

Концентратор (hub) представляет собой концентрационное устройство традиционного типа, которое, как и коммутатор, предоставляет несколько портов для соединения между собой других устройств. Концентраторы уступают коммутаторам в своих возможностях вследствие того, что подсоединенные к ним устройства остаются в одном и том же домене и при одновременной передаче возникают коллизии. Кроме того, концентраторы могут работать только в полудуплексном режиме, т.е. в каждый конкретный момент они могут либо только передавать, либо только получать данные.

Коммутаторы можно рассматривать как многопортовые мосты, которые являются стандартными для современных технологий локальных сетей Ethernet (local-area network — LAN), использующих звездообразную топологию. Коммутаторы обеспечивают выделенные виртуальные каналы типа “точка-точка” между каждым двумя подсоединенными сетевыми устройствами, поэтому при одновременной передаче коллизий не происходит. Коммутаторы могут работать в дуплексном режиме; это означает, что они могут одновременно получать данные и отправлять их. Понимание характера работы коммутаторов и умение их конфигурировать являются важным фактором для поддержки работы сети.

Локальные сети LAN охватывают пространство одного помещения, одного здания или нескольких близко расположенных зданий. Группа близко расположенных зданий, принадлежащих одной организации, в сетевой терминологии часто называется кампусом. При проектировании более крупных сетей LAN полезно исходить из следующих положений:

- На уровне доступа осуществляется подключение конечных пользователей к сети LAN;
- На уровне распределения осуществляется соединение между собой LAN-сетей конечных пользователей в котором реализуются определенные политики;
- На базовом уровне осуществляется кратчайшее соединение между точками распределения.

По мере того, как сеть увеличивается до размеров кампуса, возникает необходимость в использовании различных типов коммутаторов локальных сетей. На каждом уровне требуется свой тип коммутатора, который наилучшим образом решает задачи данного уровня. Функции и технические характеристики каждого коммутатора зависят от того, для какого уровня предназначен этот коммутатор. Правильный выбор наилучшего для данного уровня коммутатора обеспечивает максимальную эффективность работы сети для ее пользователей.

Понимание роли каждого уровня и выбор соответствующего типа коммутатора являются важными факторами эффективного проектирования сети LAN.

Включение коммутатора

Превращение отключенного или нового коммутатора в функционирующий коммутатор, управляющий передачей данных в сети, включает в себя выполнение ряда действий. В следующем разделе описаны эти действия, а также тестирование начальной загрузки коммутатора и другие операции по подготовке коммутатора к конфигурированию и вводу в действие.

Включение коммутатора Catalyst

Коммутатор представляет собой специализированный выделенный компьютер, в котором имеется модуль центрального процессора (central processing unit — CPU), оперативная память (random-access memory — RAM) и операционная система. Как показано на рис. 6.1, коммутатор обычно имеет несколько портов для подсоединения рабочих станций, а также специализированные управляющие порты. Для управления коммутатором, просмотра и изменения конфигурации осуществляется подсоединение через консольный порт, как показано на рис. 6.2.



Рис. 6.1. Порты коммутатора Cisco

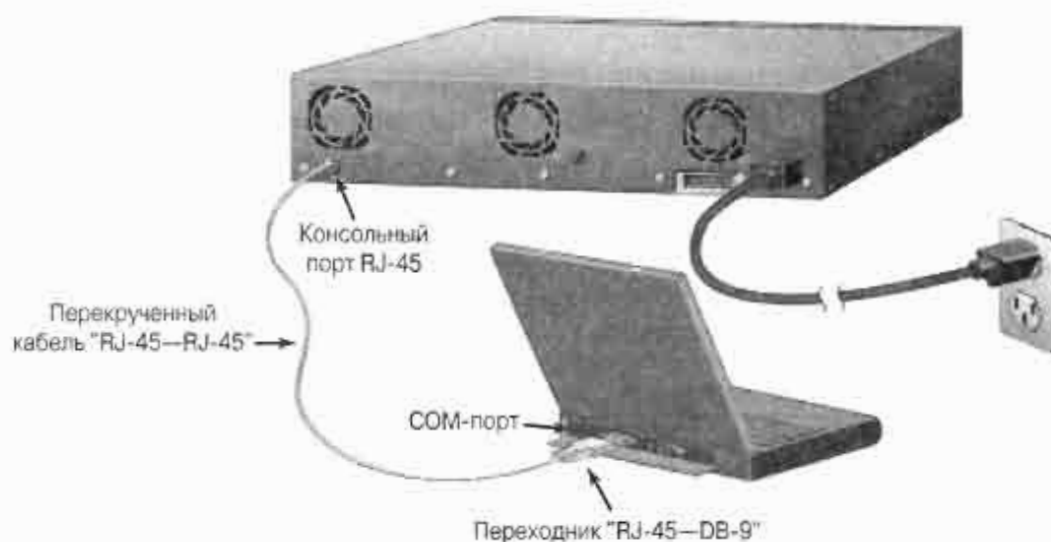


Рис. 6.2. Консольное подключение

Обычно коммутаторы не имеют выключателя питания, а просто подключаются к источнику питания или отключаются от него. В примере 6.1 приведен начальный вывод интерфейса командной строки (command-line interface — CLI) коммутатора Cisco.

Пример 6.1 Начальные сообщения коммутатора Cisco

```
32K bytes of flash-simulated non-volatile configuration memory
Base Ethernet MAC address: 00:04:4D:D2:3D:00
Motherboard assembly number:73-3382-08
Power supply part number:34-0834-01
Motherboard serial number: FAB044685H5
Power supply serial number: DAB04283EPL
Model revision number: A0
Motherboard revision number: C0
```

```

Model number: WS-C2924-XL-EN
System serial number: FAB0447S0M2

Press RETURN to get started!

00:00:27: %SYS-5-RESTART: System restarted -
Cisco Internetwork Operating System Software
IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5.2)XU,
MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2000 by Cisco Systems, Inc.

```

Светодиодные индикаторы коммутатора

На передней панели коммутатора имеется несколько индикаторов, предназначенных для наблюдения за работой коммутатора. Они представляют собой светодиоды (light emitting diode — LED). На передней панели коммутатора расположены следующие индикаторы:

- системный индикатор;
- индикатор подачи внешнего удаленного питания (Remote power supply — RPS)
- индикаторы режима работы портов (Port Mode)
- индикаторы состояния портов (Port Status).

Системный индикатор LED

Системный индикатор LED, показанный ранее на рис. 6.1, указывает, включено ли питание коммутатора и характеризует правильность его работы. В табл. 6.1 приведены возможные состояния системного индикатора.

Таблица 6.1. Индикатор состояния системы

Цвет индикатора	Состояние системы
Не горит	На систему не подано питание
Зеленый	Нормальное состояние
Желтый	Питание на систему подано, однако она функционирует некорректно

Индикатор подачи удаленного питания RPS

Индикатор подачи удаленного питания показывает, подается ли на систему напряжение от удаленного источника. Он также характеризует состояние системы при включенном удаленном источнике питания. В табл. 6.2 описано, какое состояние системы соответствует каждому цвету индикатора.

Таблица 6.2. Цвета индикатор удаленного питания

Цвет индикатора	Состояние источника удаленного питания RPS
Не горит	Удаленное питание RPS отключено или соответствующий модуль на коммутаторе не установлен
Постоянный зеленый	Удаленное питание RPS подается на коммутатор и он функционирует в нормальном режиме

Окончание табл. 6.2

Цвет индикатора	Состояние источника удаленного питания RPS
Мигающий зеленый	Удаленное питание осуществляет резервную поддержку другого коммутатора в стеке
Постоянный желтый	Удаленное питание RPS подключено, но работает некорректно
Мигающий желтый	Внутренний источник питания коммутатора не функционирует. Коммутатор работает от удаленного источника питания RPS

Индикатор режима работы порта LED

Индикатор режима работы порта указывает текущее состояние кнопки Mode. Режимы используются для того, чтобы правильно интерпретировать показания индикаторов состояния порта LED. Для выбора или изменения режима порта следует нажимать на кнопку режима (Mode) до тех пор, пока индикаторы режима не отобразят требуемый режим. Индикаторы состояния порта LED могут иметь различные значения, в зависимости от текущего значения индикатора режима порта (Mode LED) (см. табл. 6.3). Кнопка режима (Mode) на передней панели коммутатора используется для указания того, как следует интерпретировать цвет индикатора порта.

Кнопка режима (Mode) имеет три состояния:

- STAT (состояние холостого хода);
- UTL (режим использования);
- FDUP (дуплексный режим).

Мигание индикатора состояния оранжевым светом, обычно означает, что имеются какие-то аппаратные проблемы с портом, модулем или коммутатором. Это же происходит случае аварийного состояния порта или модуля.

Индикатор состояния порта

Каждый порт имеет свой индикатор состояния порта LED (Port Status LED или Port LED). Эти индикаторы отображают информацию о состоянии коммутатора и его отдельных портов. В табл. 6.3 описаны все возможные режимы портов коммутатора.

Таблица 6.3. Отображение режимов работы портов индикаторами состояния

Режим индикатора LED	Порт	Описание режима
STAT	Состояние холостого хода	Этот режим является стандартным
UTL	Коммутатор работает в обычном режиме	Коммутатор использует текущее значение полосы пропускания
DUPLX	Дуплексный режим работы порта	Этот режим может быть полудуплексным или дуплексным
SPEED	Скорость передачи на порте	Операционная скорость порта (например, 10 или 100 Мбит/с для портов 10/100)

Для выбора или изменения режима работы порта следует нажимать кнопку режима Mode до тех пор, пока индикатор не отобразит требуемый режим работы порта. Для включения отображенного на индикаторе режима следует отпустить кнопку режима Mode. В табл. 6.4 описано значение каждого цвета индикатора режима порта в различных режимах работы коммутатора.

Таблица 6.4. Отображение режима порта индикаторами состояния в различных режимах

Индикатор LED режима работы	Цвет индикатора	Описание
STAT Состояние холостого хода	Свечение отсутствует	Канал не функционирует
	Постоянный зеленый	Канал функционирует в обычном (холостом) режиме
	Мигающий зеленый	Прием или передача данных
	Поочередно зеленый/желтый	Пересылка данных по каналу
	Постоянный желтый	Порт не пересылает данные
UTIL Использование коммутатора	Зеленый	Текущий уровень использования задней панели
	Желтый	Максимальный уровень использования задней панели
	Зеленый и желтый	Если все индикаторы LED горят зеленым цветом, то это означает, что коммутатор использует 50% или более всей полосы пропускания. При снижении уровня использования цвет меняется на желтый
DUPLX Дуплексный или полудуплексный режим работы порта	Свечение отсутствует	Полудуплексный режим
	Зеленый	Дуплексный режим
SPEED Скорость порта (для портов 10/100 Мбит/с)	Свечение отсутствует	Порт функционирует на скорости 10 Мбит/с
	Зеленый	Порт функционирует на скорости 100 Мбит/с

Поведение индикаторов порта LED во время автотестирования коммутатора

После подсоединения кабеля питания коммутатор начинает выполнять ряд тестов, в совокупности называемых автотестированием при включении питания (power-on self test — POST). Эти тесты выполняются автоматически для проверки правильности функционирования коммутатора. Системный индикатор указывает на успешное прохождение теста POST или на наличие неисправностей. Если системный индикатор не горит, но питание на коммутатор подано, то это означает, что идет тестирование. Если системный индикатор горит зеленым светом, то это означает, что тестирование прошло успешно. Если системный индикатор горит желтым светом, то тест не пройден. Неудачное прохождение теста является неустранимой ошибкой. В этом случае нельзя рассчитывать на надежную работу коммутатора.

При прохождении коммутатором теста POST цвет индикатора состояния порта (Port Status LED) также меняется. Индикатор светится желтым цветом в течение примерно 30 секунд, пока коммутатор анализирует топологию сети и ищет петли. Если индикатор состояния порта начинает светиться зеленым, то это означает, что коммутатор установил канал между данным портом и устройством-получателем, таким, например, как компьютер. Если индикатор гаснет, то это свидетельствует о том, что к порту не подсоединено никакое устройство.

Вывод информации о первоначальной загрузке коммутатора

Для того, чтобы сконфигурировать коммутатор или проверить его состояние, необходимо подключить компьютер к коммутатору и установить связь между ними. Для этого используется перекрученный кабель, который подсоединяется к консольному порту на задней панели коммутатора и к СОМ-порту на задней панели компьютера. При этом используется тот же кабель, и выполняются те же действия, которые осуществляются при подсоединении консольного порта маршрутизатора.

После этого на компьютере следует запустить программу HyperTerminal. На рис. 6.3 показано окно этой программы.

При первом конфигурировании связи с коммутатором через Hyper Terminal необходимо ввести имя соединения. После этого следует в выпадающем меню выбрать СОМ-порт, к которому подсоединен коммутатор, и нажать кнопку ОК, как показано на рис. 6.4. При этом отображается второе окно диалога. Далее требуется установить параметры, как показано на рис. 6.5 и нажать кнопку ОК.



Рис. 6.3. Окно программы HyperTerminal



Рис. 6.4. Присвоение имени сеансу HyperTerminal



Рис. 6.5. Установка параметров соединения HyperTerminal

Далее следует подключить коммутатор к защищенному от всплесков напряжения источнику питания. При этом на экране программы Hyper Terminal выводятся загрузочные данные коммутатора. Далее следует проанализировать этот начальный загрузочный вывод. В нем отображается информация о коммутаторе, подробности состояния, полученные с помощью теста POST и информация об аппаратном обеспечении коммутатора.

В примерах 6.2-6.4 приведены различные варианты вывода загрузочной информации коммутатора.

Пример 6.2 Загрузка и инициализация

```

C2950 Boot Loader (CALHOUN-HBOOT-M) Version 12.0(5.3)WC(1),
MAINTENANCE INTERIM
SOFTWARE
Compiled Mon 30-Apr-01 07:56 by devgoyal
WS-C2950-24 starting...
Base ethernet MAC Address: 00:08:e3:2e:e6:00
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 162 files, 3 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7741440
flashfs[0]: Bytes used: 2961920
flashfs[0]: Bytes available: 4779520
flashfs[0]: flashfs fsck took 6 seconds.
...done initializing flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid: 4
Loading "flash:c2950-c3h2s-mz.120-5.3.WC.1.bin"...
#####
#####

File "flash:c2950-c3h2s-mz.120-5.3.WC.1.bin" uncompressed and
installed,
entry point: 0x80010000
executing...

```

Пример 6.3 Данные автотестирования POST

```

Initializing flashfs...
flashfs[1]: 162 files, 3 directories
flashfs[1]: 0 orphaned files, 0 orphaned directories
flashfs[1]: Total bytes: 7741440
flashfs[1]: Bytes used: 2961920
flashfs[1]: Bytes available: 4779520
flashfs[1]: flashfs fsck took 6 seconds.
flashfs[1]: Initialization complete.
Done initializing flashfs.
C2950 POST: System Board Test : Passed
C2950 POST: Ethernet Controller Test : Passed
C2950 POST: MII TEST : Passed

cisco WS-C2950-12 (RC32300) processor (revision B0) with 22260K
bytes of memory.
Processor board ID FOC0605W0BH
Last reset from system-reset

```

Пример 6.4 Завершение инициализации

```

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
12 FastEthernet/IEEE 802.3 interface(s)

```

```

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:08:E3:2E:E6:00
Motherboard assembly number: 73-5782-08
Power supply part number: 34-0965-01
Motherboard serial number: FOC060502HP
Power supply serial number: PHI05500C5D
Model revision number: B0
Motherboard revision number: B0
Model number: WS-C2950-12
System serial number: FOC0605W0BH

```

```
Press RETURN to get started!
```

```
C2950 INIT: Complete
```

После того, как коммутатор загрузится и выполнит тест POST, появляется диалоговое окно конфигурирования системы (System Configuration). Это конфигурирование может быть выполнено вручную с помощью диалогового окна конфигурирования или окна установки. Диалоговое окно конфигурирования коммутатора проще, чем аналогичное окно маршрутизатора. Вход в диалоговый режим установки может быть произведен в любой момент путем ввода в командной строке команды **setup**.

Получение справки из командной строки интерфейса коммутатора

Интерфейс командной строки коммутатора Cisco аналогичен интерфейсу командной строки маршрутизатора Cisco.

Команда вызова справочной системы представляет собой вопросительный знак. При вводе этой команды в командной строке выводится список доступных команд текущего режима, как показано на рис. 6.5.

Пример 6.5. Вывод по команде ? (help) вызова справочной системы

```

Switch>?
access-enable      Create a temporary Access-List entry
access-profile     Apply user-profile to interface
clear              Reset functions
connect            Open a terminal connection
disable            Turn off privileged commands
disconnect         Disconnect an existing network connection
enable             Turn on privileged commands
exit               Exit from the EXEC
help               Description of the interactive help system
lat                Open a lat connection
lock               Lock the terminal
login              Log in as a particular user
logout             Exit from the EXEC
mtrace             Trace reverse multicast path from destination to
source
name-connection    Name an existing network connection
pad                Open a X.29 PAD connection

```

```
ping          Send echo messages
ppp           Start IETF Point-to-Point Protocol (PPP)
--more--
```

Команда вызова справки может использоваться весьма гибко. Для получения списка команд, начинающихся с некоторой последовательности символов, достаточно ввести несколько символов этой последовательностью и сразу вслед за ними вопросительный знак (?). Такая форма вызова справки называется вызовом слова, поскольку команда дополняет введенные символы до полного слова. При использовании контекстно-зависимой справки пробел (или его отсутствие) имеет смысловое значение. Например, для получения списка опций команды **show** для коммутатора следует ввести команду **show** с последующим пробелом и вопросительным знаком, как показано в примере 6.6. В примере 6.7 показано, как вывести команды начинающиеся с буквы **r** путем ввода этой буквы и вопросительного знака (пробел в данном случае не используется).

Пример 6.6. Вывод по команде show ?

```
Switch>show ?

class-map      Show QoS Class Map
clock          Display the system clock
diags          Show runtime diagnostic info
exception      exception information
flash:         display information about flash: file system
history        Display the session command history
hosts          IP domain-name, lookup style, nameservers, and host
table
location       Display the system location
policy-map     Show QoS Policy Map
--more--
Example 6-7 Keyword Help Command
Switch>show r?

Rmon
Switch>show r_
```

Как показано в примере 6.6, для того, чтобы вывести ключевые слова или аргументы какой-либо команды, следует ввести вместо ключевого слова или аргумента вопросительный знак. Перед ним следует ввести пробел. Такая форма вызова справки называется справкой синтаксиса команды, поскольку она показывает, какие ключевые слова и аргументы используются с командой, ключевыми словами и аргументами, которые уже введены в командной строке.

Как и маршрутизаторы, коммутаторы имеют несколько режимов ввода команд. По умолчанию устанавливается пользовательский режим EXEC, который характеризуется наличием в конце командной строки символа ">". Доступные в этом режиме команды ограничены командами установок терминала, выполнения базовых тестов и отображением системной информации.

Команда **enable** используется для перехода из пользовательского режима EXEC в привилегированный режим EXEC.

Привилегированный режим EXEC характеризуется наличием в конце командной строки символа "#", как показано ниже.

Switch#

Набор команд привилегированного режима EXEC включает в себя команды пользовательского режима EXEC, а также команды **configure terminal**, **configure memory** или **configure network**, с помощью которых можно получить доступ к другим командным режимам. Поскольку эти режимы используются для конфигурирования коммутатора, для предотвращения несанкционированного доступа к привилегированному режиму EXEC должен быть защищен паролем. Если системный администратор установил пароль, то для получения доступа к привилегированному режиму EXEC пользователю предлагается ввести пароль. Этот пароль не отображается на экране и чувствителен к регистру. В примере 6.7 приведен список команд, доступных в привилегированном режиме EXEC.

Пример 6.7. Команды привилегированного режима EXEC

```
Switch#?
Exec commands:
access-enable      Create a temporary Access-List entry
access-profile     Apply user-profile to interface
access-template    Create a temporary Access-List entry
Archive            manage archive files
clear              Reset functions
clock              Manage the system clock
configure           Enter configuration mode
connect            Open a terminal connection
copy               Copy from one file to another
debug              Debugging functions (see also 'undebug')
delete             Delete a file
dir                List files on a filesystem
disable            Turn off privileged commands
disconnect         Disconnect an existing network connection
enable             Turn on privileged commands
erase              Erase a filesystem
--More--
```

Следует обратить внимание на то, что эти команды отличаются от доступных в пользовательском режиме Exec.

Коммутаторы сетей и иерархическое проектирование сети

Иерархический подход к проектированию сети состоит в разделении достаточно сложной задачи проектирования на ряд меньших и легче решаемых задач. Каждый уровень возникающей структуры решает свой собственный набор задач, что позволяет оптимизировать используемое аппаратное и программное обеспечение для решения конкретных, присущих этому уровню задач. Устройства самого нижнего уровня предназначены для приема данных и передачи их в сеть для последующей обработки на более высоких уровнях. Корпорацией Cisco предлагается трехуровневый подход к решению задачи проектирования сети.

В этой трехуровневой модели проектирования сетевые устройства и соединения между ними группируются и подразделяются на три уровня: базовый уровень, уровень распределения и уровень доступа, как показано на рис. 6.6. Как и эталонная модель OSI, эта трехуровневая модель является концептуальной конструкцией, т.е. абстрактной картиной сети.

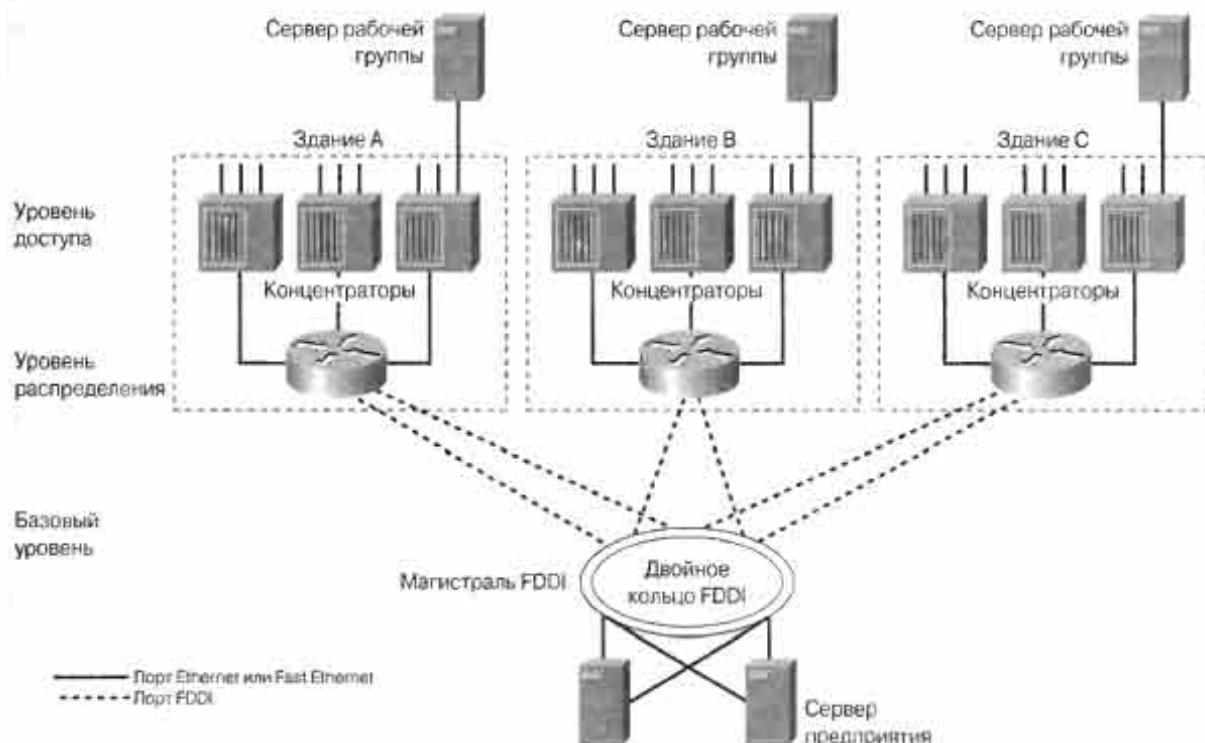


Рис. 6.6. Иерархическая модель проектирования сети

Полезность уровней моделей определяется их модульностью. Поскольку устройства одного уровня выполняют аналогичные и четко очерченные функции, сетевой администратор может легко добавлять, заменять и удалять отдельные элементы сети. Такая гибкость и адаптируемость позволяют в процессе проектирования создавать легко масштабируемую сеть.

Этот подход может быть применен при проектировании любой сети. Необходимо принимать во внимание, что три вышеупомянутых уровня модели могут реализовываться в виде отдельных физических устройств, однако это не является обязательным. Эти уровни определяются для облегчения процесса проектирования и создания эффективной сети путем четкого определения требуемых функций сети.

В то же время, понимание уровней моделей может осложняться тем, что конкретная реализация каждого уровня зависит от конкретной сети. Каждый уровень трехуровневой модели может воплощаться в виде маршрутизатора, коммутатора, соединения или их комбинации. В действительности функции каких-либо уровней могут быть объединены в одном устройстве или, наоборот, какой-либо из уровней может отсутствовать.

В последующих трех разделах каждый уровень рассматривается более подробно.

Базовый уровень

Назначение базового уровня состоит в создании оптимизированной и надежной транспортной структуры для передачи данных с большими скоростями. Иными словами, базовый уровень (*core layer*) должен передавать данные максимально быстро. Устройства этого уровня не должны быть загружены выполнением таких операций, как проверка списков доступа, шифрование данных, трансляция адресов и других функций, которые препятствуют коммутации (*switching*) пакетов с максимально возможной скоростью.

Уровень распределения

Уровень распределения (*distribution layer*) расположен между уровнем доступа и базовым уровнем. Его назначение состоит в отделении процессов базового уровня от остальной части сети. В частности, он должен создать границу входа в сеть путем использования списков доступа и других фильтрующих средств. Таким образом, этот уровень определяет политику доступа к сети. Под политикой понимается подход к обработке определенных типов передаваемых данных, включая обновления маршрутов, обобщение маршрутов, данных, передаваемых по виртуальным сетям VLAN и обобщение (агрегирование) адресов. Различные политики могут быть использованы для обеспечения безопасности сети и для экономии ресурсов путем предотвращения передачи нежелательных данных.

Если в сети используются два или более протокола маршрутизации, такие, например, как протокол маршрутной информации (Routing Information Protocol — RIP) и протокол маршрутизации внутреннего шлюза (Interior Gateway Routing Protocol — IGRP), то обмен информацией между доменами с различными протоколами и ее перераспределение также выполняются на уровне распределения.

Уровень доступа

На уровне доступа (*access layer*) происходит передача данных в сеть и осуществляется входной контроль. Через этот уровень конечные пользователи получают доступ к сети. Выступая в качестве “парадной двери” уровень доступа использует списки доступа, которые предназначены для предотвращения доступа к сети несанкционированных пользователей. Уровень доступа также предоставляет доступ к узлам удаленных сетей с использованием технологий распределенных сетей, таких как Frame Relay, ISDN или выделенные линии.

Обзор уровня доступа в коммутируемых локальных сетях

Создание LAN-сети, которая удовлетворит потребности средних и крупных организаций значительно облегчается, если при ее проектировании используется иерархическая модель. Использование такой модели также значительно облегчает внесение в сеть изменений по мере роста организации.

Уровень доступа является точкой входа в сеть для рабочих станций пользователей и серверов. В кампусной LAN в качестве устройства уровня доступа может выступать концентратор или коммутатор. Если используется концентратор, то доступная полоса пропускания используется совместно всеми устройствами. Если используется коммутатор, то полоса пропускания является выделенной для каждой пары устройств, осуществляющих соединение.

Если две или более рабочих станции или два сервер непосредственно подсоединены к портам коммутатора, то вся полоса пропускания соединения с коммутатором предоставляется компьютерам, осуществляющим соединение. Если два или более компьютера подсоединены к концентратору, то каждому компьютеру предоставляется полоса пропускания, равная общей полосе пропускания, поделенной на количество подсоединенных к концентратору компьютеров. Концентратор может быть подсоединен к порту коммутатора. В этом случае полоса пропускания используется совместно всеми устройствами, подсоединенными к порту коммутатора через концентратор.

Уровень доступа выполняет следующие функции:

- предоставление совместно используемой полосы пропускания;
- предоставление коммутируемой полосы пропускания;
- фильтрация на MAC-уровне;
- микросегментация.

Фильтрация на MAC-уровне позволяет коммутаторам направлять фреймы непосредственно на порт коммутатора, соединенный с требуемым устройством-получателем. Коммутатор создает небольшие сегменты 2-го уровня, называемые микросегментами. Эти коллизийные домены могут включать в себя всего лишь два устройства (т.е. устройство-получатель и соединенный с ним порт коммутатора). На уровне доступа используются коммутаторы 2-го уровня.

Коммутаторы уровня доступа

Как показано на рис. 6.7, коммутаторы уровня доступа функционируют на 2-м уровне эталонной модели OSI и, в частности, предоставляют службу виртуальных локальных сетей (virtual LAN — VLAN). Главной целью коммутатора уровня доступа является соединение конечных пользователей с сетью. Коммутатор уровня доступа должен выполнять эту функцию с минимальными затратами и максимальной плотностью портов.

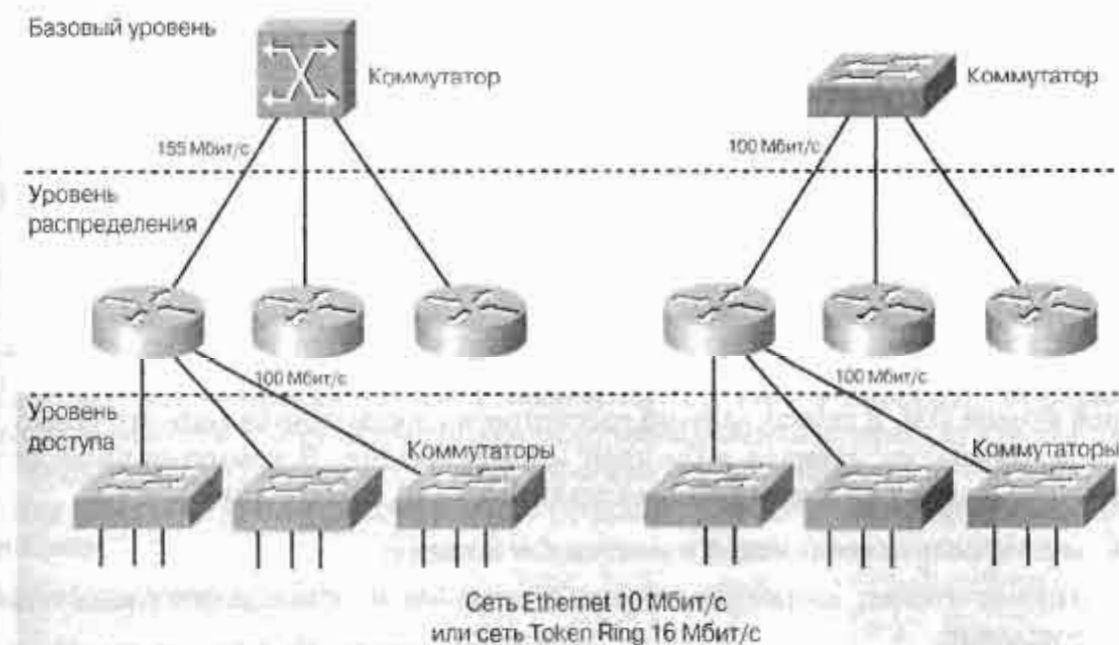


Рис. 6.7. Коммутаторы уровня доступа

На уровне доступа обычно используются следующие модели коммутаторов Cisco:

- Catalyst 1900;
- Catalyst 2820;
- Catalyst 2950;
- Catalyst 4000;
- Catalyst 5000.

Функции этих коммутаторов уровня доступа описаны в табл. 6.5.

Модели 1900 и 2820 являются эффективными устройствами доступа в небольших или средних сетях кампусов. Использование модели Catalyst 2950 целесообразно для обеспечения доступа серверов и пользователей, которым требуется широкая полоса пропускания. Это становится возможным благодаря наличию у этой модели портов Fast Ethernet. Модели коммутаторов Catalyst 4000 и 5000 имеют порты Gigabit Ethernet и являются эффективными устройствами доступа для большого количества пользователей в крупных кампусных сетях.

В сетях большего размера, чем сети кампусов, на уровне доступа удаленные узлы получают доступ к корпоративной сети с помощью технологий распределенных сетей, таких как Frame Relay, ISDN, абонентские цифровые каналы (xDSL) или по выделенным линиям.

Часто ошибочно полагают, что три рассматриваемых уровня (базовый, распределения и доступа) должны быть явно выражены конкретными физическими устройствами, однако это не является обязательным. На самом деле эти три уровня определяются для успешного проектирования сети и четкого определения функций, которые должна выполнять сеть. Конкретный способ реализации этих уровней зависит от потребностей проектируемой сети. Однако важно помнить, что для того, чтобы сеть оптимально функционировала и сохраняла масштабируемость по мере ее роста, в процессе ее проектирования должен быть соблюден иерархический принцип.

Обзор уровня распределения

Уровень распределения расположен между уровнем доступа и базовым уровнем и предназначен для определения и отделения базового уровня. Его функция состоит в задании границ, в которых может происходить какая-либо обработка пакетов. На этом уровне происходит сегментация сети на отдельные широковещательные домены. Здесь же с помощью списков доступа может определяться политика и производиться фильтрация пакетов. Этот уровень обеспечивает изоляцию основной части сети от проблем, которые могут возникать в рабочих группах, с тем чтобы они не затрагивали базовый уровень. Коммутаторы этого уровня могут работать на 2-м и 3-м уровнях эталонной модели OSI. В рамках данного рассмотрения достаточно считать что коммутация 3-го уровня заключается в быстрой маршрутизации. В коммутируемых сетях уровень распределения выполняет несколько функций, в частности:

- агрегирование соединений в монтажных шкафах;
- задание границ широковещательных доменов и доменов многоадресной рассылки;
- VLAN-маршрутизация;

- все переходы из одной среды передачи в другую;
- обеспечение безопасности.

Таблица 6.5. Коммутаторы уровня доступа

Коммутатор Catalyst	Тип коммутатора	Поддерживаемые уровни модели OSI	Количество портов Ethernet	Количество портов Fast Ethernet	Количество портов Gigabit Ethernet	Масштаб предприятия
Модель 1900	Фиксированная конфигурация	2-й уровень	12 или 24	2	0	Малое/среднее
Модель 2820	Модульные платы расширения	2-й уровень	24	2	0	Малое/среднее
Модель 2950	Фиксированная конфигурация	2-й уровень	0	Конфигурируются 12 или 24 скорости передачи	0 или 2	Малое/среднее
Модель 4000	Несколько модульных слотов на каждом шасси	2-й и 3-й	0	Конфигурируемые порты — до 240	Конфигурируемые порты — до 240	Среднее/крупное
Модель 5000	Несколько модульных слотов на каждом шасси	2-й и 3-й	0	Зависит от выбранной конфигурации системы	Зависит от выбранной конфигурации системы	Среднее/крупное

Коммутаторы уровня распределения

Коммутаторы уровня распределения представляют собой точки концентрации (агрегирования) нескольких коммутаторов уровня доступа. Эти коммутаторы должны быть способны обрабатывать весь объем данных, поступающих от устройств уровня доступа и поэтому должны иметь высокую производительность.

Коммутатор уровня распределения является граничной точкой широковещательного домена. На уровне распределения происходит объединение потоков данных виртуальных локальных сетей; этот уровень является фокусной точкой для принятия решений о политике доступа к сети и управления потоками данных. Коммутаторы уровня распределения работают как на 2-м, так и на 3-м уровнях эталонной модели OSI. По этой причине коммутаторы этого уровня часто называют многоуровневыми коммутаторами. Они соединяют в одном устройстве функции маршрутизатора и коммутатора, однако предназначены для коммутации потоков данных с большей скоростью, чем это делает обычный маршрутизатор. Если в таких многоуровневых коммутаторах отсутствует встроенный маршрутизирующий модуль, то для выполнения функций 3-го уровня используется внешний маршрутизатор.

Для работы на уровне распределения используются следующие типы коммутаторов Cisco:

- Catalyst 2926G;
- Семейство коммутаторов Catalyst 5000;
- Семейство коммутаторов Catalyst 6000.

Устройствам уровня распределения требуется меньшее количество *интерфейсов* (*interfaces*) и меньшая скорость коммутации, чем коммутаторам базового уровня, поскольку им приходится обрабатывать меньшие объемы данных. Тем не менее молниеносная скорость на базовом уровне становится бесполезной, если низкая скорость уровня распределения не позволяет пользователям получать быстрый доступ к нему.

Уровень распределения отделяет друг от друга уровень доступа и базовый уровень и помогает четко очертить их соответствующие функции (рис. 6.8). Этот уровень определяет границы функциональной области, в которой происходят операции с пакетами. В среде кампуса уровень распределения может выполнять несколько функций, в частности:

- агрегирование адресов или зон;
- управление доступом на уровне отдела или рабочей группы;
- определение границ широковещательной и многоадресной рассылки;
- управление маршрутизацией сетей VLAN;
- все переходы из одной среды передачи в другую;
- обеспечение безопасности.

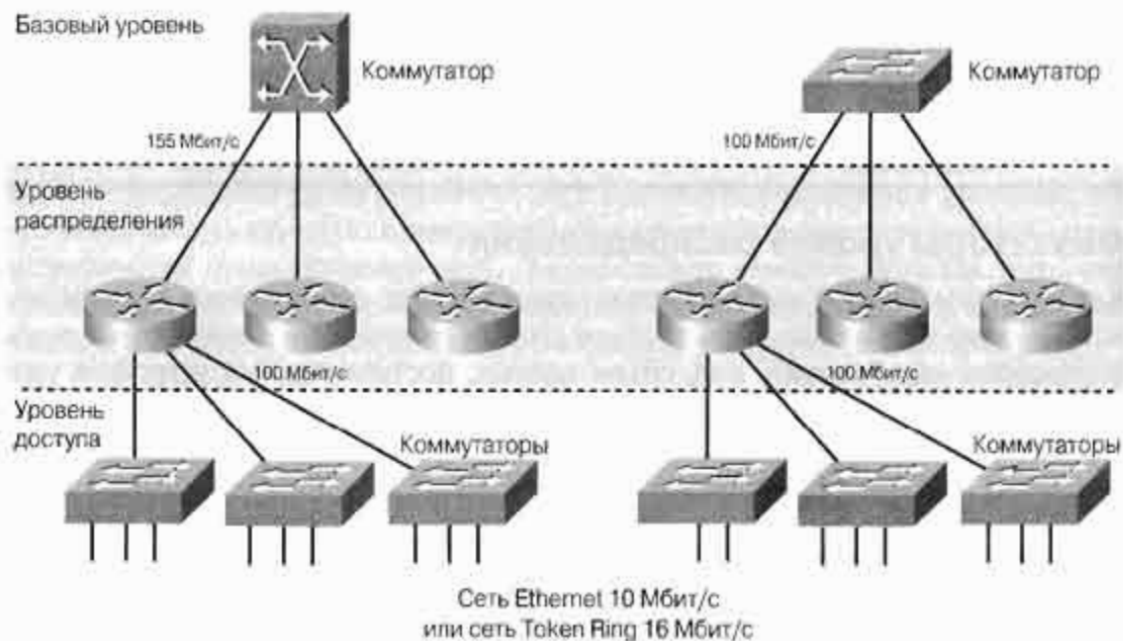


Рис. 6.8. Коммутатор уровня распределения

В средах, не являющихся сетями кампусов, уровень распределения может быть точкой перераспределения между доменами маршрутизации или точкой демаркации между протоколами статической и динамической маршрутизации. Он может также быть точкой доступа с удаленных узлов к корпоративной сети.

В целом уровень распределения можно охарактеризовать как уровень, на котором обеспечиваются соединения пользователей в соответствии с принятой в сети политикой.

Обзор базового уровня

Поскольку базовый уровень является центральной частью сети, он должен быть спроектирован для быстрой и надежной работы. Использование на базовом уровне списков доступа нежелательно, поскольку они вносят дополнительную задержку. Более того, сам доступ конечных пользователей к базовому уровню весьма нежелателен. В качестве аналогии можно привести яблоко: невозможно добраться до косточек, не проникнув сначала через его кожуру. В иерархической сети данные конечных пользователей должны попадать на маршрутизаторы базового уровня только после того, как они прошли уровни доступа и распределения, где к ним могут быть применены списки доступа. Поскольку маршрутизация на базовом уровне осуществляется без использования списков доступа, трансляции адресов и других операций с пакетами, может показаться, что для выполнения столь простой задачи достаточно даже и маломощных маршрутизаторов. Однако верно как раз обратное — на этом уровне используются самые мощные маршрутизаторы Cisco, поскольку в них используются самые быстрые технологии коммутации и они имеют наибольшее количество физических интерфейсов.

Коммутаторы базового уровня

Как показано на рис. 6.9, базовый уровень является магистралью сети кампуса использующей коммутацию. Коммутаторы этого уровня могут использовать ряд технологий 2-го уровня. Если расстояния между коммутаторами базового уровня невелики, то для связи коммутаторов между собой может использоваться технология Ethernet. Также могут использоваться и другие технологии 2-го уровня, такие как асинхронный режим передачи ячеек (Asynchronous Transfer Mode — ATM). При проектировании сети в качестве базового уровня может быть использован уровень маршрутизации (3-й уровень). Коммутаторы базового уровня должны при необходимости обеспечивать эффективное выполнение функций 3-го уровня. Перед тем, как выбрать базовый коммутатор, следует рассмотреть такие факторы как потребности сети, стоимость коммутатора и его производительность.

Для работы на базовом уровне используются следующие модели коммутаторов Cisco:

- Catalyst 6500;
- Catalyst 8500;
- IGX 8400;
- Lightstream.

Представленные на рынок корпорацией Cisco в качестве маршрутизаторов базового уровня для предприятий, маршрутизаторы моделей 7000, 7200 и 7500 обеспечивают максимальные доступные скорости коммутации. Маршрутизатор модели 12000 также является маршрутизатором базового уровня, однако он в первую очередь предназначен для удовлетворения потребности в маршрутизации провайдеров служб Internet (Internet service providers — ISP). Если компания не занимается предоставлением доступа к Internet другим компаниям, то маловероятно увидеть в ее монтажном шкафу маршрутизатор модели 12000. В отличие от других моделей маршрутизаторов, таких как Cisco 2500, 7000, 7200 и 7500, маршрутизаторы модели 12000 имеют модульную структуру, поэтому при необходимости к ним могут быть добавлены другие интер-

фейсные модули. Большие шасси маршрутизаторов этой серии позволяют создать десятки интерфейсов на различных модулях практически для любой среды передачи, что делает эти маршрутизаторы масштабируемым и надежным решением задач базового уровня.

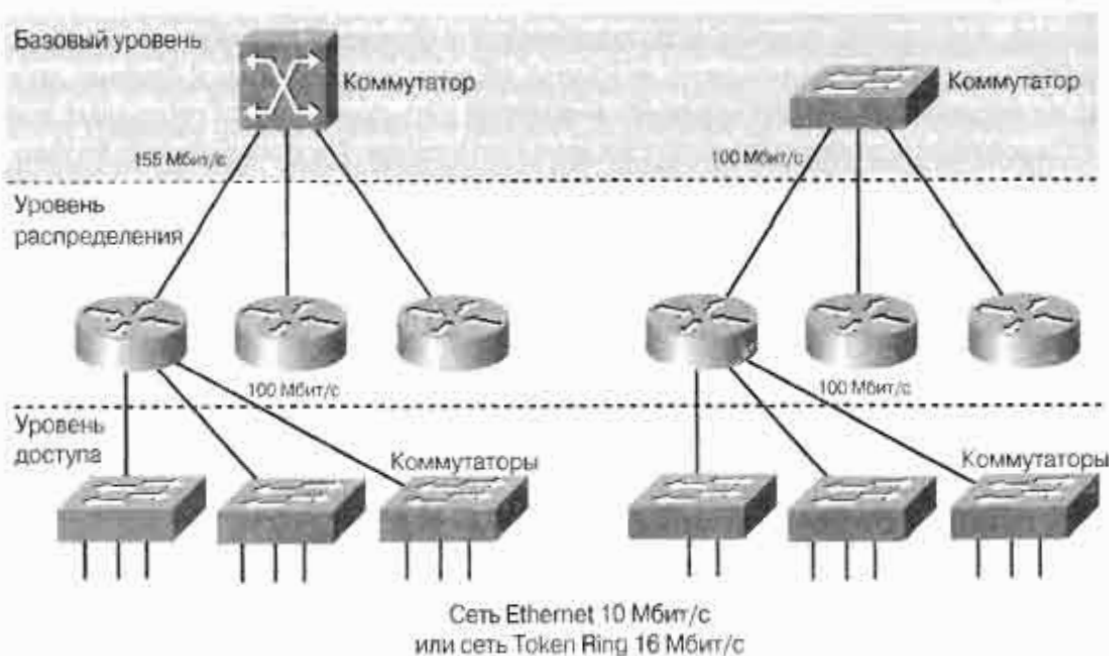


Рис. 6.9. Коммутаторы базового уровня

Одним из способов обеспечения надежности, используемым в маршрутизаторах базового уровня, является использование избыточных каналов, обычно к другим маршрутизаторам базового уровня. При наличии возможности эти избыточные каналы следует делать симметричными (т.е. с одинаковой пропускной способностью), с тем, чтобы можно было использовать распределение (балансирование) нагрузки.

В этом причина того, что базовым маршрутизаторам требуется относительно большое количество интерфейсов. Другим способом обеспечения надежности является использование избыточных источников питания. Базовые маршрутизаторы обычно имеют два или более “заменяемых на ходу” источника питания, которые могут быть удалены или заменены индивидуально без выключения питания маршрутизатора.

Базовые каналы оказываются самыми быстрыми, самыми надежными, но и самыми дорогостоящими выделенными соединениями в распределенных сетях на основе линий T1, T3, OC3 и более скоростных. Если для базовой магистральной распределенной сети используются избыточные каналы T1, то каждому маршрутизатору требуются четыре последовательных интерфейса для двух соединений типа “точка-точка” с каждым узлом. Использование мощных маршрутизаторов и каналов сетей WAN может сделать базовый уровень сети крайне дорогостоящим. Для уменьшения расходов некоторые проектировщики сетей выбирают вариант несимметричных каналов. Вместо избыточных каналов в качестве резервных могут быть использованы технологии коммутации пакетов или коммутации по требованию, такие как Frame Relay или ISDN. Компромиссное решение, позволяющее сэкономить средства при использовании таких технологий определяется достигаемым уровнем производи-

тельности сети. Например, при использовании BRI ISDN в качестве резервного канала теряется возможность распределения нагрузки по каналам с равной оценкой.

Базовый уровень сети не должен реализовываться в сети WAN. В некоторых случаях магистраль LAN-сети также может быть причислена к базовому уровню. В сетях кампусов или в крупных сетях, охватывающих комплекс офисов или смежных зданий, базовая магистраль может проходить по сети LAN. В этом случае в качестве технологий базового уровня типичным является использование Fast Ethernet и Gigabit Ethernet, обычно на основе оптоволоконного кабеля. Промышленные коммутаторы, такие как модели 4000, 5000 и 6000, принимают на себя основную нагрузку в базовых LAN, поскольку они коммутируют фреймы на 2-м уровне со значительно большей скоростью, чем маршрутизаторы коммутируют пакеты на 3-м уровне. На практике эти коммутаторы, являясь модульными устройствами, могут быть оснащены модулями коммутации маршрутов (route switch modules — RSMs), что добавляет к функциям основного шасси маршрутизацию на 3-м уровне.

Резюме

В настоящей главе была рассмотрена общая модель, которую целесообразно использовать при анализе или проектировании сети.

Согласно этой модели крупные сети включают в себя три уровня:

- уровень доступа;
- уровень распределения;
- базовый уровень.

Было показано, что с каждым уровнем связано выполнение определенных специализированных функций. Также показано, что при проектировании коммутируемой сети для каждого уровня имеются свои типы коммутаторов, наилучшим образом выполняющих функции этого конкретного уровня. Для каждого уровня были рассмотрены основные свойства коммутаторов. С течением времени технологии и потребности в полосе пропускания и производительности изменяются. Устройства, которые успешно решают сегодняшние задачи, могут оказаться недостаточно эффективными в будущем. На проектировщика сети, как сетевого профессионала, возлагается задача выбора наилучших типов устройств для каждой конкретной сети.

В дополнение к изложенному в настоящей главе материалу рекомендуется изучить относящиеся к ней видеоклипы, фотографии и выполнить лабораторные работы, находящиеся на компакт-диске CD-ROM, прилагаемом к книге.

Глоссарий

Базовый уровень (core layer). Магистраль сети кампуса, использующей коммутацию. На этом уровне коммутаторы могут использовать ряд технологий 2-го уровня.

Интерфейс (interface). 1. Соединение между двумя системами или устройствами. 2. В терминологии маршрутизации — соединение в сети.

Коммутатор (switch). Сетевое устройство, которое фильтрует, пересылает или рассылает лавинным способом фреймы на основе адреса получателя каждого фрейма. Коммутатор функционирует на канальном уровне эталонной модели OSI.

Коммутация (switching). Процесс получения фрейма на одном интерфейсе и отправки его с другого интерфейса.

Концентратор (hub). Обычно устройство выполняющее роль центра сети со звездообразной топологией.

Магистраль (backbone). Структурная основа сети, соединяющая в одно целое все компоненты сети, делая возможной связь по сети.

Микросегментация (microsegmentation). Процесс разделения отдельного коллизийного домена на два или более домена меньшего размера, что уменьшает количество коллизий и вероятность переполнения в сети.

Порт (port). Интерфейс сетевого устройства (такого, например, как маршрутизатор). Гнездо на распределительной панели, в которое вставляется штекер того же размера, как, например, в разьеме RJ-45. В таких портах для перекрестных соединений компьютеров между собой на распределительной панели используются соединительные кабели. Именно эти перекрестные соединения позволяют функционировать LAN-сети.

Уровень доступа (access layer). На уровне доступа происходит передача данных от конечных пользователей в сеть и выполняются все виды входного контроля. Через этот уровень в сеть входят конечные пользователи.

Уровень распределения (distribution layer). Этот уровень определяет границу до которой над пакетами выполняются различные операции.

Контрольные вопросы

1. Что предоставляет пользователю уровень доступа?
 - A. Точку входа в сеть для конечных пользователей и серверов
 - B. Точку, в которой все устройства подсоединяются к сети
 - C. Всю доступную полосу пропускания для каждого пользователя
 - D. Соединение между коммутаторами и самыми производительными маршрутизаторами сетей
2. Какое из приведенных ниже утверждений верно по отношению к базовому уровню?
 - A. Он выполняет максимально возможную обработку пакетов для обеспечения безопасности
 - B. Он выступает в качестве высокоскоростной коммутирующей магистрали для пересылки данных из одной области (зоны) в другую
 - C. На нем используются только коммутаторы 2-го уровня
 - D. Он использует несколько маршрутов передачи данных для замедления потоков
3. Что из ниже перечисленного является преимуществом использования устройств 3-го уровня в локальной сети LAN?
 - A. Оно позволяет сегментировать сеть LAN на уникальные физические и логические сети
 - B. Оно фильтрует на канальном уровне широковещательные данные и данные многоадресной рассылки, а также обеспечивает WAN-соединения

- C. Оно обеспечивает логическое структурирование сети
 - D. Все вышеперечисленное
4. Какое из перечисленных ниже устройств обеспечивает логическую сегментацию сети LAN?
- A. Маршрутизатор
 - B. Мост
 - C. Коммутатор
 - D. Концентратор
5. Что является результатом микросегментации с помощью коммутаторов?
- A. Создаются дополнительные широковещательные домены
 - B. Уменьшается количество сегментов сети
 - C. Создаются дополнительные коллизийные домены
 - D. Ответы A и C.



В этой главе...

- Описана микросегментация
- Описано, как коммутатор узнает адреса других устройств
- Описана скоростная коммутация
- Описана работа коммутатора и коллизийные домены
- Описаны широковещательные домены
- Описано конфигурирование коммутаторов в локальных сетях
- Рассмотрено тестирование конфигурации коммутатора локальной сети LAN
- Описано управление коммутаторами локальных сетей LAN

Конфигурирование коммутаторов

Коммутаторы являются устройствами 2-го уровня, которые используются для смягчения нехватки полосы пропускания и решения проблемы переполнения в сети. Коммутаторы могут сегментировать локальную сеть LAN на *микросегменты (microsegments)*, которые состоят из двух рабочих станций. Таким образом из одного крупного сегмента создаются свободные от коллизий домены. Хотя коммутатор LAN ликвидирует *коллизионные домены (collision domains)*, все подсоединенные к нему устройства остаются частью одного *широковещательного домена (broadcast domain)*. Вследствие этого все узлы, подсоединенные к коммутатору LAN, получают широко-вещательные сообщения от всего лишь одного передающего их узла.

В настоящей главе приведен обзор базовых атрибутов коммутаторов, а также их операционные характеристики. Основное внимание в ней уделено базовому конфигурированию, тестированию и управлению коммутаторами, работающими на основе IOS Cisco. Также приведены рекомендации по установке IP-адресов портов и других параметров конфигурации коммутаторов.

Рекомендуется выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Микросегментация

Сегментация локальной сети LAN осуществляется по двум основным причинам. Первая состоит в необходимости изолировать передачу потоков данных внутри отдельных сегментов, а вторая — в предоставлении большей полосы пропускания каждому пользователю путем создания коллизионных доменов меньшего размера.

Сегментирование сети LAN вызвано определенными причинами и предоставляет определенные преимущества. Первая из них состоит в том, что без использования сегментации локальные сети, размеры которых превышают размеры небольшой рабочей группы, быстро переполняются передаваемыми потокам и данных и эффективность их работы резко снижается вследствие коллизий. В результате фактически доступная пользователям полоса пропускания практически исчерпывается.

Сегментация сети LAN может быть выполнена с использованием мостов, коммутаторов или маршрутизаторов. Каждое из этих устройств имеет свои достоинства и недостатки. Добавление в сеть таких устройств сегментирует LAN на коллизионные домены меньшего размера. На рис. 7.1 проиллюстрировано создание четырех коллизионных доменов.

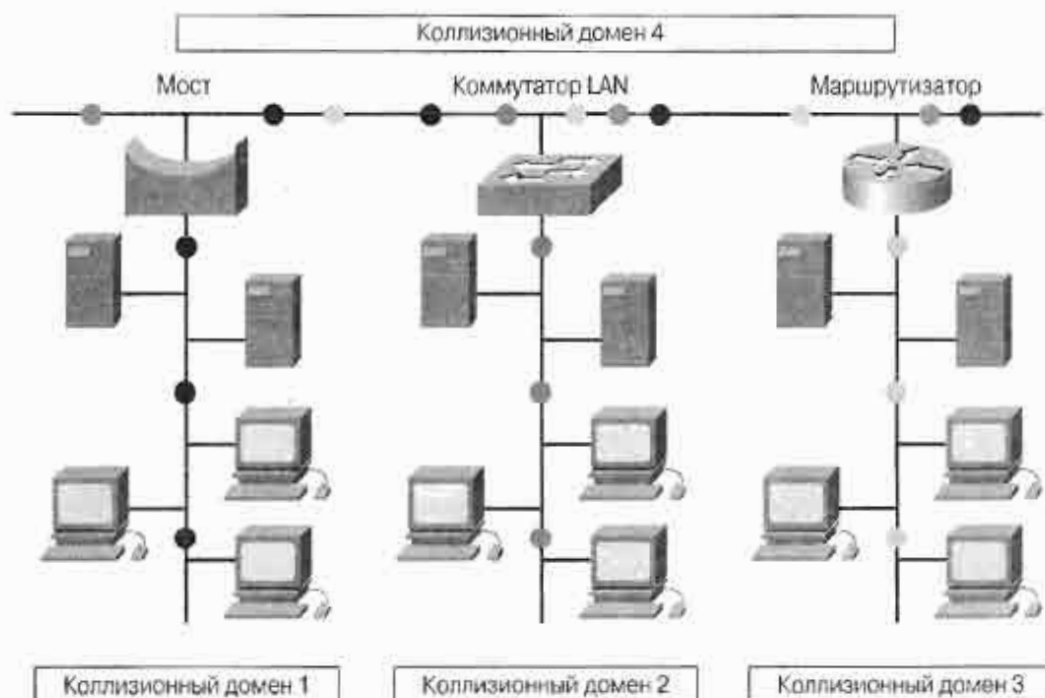


Рис. 7.1 Коллизийные домены

Разделение мостами и коммутаторами крупной сети на замкнутые модули предоставляет несколько преимуществ. Использование мостов и коммутаторов уменьшает объем данных, получаемых устройствами от всех подсоединенных сегментов, поскольку за пределы сегмента выходит лишь часть пересылаемых данных. При этом увеличивается количество коллизийных доменов с одновременным уменьшением размера каждого домена. Размер широковещательного домена при этом не изменяется.

Каждый интерфейс маршрутизатора подсоединен к отдельной сети, поэтому при добавлении маршрутизатора в локальную сеть LAN создаются как коллизийные, так и широковещательные домены меньшего размера. Это происходит потому, что маршрутизаторы не пересылают далее широковещательные сообщения, если они не сконфигурированы для этого специально.

Коммутаторы используют микросегментацию для уменьшения размеров коллизийных доменов в локальной сети LAN. Это осуществляется путем создания выделенных сетевых сегментов (соединений типа "точка-точка") и соединения этих сегментов в виртуальную сеть внутри коммутатора.

Эта виртуальная сеть существует только тогда, когда двум узлам требуется обменяться данными. Такая сеть называется виртуальной, поскольку она существует только в случае необходимости и устанавливается внутри коммутатора. На рис. 7.2 показана сеть до и после микросегментации.



Рис. 7.2 Микросегментация сети

Микросегментация

Использование микросегментации позволяет рассматривать коммутаторы локальных сетей LAN как многопортовые мосты. Обмен данными в них происходит с высокой скоростью путем пересылки фрейма к получателю. Как показано на рис. 7.3, считывая MAC-адрес получателя (2-го уровня) коммутаторы могут достигать высокой скорости передачи данных, которая характерна для мостов. Пересылка фрейма принимающей станции начинается еще до того, как весь фрейм поступит на коммутатор. Благодаря этому значительно сокращается задержка и увеличивается скорость пересылки фреймов. На рис. 7.4 показана таблица коммутации.

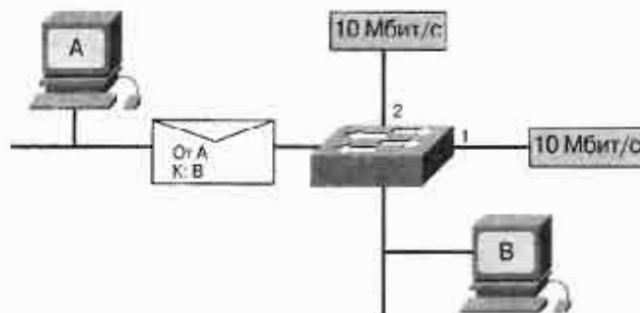


Рис. 7.3 Функционирование коммутатора в сети LAN

Ethernet-коммутация увеличивает доступную полосу пропускания сети. Это осуществляется путем создания выделенных сетевых сегментов (соединений типа “точка-точка”) и соединения этих сегментов в виртуальную сеть внутри коммутатора.

Эта виртуальная сеть существует только тогда, когда двум узлам требуется обмениваться данными. Такая сеть называется виртуальной, поскольку она существует только в случае необходимости и устанавливается внутри коммутатора.



Рис. 7.4. Таблица коммутации

Хотя коммутаторы локальных сетей LAN уменьшают размер коллизийных доменов, все узлы, подсоединенные к коммутатору, остаются в одном и том же широковещательном домене. Вследствие этого при передаче широковещательного сообщения одним из узлов все остальные узлы, подсоединенные LAN-коммутатору, также получают его. Коммутаторы являются устройствами канального уровня, которые, как и мосты, позволяют соединить несколько физических LAN-сегментов в более крупную сеть. Как и мосты, коммутаторы пересылают фреймы на основе содержащихся в них MAC-адресов. Поскольку коммутация происходит в средствах аппаратного, а не программного обеспечения, она осуществляется значительно быстрее. Каждый порт коммутатора фактически выполняет функции микромоста. Он действует как отдельный мост и предоставляет каждому узлу всю доступную полосу пропускания среды. На рис. 7.5 приведен пример того, как коммутатор сегментирует сеть, которая остается одним широковещательным доменом.



Рис. 7.5 Обзор LAN-коммутации

Как коммутатор узнает адреса устройств

Коммутатор сети Ethernet может узнать адреса всех устройств сети путем считывания MAC-адресов источников каждого получаемого фрейма каждого получаемого фрейма данных и регистрируя порт, через который фрейм поступил на коммутатор. После этого коммутатор добавляет эту информацию в свою базу данных пересылки, называемую также таблицей коммутации. Адреса регистрируются в этой таблице динамически, т.е. по мере поступления. Это означает, что по мере считывания новых адресов они анализируются и хранятся в *адресуемой по содержанию памяти (content-addressable memory — CAM)*. Если адрес источника в полученном фрейме отсутствует в памяти CAM, то он анализируется и хранится для будущего использования.

При каждой записи адреса в память регистрируется текущее время. Это позволяет хранить адрес в течение заданного периода времени. При каждом использовании этого адреса или обнаружения его в памяти CAM (при анализе новых адресов) он получает новую метку времени. Если в течение определенного времени на адрес не было ссылок, то он удаляется из списка. Путем удаления устаревших адресов память CAM поддерживает точную и полнофункциональную базу данных пересылки. Это особенно важно если у рабочей станции заменяется карта сетевого интерфейса (сетевой адаптер).

Если станции А требуется передать данные станции В, то посылаемые ею данные проходят через коммутатор, как показано на рис. 7.6. Следует помнить о том, что при прохождении данных по сети коммутатор функционирует на 2-м уровне, т.е. просматривает лишь адрес управления доступом к среде, называемый MAC-адресом (Media Access Control — MAC). Как показано на рис. 7.7, по мере прохождения фреймов данных через коммутатор осуществляется просмотр MAC-адресов источников и, при необходимости, их сохранение в адресной таблице.

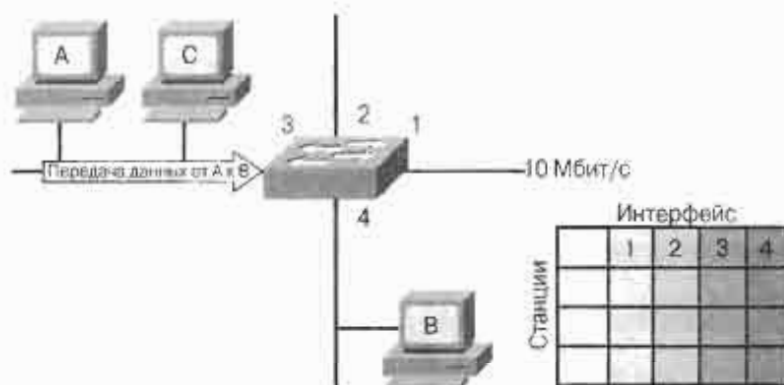


Рис. 7.6. Пример выполнения коммутации в среде локальной сети LAN

При поступлении пакета на порт коммутатора в этой таблице создается позиция, указывающая MAC-адрес станции, отправившей этот пакет, и порт, на который он поступил.

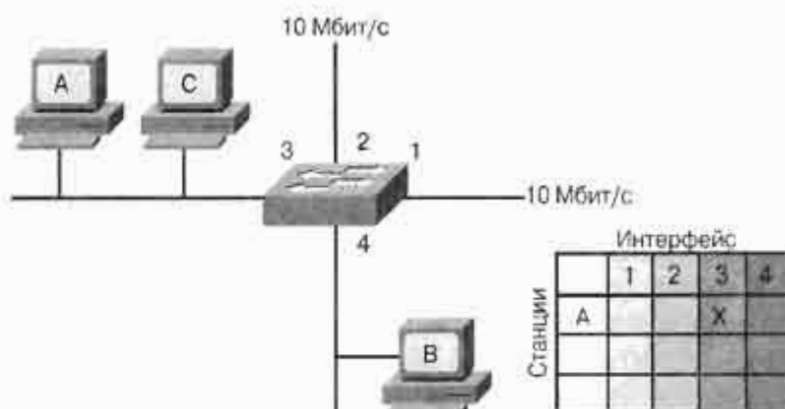


Рис. 7.7. Обновление таблицы пересылки

При необходимости переслать фрейм коммутатор анализирует его MAC-адрес и просматривает свою память CAM в поисках порта, с которого можно было бы отправить фрейм по этому адресу. Если коммутатор не находит в своей таблице пересылки позиции, соответствующей этому адресу, то он рассылает этот фрейм со всех своих портов, за исключением того, на котором он был получен (такая рассылка называется лавинной, flood), как показано на рис. 7.8. Если станция A посылает фрейм станции B, то коммутатор рассылает его со всех своих портов, поскольку пункт назначения неизвестен. Однако когда станция B отвечает станции A, коммутатор рассматривает MAC-адрес станции B как адрес источника и создает для него позицию в памяти CAM. Теперь коммутатору известно, где станция B подсоединена к сети.

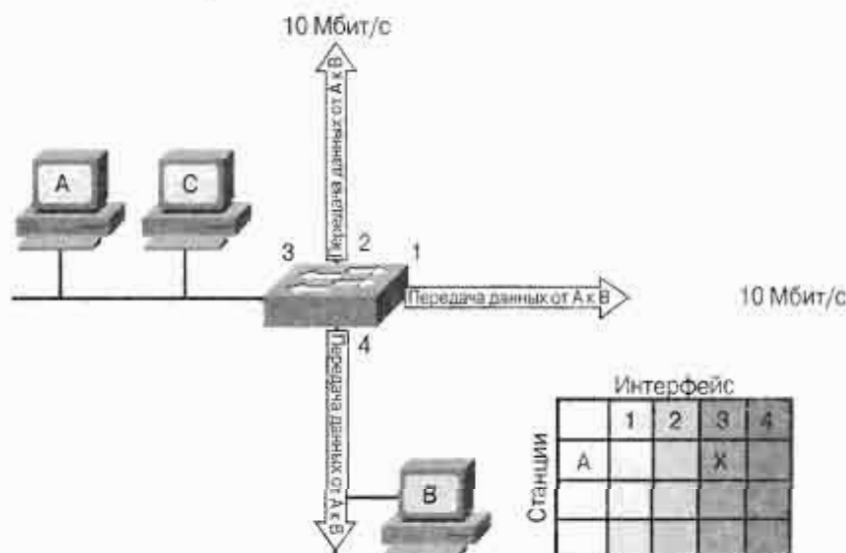


Рис. 7.8. Лавинная рассылка фрейма

Теперь данные пересылаются через коммутатор от станции A к станции B и при этом не требуется лавинная рассылка. Коммутатор посылает данные только с порта 3, поскольку ему известно расположение станции A в сети. Как показано на рис. 7.9, станция B посылает данные коммутатору. На рис. 7.10 показано как коммутатор передает данные от станции B к станции A. Первоначальная передача данных указала коммутатору откуда поступил MAC-адрес, что позволило ему в дальнейшем передавать данные по сети более эффективным образом.

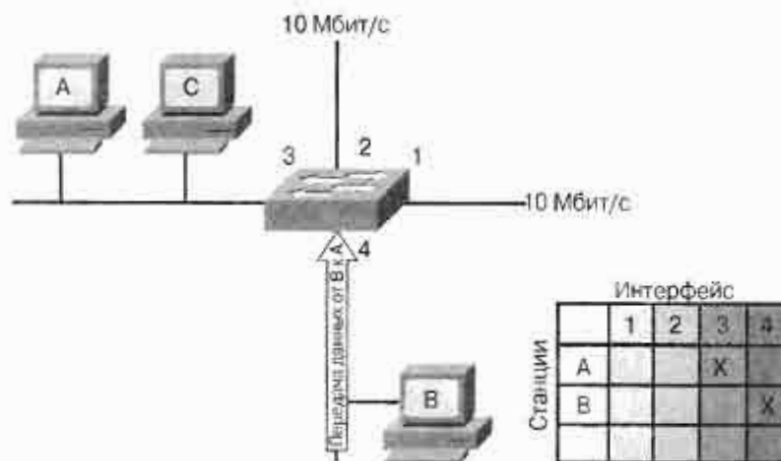


Рис. 7.9. Передача данных от станции В коммутатору

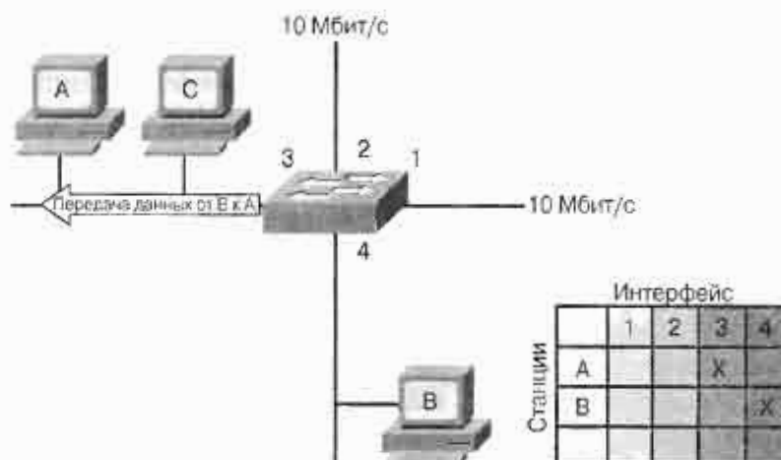


Рис. 7.10. Передача данных от станции В к станции А

Пересылка данных коммутатором

Пересылка фреймов коммутатором может осуществляться в двух режимах: в сквозном режиме (cut-through) или в режиме с промежуточным хранением (store-and-forward).

Пересылка данных с промежуточным хранением

При пересылке данных с промежуточным хранением (store-and-forward switching) перед отправкой фрейма коммутатор ожидает пока он поступит полностью. Перед пересылкой фрейма к нему применяются фильтры, и коммутатор считывает адреса источника и получателя. До полного получения фрейма проходит некоторый промежуток времени, называемый задержкой. Задержка увеличивается при увеличении размера фрейма, поскольку для его прочтения требуется большее время. Однако, с другой стороны, в ожидании полного получения фрейма коммутатор может проверить фрейм на наличие в нем ошибок, как показано на рис. 7.11.



Рис. 7.11. Заголовок фрейма

Сквозная пересылка

При использовании *сквозной коммутации (cut-through switching)* коммутатор считывает адрес получателя только в начале получения фрейма. После этого, еще до полного поступления фрейма, начинается его пересылка. В таком режиме уменьшается задержка при передаче, однако возможности коррекции ошибок ограничены (рис. 7.12).

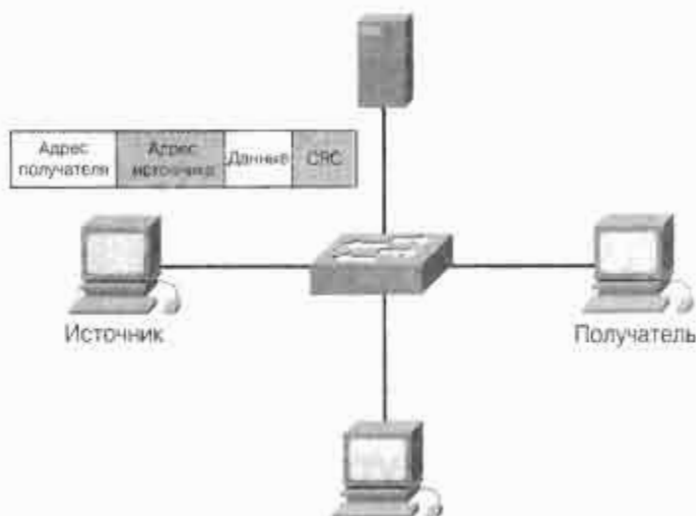


Рис. 7.12. Коммутация с промежуточным хранением

Используются два вида сквозной коммутации:

- **Быстрая пересылка (Fast-forward switching)** — Этот тип коммутации обеспечивает минимальную задержку, поскольку пересылка пакета начинается сразу после получения части фрейма, содержащей адрес получателя. Поскольку быстрая пересылка начинается до полного получения пакета, пакеты могут передаваться с ошибками. Хотя ошибки бывают относительно редко, а сетевой адаптер получателя отбрасывает пакеты с ошибками при их получении, в некоторых ситуациях передача данных с ошибками может оказаться неприемлемой. Для уменьшения количества пакетов с ошибками рекомендуется использовать режим коммутации без фрагментации. В режиме быстрой пересылки задержка измеряется периодом времени от первого полученного бита до первого отправленного, т.е. по принципу “первым пришел — первым ушел” (first in, first out — FIFO).

- **Коммутация без фрагментации (Fragment-free switching)** — При использовании этого типа коммутации перед отправкой пакетов происходит фильтрация коллизийных фрагментов, которые составляют большинство пакетов с ошибками. В корректно работающей сети попавшие в коллизию фрагменты имеют размер менее 64 байтов. Все пакеты, имеющие размер более 64 байтов, считаются действительными и обычно не содержат ошибок. При коммутации без фрагментации перед пересылкой пакета проверяется, не является ли он коллизийным фрагментом. При использовании этого вида коммутации задержка также измеряется по методу FIFO.

В каждом режиме коммутации задержка зависит от способа, которым коммутатор пересылает фрейм. Быстрые режимы коммутации приводят к меньшей задержке пакетов на коммутаторе. Однако при быстрой пересылке у коммутатора остается меньше времени на коррекцию ошибок. Меньший уровень коррекции ошибок приводит к увеличению объема повторных передач, поэтому при выборе метода коммутации требуется находить компромиссное решение. Другим вариантом является использование коммутации с промежуточным хранением, которая увеличивает задержку, но гарантирует целостность данных.

Симметричная коммутация

Понятие *симметричной коммутации (Symmetric switching)* характеризует коммутатор сети LAN в отношении ширины полосы пропускания, выделяемой каждому порту коммутатора, как показано на рис. 7.13. Симметричный коммутатор обеспечивает соединения между портами с одинаковой полосой пропускания, т.е. между портами 10 Мбит/с или портами 100 Мбит/с. Как показано на рис. 7.14, асимметричный коммутатор сети LAN поддерживает соединения между портами с различной полосой пропускания, например между портом 10 Мбит/с и портом 100 Мбит/с.

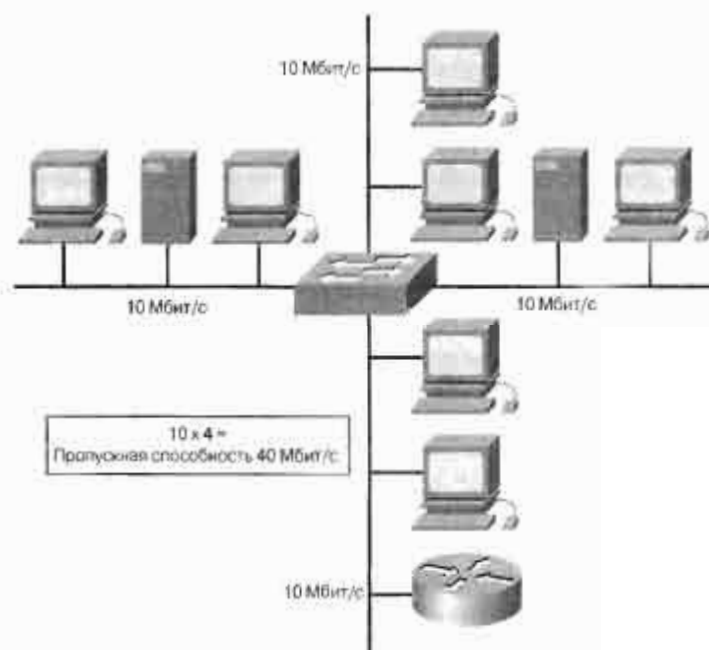


Рис. 7.13. Симметричная коммутация

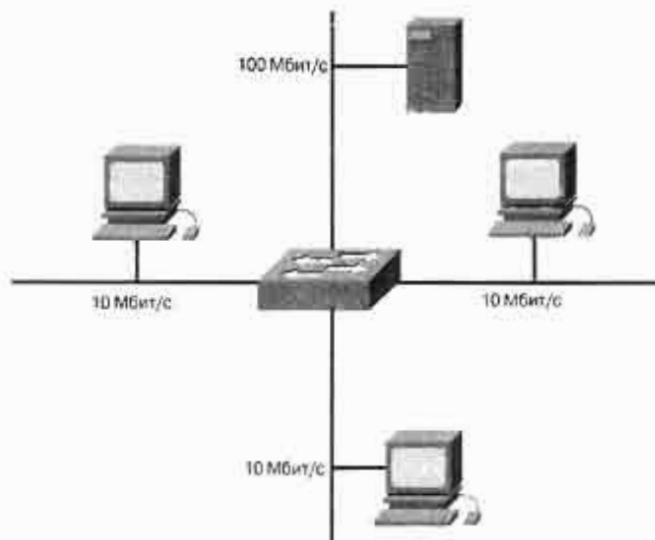


Рис. 7.14. Асимметричная коммутация

Асимметричная коммутация

Асимметричная коммутация (Asymmetric switching) преобладает в сетях модели “клиент-сервер”, в которых несколько пользователей одновременно осуществляют связь с сервером, что требует большей полосы пропускания у порта коммутатора, подсоединенного к серверу, для того чтобы предотвратить переполнение на этом порте. Как будет показано в следующем разделе, в асимметричном коммутаторе необходимо использовать буфер памяти для пересылки данных с порта 100 Мбит/с на порт 10 Мбит/с не вызывая при этом переполнения на порте 10 Мбит/с.

Использование буфера памяти

Метод буферизации данных в памяти может использоваться для пересылки с промежуточным хранением. Буферизация может также использоваться в тех случаях, когда порт получателя занят получением других данных. Область памяти, в которой коммутатор хранит данные, называется буфером памяти. Для пересылки пакетов буфер может использовать два метода: *буферизация по портам (port-based memory buffering)* и *буферизация в общей памяти (shared memory buffering)*.

При использовании буферизации по портам пакеты хранятся в очередях, связанных с конкретными входными портами. Пакет передается на выходной порт только тогда, когда успешно переданы все находящиеся перед ним пакеты очереди. В такой ситуации отдельный пакет в случае занятости его порта-получателя может задержать передачу всех остальных пакетов, находящихся в памяти. Эта задержка происходит даже в том случае, если все остальные пакеты могут быть отправлены на свои открытые порты получателей.

При буферизации в общей памяти все пакеты размещаются в буфере коммутатора, который совместно используется всеми портами. При этом каждому порту выделяется требуемый ему объем памяти. Такой метод называется *динамическим выделением буферной памяти (dynamic allocation of buffer memory)*. Пакеты динамически связываются с передающим портом; при этом каждый пакет хранится в области памяти, вы-

деленной этому порту. Это позволяет принимать пакет на одном порте, а отправлять его с другого порта, не перемещая его в другую очередь.

Коммутатор при этом поддерживает карту портов, на которые должны быть отправлены хранящиеся в буфере пакеты. Соответствующие позиции этой карты очищаются только после того, как пакет был успешно отправлен. Поскольку буфер памяти совместно используется всеми портами, размер пакета ограничивается не тем объемом памяти, который выделен его порту, а лишь всем объемом буфера памяти. При передаче крупных пакетов это приводит к уменьшению количества отброшенных пакетов. Это важно при асимметричной коммутации 10/100 Мбит/с, когда данные с порта 100 Мбит/с требуется передавать на порт 10 Мбит/с.

Коммутаторы и коллизийные домены

Главным недостатком сетей Ethernet/802.3 является то, что в них часто возникают коллизии. Они являются результатом попытки двух станций одновременно передавать фреймы. Особенно часто коллизии возникают в ныне устаревших реализациях сетей Ethernet: в топологии с общей шиной и при использовании концентраторов. При возникновении коллизий передаваемые фреймы повреждаются или уничтожаются. Согласно используемому в спецификации Ethernet/802.3 методу множественного доступа с обнаружением коллизий (carrier sense multiple access collision detect — CSMA/CD) в случае возникновения коллизии передающие станции прекращают передачу на некоторый случайно выбираемый промежуток времени. Как показано на рис. 7.15, коллизии понижают эффективность работы сети.

Под коллизийным доменом понимается область сети в, которой формируются и сталкиваются фреймы. Как показано на рис. 7.16, любая среда передачи, которая совместно используется несколькими устройствами, является коллизийным доменом. При подсоединении рабочей станции к порту коммутатора последний создает выделенное для этой станции соединение. Это соединение рассматривается как индивидуальный коллизийный домен. Например, если к каждому порту 12-портового коммутатора подсоединено отдельное устройство, то создаются 12 коллизийных доменов.



Рис. 7.15. Коммутаторы и коллизийные домены

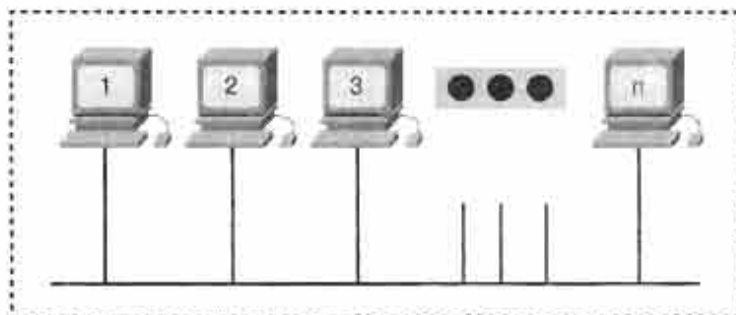


Рис. 7.16. Совместный доступ устройств к среде передачи

Коммутатор строит свою таблицу коммутации путем изучения MAC-адресов 2-го уровня устройств, подсоединенных ко всем портам коммутатора. Если двум устройствам требуется установить связь друг с другом, то коммутатор просматривает таблицу коммутации и устанавливает виртуальное соединение между соответствующими портами. Это соединение называется виртуальным по той причине, что оно существует только в случае необходимости. Если оно больше не требуется, то происходит его отключение.

Это, в свою очередь, создает микросегмент. Микросегмент ведет себя так, как если бы сеть имела только две рабочих станции: одну передающую данные, а другую получающую их. Это позволяет в максимальной степени использовать доступную полосу пропускания. Таким образом, коммутаторы уменьшают количество коллизий в сети и увеличивают полосу пропускания в сетевых сегментах, поскольку они обеспечивают выделенную полосу пропускания каждому сетевому сегменту.

Коммутаторы и широковещательные домены

Обмен данными в сети может происходить тремя способами. Типичным способом является одноадресная передача. При ее использовании отправитель пытается передать данные одному получателю.

Другим способом является многоадресная передача. Такой способ передачи используется в тех случаях, когда данные от одного отправителя требуется передать группе получателей, находящихся в некотором сегменте сети. В такой группе многоадресной рассылки участвуют только те станции, которым требуются передаваемые многоадресные данные. На рис. 7.17 показаны коммутаторы и различные широковещательные домены.

Последним из рассматриваемых способов является широковещательная передача. Если передающему устройству требуется передать данные все получателям в сети, то оно посылает широковещательное сообщение. В этом случае каждый узел сегмента получает широковещательные фреймы, как показано на рис. 7.17.

Если устройству требуется отправить широковещательное сообщение на 2-м уровне, то в качестве MAC-адреса получателя во фрейме устанавливается максимально возможное значение, т.е. FF : FF : FF : FF : FF : FF. Установка такого адреса получателя обеспечивает получение и обработку такого широковещательного фрейма всеми устройствами сегмента. Широковещательный домен на 2-м уровне называется также MAC-доменом. Этот MAC-домен состоит из всех устройств данной сети LAN, которые получают широковещательные фреймы, передаваемый любым из устройств этого домена.

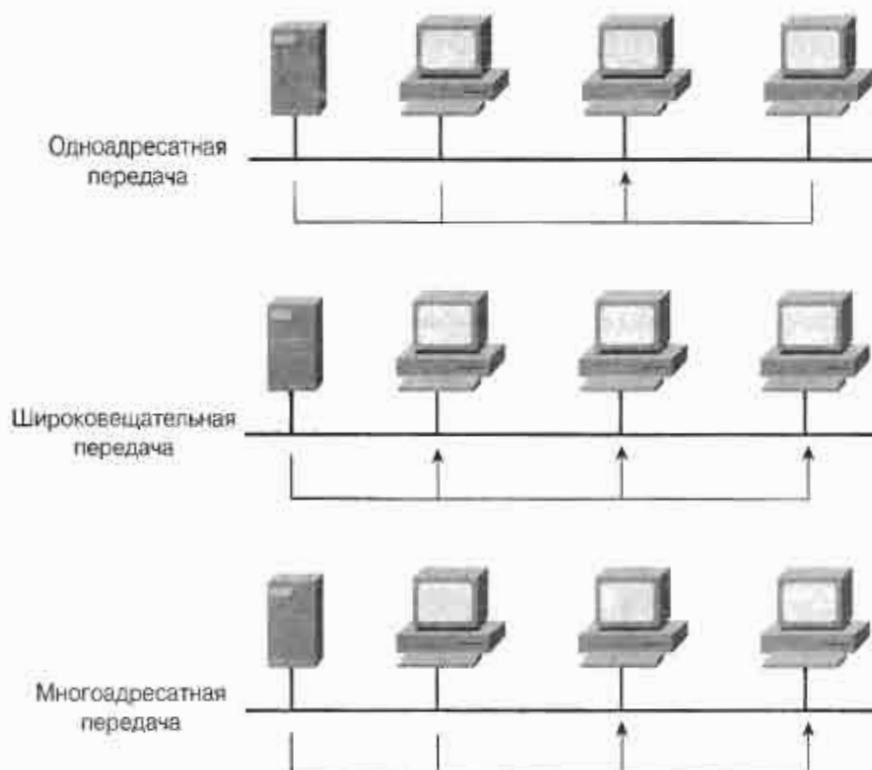


Рис. 7.17. Коммутаторы и широковещательные домены

Коммутатор представляет собой устройство 2-го уровня. При получении широковещательного фрейма коммутатор пересылает его на все свои порты, за исключением того, на который он поступил. Каждое подсоединенное к данному коммутатору устройство должно обработать этот широковещательный фрейм. Это приводит к понижению эффективности работы сети, поскольку часть доступной полосы пропускания расходуется на широковещание, как показано на рис. 7.18.

При соединении двух коммутаторов размер широковещательного домена увеличивается. В данном примере широковещательный фрейм направляется на все порты коммутатора Switch 1. Если подсоединить коммутатор Switch 1 к коммутатору Switch 2, то этот фрейм будет пересылаться и всем устройствам, подсоединенным к коммутатору Switch 2, как показано на рис. 7.19.

Результатом этого станет уменьшение доступной полосы пропускания, поскольку все устройства широковещательного домена должны будут принять и обработать этот широковещательный фрейм.

Маршрутизаторы являются устройствами 3-го уровня. Они не распространяют дальше полученные широковещательные фреймы и поэтому используются для превращения в отдельные сегменты как коллизионных, так и широковещательных доменов.

Широковещательный домен

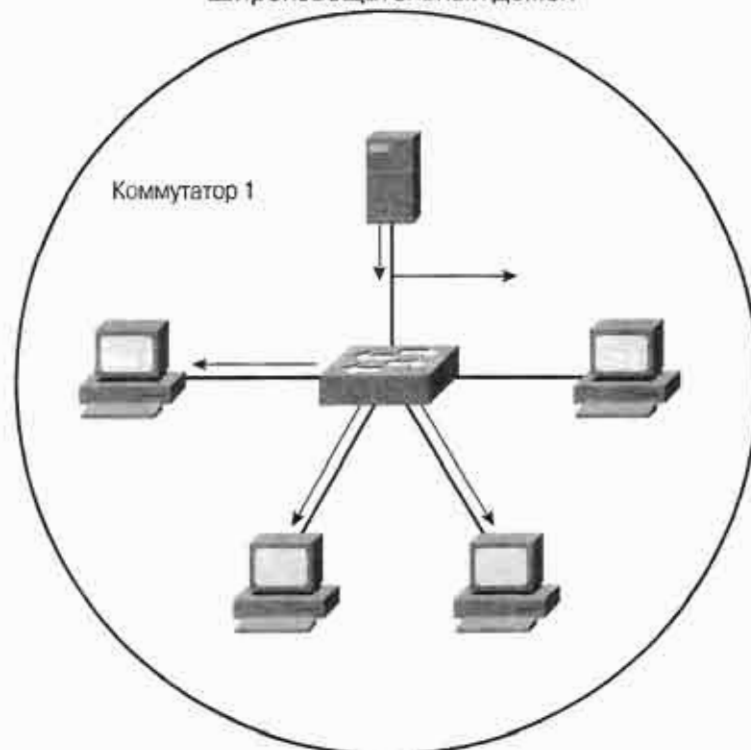


Рис. 7.18. Отдельный широковещательный домен

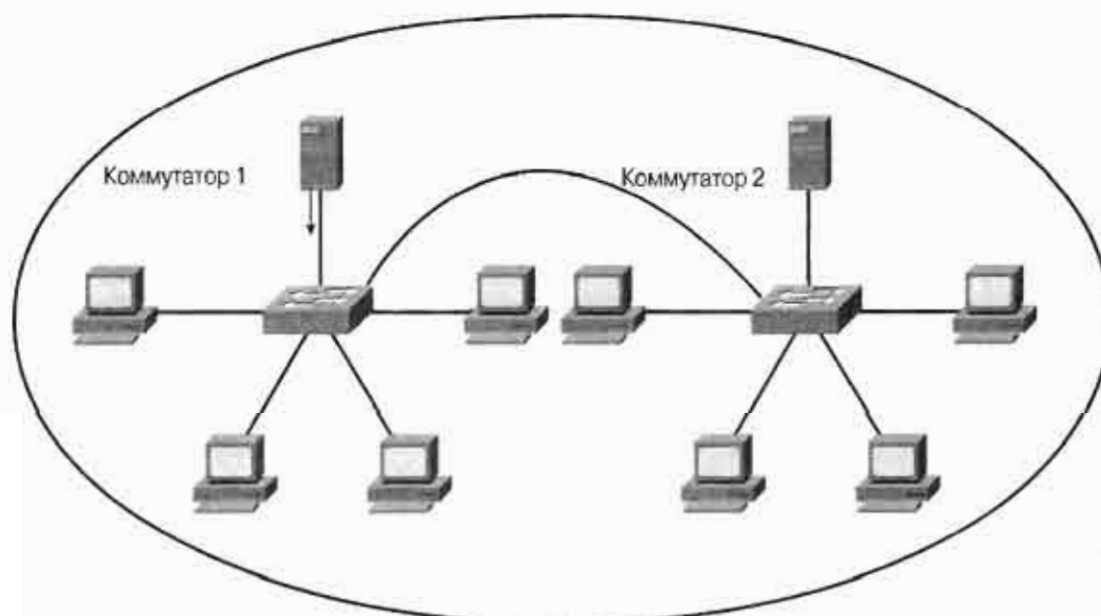


Рис. 7.19. Несколько широковещательных доменов коммутатора

Связь между коммутаторами и персональными компьютерами

Коммутатор является устройством 2-го уровня, которое обладает интеллектуальными функциями и использует их для изучения MAC-адресов устройств, которые подсоединены к его портам. Эти данные заносятся в таблицу коммутации. После того, как эта таблица сформирована, коммутатор может прочитать MAC-адрес получателя в поступающем на какой-либо его порт фрейме, просмотреть свою таблицу коммутации и переслать этот фрейм данных с порта, который соответствует MAC-адресу получателя.

Передача данных от персонального компьютера к коммутатору

Когда персональный коммутатор PC подсоединяется к коммутатору, он не знает о существовании других устройств, которые также подсоединены к среде передачи данной локальной сети. Коммутатор просто направляет фреймы данных через сетевой адаптер (карту сетевого интерфейса) в среду передачи. Персональный компьютер PC может быть подсоединен к другому PC с помощью перекрученного кабеля или к другому сетевому устройству, такому как концентратор, коммутатор или маршрутизатор с помощью прямого кабеля.

Осуществление связи между коммутаторами

Если рабочая станция А, имеющая MAC-адрес А, передает данные станции В, имеющей MAC-адрес В, то передаваемый фрейм поступает на порт 1 коммутатора А. Этот коммутатор считывает MAC-адрес входящего фрейма данных и просматривает свою таблицу коммутации. Из нее он узнает, что MAC-адрес станции В соответствует порту 2 и передает этот фрейм на данный выходной порт.

ПРИМЕЧАНИЕ

Для подсоединения рабочей станции к коммутатору следует использовать прямой кабель.

Одному порту коммутатора в таблице коммутации могут соответствовать несколько MAC-адресов. Такая ситуация типична при подсоединении к коммутатору концентраторов, соединяющих несколько рабочих станций или в случае соединения между собой коммутаторов.

Аналогичная ситуация возникает в тех случаях, когда необходимо осуществить обмен данными между двумя коммутаторами. В данном случае станции А требуется передать данные станции F, имеющей MAC-адрес F.

Станция А передает фрейм на порт А коммутатора А. Коммутатор А просматривает свою таблицу коммутации, но не находит в ней MAC-адрес получателя, т.е. порта F. В этом случае он рассылает поступивший к нему фрейм со всех своих портов, за исключением того, на который данный фрейм поступил. Такой метод называется лавинной рассылкой. Станции В и С анализируют MAC-адрес поступающего к ним фрейма и отбрасывают его, поскольку адрес получателя в нем не соответствует их MAC-адресам. Фрейм данных также пересылается на порт 2 коммутатора В. Этот коммута-

тор 2 просматривает свою таблицу коммутации и находит в ней MAC-адрес получателя. После этого он пересылает фрейм станции F, имеющей MAC-адрес F, через порт 4.

Когда станция F отвечает станции A, эта процедура выполняется в обратном порядке. Узел A может теперь обновить свою таблицу коммутации, логически связав станцию F с портом 4. Коммутатор 2 также может обновить свою таблицу коммутации, связав станцию A с портом 2.

В конечном итоге коммутатор A будет знать, что станции D, E и F логически связаны с портом 4, а для коммутатора B станции A, B и C будут связаны с портом 2.

Тестирование начальной конфигурации коммутатора Catalyst

Новый коммутатор имеет стандартную начальную конфигурацию, установленную производителем. Эта конфигурация редко совпадает с той, которая нужна сетевому администратору. Конфигурирование и управление коммутатором могут осуществляться через интерфейс командной строки. В настоящее время все более широкое применение получает конфигурирование и управление сетевыми устройствами через Web-интерфейс с использованием браузера.

Для эффективного управления сетью, содержащей коммутаторы, сетевой администратор должен уметь решать разнообразные задачи. Некоторые из этих задач связаны с поддержкой работы коммутатора и установленной на нем межсетевой операционной системы (Internetworking Operating System — IOS), другие — с управлением интерфейсами коммутатора и его таблицами с целью обеспечения оптимальной, надежной и безопасной его работы.

Бывают случаи, когда пользователь забывает пароль и в этом случае сетевой администратор должен выполнить процедуру восстановления пароля для получения доступа к коммутатору. Базовое конфигурирование коммутатора, обновление версии операционной системы и восстановление паролей являются существенными навыками, которыми должен владеть сетевой администратор.

Тестирование стандартной конфигурации коммутатора Catalyst

При первом включении питания коммутатора в его файле текущей конфигурации (running configuration file) содержатся стандартные установки. Коммутатор имеет стандартное имя Switch. На консоли и линиях виртуального терминала (virtual terminal — vty) пароли не установлены. В примере 7.1 команда **show run** используется для отображения стандартной конфигурации коммутатора, работающего в среде операционной системы Cisco IOS, такого, например, как коммутатор серии Cisco 2900.

Пример 7.1. Стандартная конфигурация коммутатора

```
Switch#show run
Building configuration...
Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
!
hostname Switch
!
!
ip subnet-zero
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
<OUTPUT OMITTED>
!
line con 0
transport input none
stopbits 1
line vty 5 15
!
end
```

Свойства портов коммутатора

Для просмотра свойств интерфейса используется команда IOS **show interface**. В ней необходимо указать номер слота и порта (в формате 0/1). По умолчанию порты коммутатора (интерфейсы) установлены на автоматический режим, как показано в примере 7.2. Это означает, что они автоматически определяют режим работы — дуплексный или полудуплексный, а также скорость порта — 10 Мбит/с или 100 Мбит/с.

Пример 7.2. Стандартные свойства интерфейса

```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is down, line protocol is down
Hardware is Fast Ethernet, address is 0008.e32e.e601
(bia 0008.e32e.e601)
MTU 1500 bytes, BW 0 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
Auto-duplex , Auto Speed
, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:31:54, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
```

```

5 minute output rate 0 bits/sec, 0 packets/sec
1 packets input, 64 bytes
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast
0 input packets with dribble condition detected
5 packets output, 495 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier

```

Свойства виртуальной локальной сети VLAN

По умолчанию все порты коммутатора находятся в 1-й виртуальной локальной сети LAN (virtual LAN — VLAN). Эта сеть VLAN 1 считается стандартной сетью управления (management VLAN). Для отображения информации о сетях VLAN, определенных на коммутаторе, используется команда **show vlan**. В примере 7.3 показаны стандартные свойства для локальной виртуальной сети VLAN 1. Следует отметить, что все 12 портов этого коммутатора находятся в сети VLAN 1; по умолчанию все порты первоначально принадлежат этой сети VLAN 1.

Пример 7.3. Стандартные свойства сети VLAN 1

Switch#show vlan									
VLANName		Status	Ports						
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12						
1002	fddi-default	active							
1003	token-ring-default	active							
1004	fddinet-default	active							
1005	trnet-default	active							
VLANType	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode		
Trans1	Trans2								
1	enet	100001	1500	-	-	-	-	-	-
	1002 1003								
1002	fddi	101002	1500	-	-	-	-	-	-
	1 1003								
1003	tr	101003	1500	1005	0	-	-	srb	
	1 1002								
1004	fdnet	101004	1500	-	-	1		ibm	-
	0 0								
1005	trnet	101005	1500	-	-	1		ibm	-
	0 0								

Флэш-каталог (Flash Directory)

Поскольку новый коммутатор еще не конфигурировался, в его флэш-каталоге отсутствуют файл базы данных сетей VLAN (**vlan.dat**) и файл сохраненной конфигурации (**config.text**). Файл **vlan.dat** используется для хранения информации о локальных VLAN этого коммутатора и коммутатор использует его для совместного

использования информации о сетях VLAN с другими коммутаторами. По умолчанию во флэш-каталоге имеется файл, содержащий образ операционной системы IOS (с расширением `.bin`), файл переменных среды с именем `env_vars` и подкаталог с именем `html`. Для отображения содержимого флэш-каталога используется команда **dir flash:**, как показано в примере 7.4.

Пример 7.4. Отображение содержимого флэш-каталога

```
Switch#directory flash:
Directory of flash:/
 2  -rwx 1674921   Apr 30 2001 15:09:51 c2950-c3h2s-mz.120-
5.3.WC.1.bin
 3  -rwx 269      Jan 01 1970 00:00:57 env_vars
 4  drwx 10240    Apr 30 2001 15:09:52 html
7741440 bytes total (4780544 bytes free)
```

Отображение информации о версии операционной системы IOS

Узнать номер установленной на коммутаторе версии IOS и установки регистра конфигурации можно с помощью команды **show version**, как показано на рис. 7.5. При этом также отображается другая информация, такая как имя файла образа операционной системы IOS, номер модели коммутатора, серийный номер, объем доступной памяти, а также количество и тип всех портов коммутатора.

Пример 7.5. Отображение версии IOS и установок регистра конфигурации

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-C3H2S-M), Version 12.0(5.3)WC(1),
MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 07:56 by devgoyal
Image text-base: 0x80010000, data-base: 0x8031A000
ROM: Bootstrap program is CALHOUN boot loader
Switch uptime is 1 hour, 24 minutes
System returned to ROM by power-on
System image file is "flash:c2950-c3h2s-mz.120-5.3.WC.1.bin"
cisco WS-C2950-12 (RC32300) processor (revision B0) with 22260K
bytes of memory.
Processor board ID FOC0605W0BH
Last reset from system-reset
Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
12 FastEthernet/IEEE 802.3 interface(s)
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:08:E3:2E:E6:00
Motherboard assembly number: 73-5782-08
Power supply part number: 34-0965-01
Motherboard serial number: FOC060502HP
Power supply serial number: PHI05500C5D
Model revision number: B0
Motherboard revision number: B0
Model number: WS-C2950-12
System serial number: FOC0605W0BH
Configuration register is 0xF
```


Преимущества использования стандартной конфигурации

В этой стандартной конфигурации коммутатор имеет один широковещательный домен и может управляться и конфигурироваться через консольный порт с использованием интерфейса командной строки. В этой конфигурации также установлен протокол связующего дерева. При этом обеспечен повышенный уровень безопасности, поскольку коммутатору еще не был назначен IP-адрес.

Для небольших сетей стандартная конфигурация может оказаться вполне достаточной. Пользователь сразу может воспользоваться преимуществами микросегментации и высокой производительности сети, которые обеспечиваются коммутатором.



Лабораторная работа: тестирование стандартной конфигурации коммутатора

В этой лабораторной работе анализируются (изучаются) установки коммутатора модели Catalyst 29xx. Требуется подключиться к консольному порту коммутатора с использованием программы HyperTerminal и с помощью различных команд **show** собрать информацию о текущей конфигурации коммутатора.

Изменение сетевых установок коммутатора Catalyst

Коммутатор может быть уже сконфигурирован и потребуются только ввести пароли для входа и получения доступа к режимам пользователя: EXEC, ENABLE и PRIVILEGED EXEC. Вход в режим конфигурирования коммутатора происходит из режима PRIVILEGED EXEC. В командной строке стандартная заставка для привилегированного exec-режима имеет вид Switch#. В EXEC-режиме пользователя заставка имеет вид Switch>.

Изменение стандартных установок коммутатора

При необходимости пользователь может полностью изменить существующую конфигурацию как показано на рис. 7.6. Для этого следует выполнить описанные ниже действия.

- Удалить существующую VLAN-информацию путем удаления файла `vlan.dat` базы данных VLAN из флэш-каталога.
- Удалить резервный файл конфигурации `startup-config`. (В примере показано, как сделать это для коммутаторов catalyst 2950 и 1900).
- Перезагрузить коммутатор.

Пример 7.6 Изменение стандартных установок конфигурации коммутаторов серий 2950 и 1900

```
Catalyst 2950
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#erase startup-config
```

```
<output omitted>
Switch#reload
```

```
Catalyst 1900
Switch#delete nvram
```

Назначение коммутатору имени и задание паролей

Ведение документации, обеспечение безопасности и управления являются важной частью работы с любым устройством объединенной сети. Коммутатору необходимо назначить имя, а на консоли и на каналах vty (Telnet) должны быть заданы пароли, как показано в примере 7.7.

Пример 7.7 Назначение имени коммутатору и задание паролей каналам

```
Switch(config)#hostname ALSwitch
ALSwitch(config)#line configuration 0
ALSwitch(config-line)#password
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 4
ALSwitch(config-line)#password
ALSwitch(config-line)#login
```

Назначение коммутатору IP-адреса и шлюза по умолчанию

Для того, чтобы к коммутатору могли получить доступ Telnet и другие приложения TCP/IP, ему необходимо назначить IP-адрес и задать стандартный шлюз (шлюз по умолчанию). В примере 7.8 показано как это сделать для коммутаторов моделей Catalyst 2950 и 1900. По умолчанию сеть VLAN 1 является виртуальной сетью управления. В сети, построенной на коммутаторах, все устройства объединенной сети должны находиться в сети управления VLAN. Это позволяет с одной рабочей станции получать доступ ко всем устройствам объединенной сети, конфигурировать их и управлять ими.

Пример 7.8 Назначение коммутатору IP-адреса и задание стандартного шлюза

```
Catalyst 2950
ALSwitch(config)#interface VLAN1
ALSwitch(config-if)#ip address 192.168.1.2 255.255.255.0

ALSwitch(config)#ip default-gateway 192.168.1.1

Catalyst 1900
ALSwitch(config)#ip address 192.168.1.2 255.255.255.0
ALSwitch(config)#ip default-gateway 192.168.1.1
```

Установка характеристик порта

Порты FastEthernet коммутатора по умолчанию установлены на автоматическое определение скорости передачи и на дуплексный режим. Это позволяет интерфейсам устройств, участвующих в сеансе связи, изменять эти установки. Если сетевому администратору требуется удостовериться в том, что какой-либо интерфейс имеет конкретную скорость передачи (10 Мбит/с или 100 Мбит/с) или режим дуплексирования (дуплексный или полудуплексный), то эти значения могут быть установлены вручную, как показано в примере 7.9.

Пример 7.9 Установка на порте скорости передачи и режима дуплексирования

```

Switch(config)#interface FastEthernet0/2
Switch(config-if)#duplex full
Switch(config-if)#
00:34:01: %LINK-3-UPDOWN: Interface FastEthernet0/2,
changed state to down
00:34:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2,
changed state to down
00:34:03: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
00:34:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2,
changed state to up
Switch(config-if)#speed 100
Switch(config-if)#
00:34:24: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to
down
00:34:25: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2,
changed state to down
00:34:27: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
00:34:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2,
changed state to up

```

Другой полезной функцией, которая может быть установлена на порте, является опция **portfast**. Если порт коммутатора подсоединен только к станциям конечного пользователя (т.е. не подсоединен к другому коммутатору или мосту), то следует установить функцию portfast коммутатора Catalyst на этих портах конечных пользователей. При установленной опции portfast при первом использовании порта он автоматически переходит из заблокированного состояния в состояние пересылки. Установка опции portfast особенно полезна для пользователей сетей Novell NetWare, которым требуется вступить в контакт с сервером NetWare при загрузке для того, чтобы to log on. В примере 7.10 проиллюстрирована установка опции portfast. Состояние portfast показано в столбце *Fast-Start*.

Пример 7.10 Установка на порте опции Portfast и тестирование конфигурации

```

Switch># set spanntree portfast 4/1 enable
Warning: Spanntree port fast start should only be enabled on ports
connected
to a single host. Connecting hubs, concentrators, switches, bridges,
etc. to
a fast start port can cause temporary spanning tree loops. Use with
caution.
Spanntree port 4/1 fast start enabled.
Switch># show spanntree 4/1

```

Port	Vlan	Port-State	Cost	Priority	Fast-Start	Group-method
4/1	1	blocking	19	20	enabled	
4/1	100	forwarding	10	20	enabled	
4/1	521	blocking	19	20	enabled	
4/1	522	blocking	19	20	enabled	

```

4/1      523   blocking      19      20      enabled
4/1      524   blocking      19      20      enabled
4/1      1003  not-connected  19      20      enabled
4/1      1005  not-connected  19      4       enabled
Switch>#

```

Web-интерфейсы

Сетевые устройства, обладающие интеллектуальными функциями, могут обеспечить конфигурирование и управление через Web-интерфейсы. Это становится возможным после того, как на коммутаторе сконфигурирован IP-адрес и стандартный шлюз. Для реализации этой Web-службы браузер должен быть установлен на IP-адрес и порт (по умолчанию [стандартное значение] 80). Пользователь может включить или отключить службу http, а также выбрать для этой службы адрес порта, как показано на рис. 7.11.

Пример 7.11 Включение службы протокола HTTP и выбор порта

```

Switch(config)#ip http ?
access-class Restrict access by access-class
authentication Set http authentication method
path Set base path for HTML
port HTTP port
server Enable HTTP server
Switch(config)#ip http server
Switch(config)#ip http port ?
<0-65535> HTTP port
Switch(config)#ip http port 80
Switch(config)#

```

Любое дополнительное программное обеспечение (апплет) может быть загружено в браузер с коммутатора или с сетевых устройств, управляемых основанным на браузере графическим интерфейсом пользователя (graphical user interface — GUI).



Лабораторная работа: базовая конфигурация коммутатора

В этой лабораторной работе назначить коммутатору IP-адрес и удостовериться в том, что обеспечен доступ к интерфейсу командной строки. Далее следует задать скорость передачи порта и режим дуплексирования, после чего сохранить активную конфигурацию. Необходимо также просмотреть на коммутаторе интерфейс браузера.

Работа с таблицей MAC-адресов

Коммутаторы узнают MAC-адреса персональных компьютеров PC или рабочих станций, подсоединенных к их портам путем анализа адресов источников во фреймах, поступающих на данный порт. Далее эти адреса заносятся в таблицу MAC-адресов коммутатора. Фреймы, адрес получателя которых имеется в этой таблице, могут быть корректно отправлены с соответствующего интерфейса.

Для просмотра известных коммутатору адресов необходимо войти в привилегированный exec-режим, как показано в примере 7.12.

Пример 7.12 Вывод по команде show mac-address-table

```
Switch#show mac-address-table
Dynamic Address Count: 2
Secure Address Count: 0
Static Address (User-defined) Count: 0
System Self Address Count: 13
Total MAC addresses: 15
Maximum MAC addresses: 8192
Non-static Address Table:
Destination Address      Address Type      VLAN Destination Port
-----
0010.7a60.ad7e           Dynamic           1      FastEthernet0/2
00e0.2917.1884           Dynamic           1      FastEthernet0/5
```

Адреса изучаются динамически и коммутатор может поддерживать в целом тысячи MAC-адресов, при этом на каждом порте могут быть несколько адресов. Для экономии памяти и оптимального функционирования коммутатора иногда становится необходимым удалить какие-либо позиции из таблицы MAC-адресов. Для этого все позиции таблицы снабжены временными метками, отображающими время поступления на порт пакета с данным адресом. Рабочие станции могут быть отсоединены от порта, выключены или переключены на другой порт этого же или другого коммутатора. Возможен также случай замены карты сетевого интерфейса (сетевого адаптера). Это может привести к путанице при пересылке фреймов. В силу вышеупомянутых причин коммутатор настроен таким образом, что при отсутствии фреймов с ранее записанным адресом в течение определенного времени (обычно 300 секунд) соответствующая позиция MAC-адреса автоматически удаляется из таблицы.

Вместо ожидания естественного устаревания динамической позиции адреса администратор может использовать для ее удаления команду привилегированного режима **clear mac-address-table**. В примере 7.13 показан вывод по команде **clear mac-address-table**. Позиции MAC-адресов, сконфигурированные администратором, также могут быть удалены подобным образом. Такой способ обеспечивает немедленное удаление позиций таблицы с адресами, которые стали недействительными.

Пример 7.13 Вывод по команде clear mac-address-table

```
Switch#clear mac-address-table
Switch#show mac-address-table
Dynamic Address Count: 0
Secure Address Count: 0
Static Address (User-defined) Count: 0
System Self Address Count: 13
Total MAC addresses: 14
Maximum MAC addresses: 8192
Non-static Address Table:
Destination Address      Address Type      VLAN Destination Port
-----
```

**Лабораторная работа: корректировка таблицы MAC-адресов**

В этой лабораторной работе необходимо создать базовую конфигурацию маршрутизатора и выполнить корректировку таблиц MAC-адресов

Конфигурирование статических MAC-адресов

Возможна ситуация, в которой целесообразно постоянно связать некоторый MAC-адрес с конкретным интерфейсом коммутатора. В этом случае автоматического удаления MAC-адреса после истечения обычного срока сохранения адреса не произойдет.

Постоянный адрес может быть связан с интерфейсом в случае необходимости подсоединить сервер или рабочую станцию пользователя к данному порту при условии что MAC-адрес известен. При этом также может быть повышен уровень безопасности.

Для установки позиции статического MAC-адреса на интерфейсе коммутатора используется приведенный ниже синтаксис команды в режиме глобального конфигурирования.

```
Switch(config)#mac-address-table static mac-address-of-host  
Switch(config)#interface FastEthernet ethernet-number vlan vlan-name
```

Для удаления позиции адреса из таблицы используется форма этой команды с ключевым словом **no**.

Вывод по команде **mac-address-table** приведен в примере 7.14.

Пример 7.14 Конфигурирование статического MAC-адреса

```
Switch(config)#mac-address-table ?  
aging-time Set MAC address table entry maximum age  
secure Configure a secure address  
static Configure a static 802.1d static address  
Switch(config)#mac-address-table static 0010.7a60.1884 interface  
FastEthernet0/5 vlan VLAN1  
Remove Static MAC Address  
Switch(config)#no mac-address-table static 0010.7a60.1884 interface  
FastEthernet0/5 vlan VLAN1
```

**Лабораторная работа: конфигурирование статического MAC-адреса**

В этой лабораторной работе требуется выполнить операции по установке и удалению статических MAC-адресов на портах коммутатора.

Меры безопасности для портов коммутаторов

Обеспечение безопасности в объединенной сети является важной задачей сетевого администратора. Порты коммутатора, относящиеся к уровню доступа, в силу структурной схемы прокладки кабелей доступны в стенных разъемах офисов и других помещений и к любой из них можно подключиться с помощью персонального или переносного компьютера. Они, соответственно, являются потенциальными точками входа в сеть для несанкционированных пользователей. Коммутаторы обладают функцией, называемой обеспечением безопасности портов. В частности, администратор может ограничить количество адресов, которые можно узнать на конкретном интерфейсе. В конфигурации могут быть заданы определенные действия коммутатора в том случае

если это количество превышено, как показано на рис. 7.15. Эти безопасные MAC-адреса могут быть установлены статическим образом. Однако обеспечение безопасности MAC-адресов статическим способом может оказаться достаточно сложной задачей, при решении которой велика вероятность ошибок.

Пример 7.15 Конфигурирование безопасности порта

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#port security ?
action          action to take for security violation
max-mac-count   maximum mac address count
<cr>
Switch(config-if)#port security action ?
shutdown        shut down the port from which security violation
is detected
trap            trap send snmp trap for security violation
```

Альтернативным подходом является реализация мер безопасности для порта на интерфейсе коммутатора. Первым адресом, который динамически узнает коммутатор, становится безопасный адрес. Для изменения типа безопасности на интерфейсе используется форма этой команды с ключевым словом **no**. Для тестирования статуса безопасности на порте используется команда **show port security**.



Лабораторная работа: конфигурирование безопасности на порте

В этой лабораторной работе требуется сконфигурировать меры безопасности на отдельных портах Fast Ethernet коммутатора Catalyst и протестировать управление ими.

Добавление, перемещение и изменение подключения устройств к коммутатору

При установке в сети нового коммутатора ему требуется задать имя, IP-адрес в сети управления VLAN, стандартный шлюз и пароли каналов. Для этого необходимо выполнить описанные ниже действия.

- Присвоить коммутатору имя.
- Выбрать и сконфигурировать IP-адрес для целей управления коммутатором.
- Задать стандартный шлюз.
- Сконфигурировать административный доступ к консольному, вспомогательному интерфейсам, а также к интерфейсу виртуального терминала.
- Сконфигурировать на устройстве меры безопасности.
- При необходимости сконфигурировать порты доступа коммутатора.

Если подключение рабочей станции изменяется с одного порта на другой, то следует удалить элементы конфигурации которые могут вызвать неожиданное поведение коммутатора. После этого могут быть добавлены новые элементы конфигурации. При добавлении, изменении или перемещении рабочих станций необходимо выполнить описанные ниже действия.

- Добавление MAC-адреса:
 - Сконфигурировать на порте меры безопасности;
 - Задать ввести в таблицу MAC-адрес;
- При изменении MAC-адреса:
 - Удалить ограничения на MAC-адрес;
- При перемещении рабочей станции:
 - Задать адрес новому порту;
 - Сконфигурировать меры безопасности на новом коммутаторе;
 - Ввести MAC-адрес порта, который выделен для нового пользователя;
 - Удалить прежнюю конфигурацию порта.



Лабораторная работа: добавление, изменение MAC-адреса и перемещение устройств

В этой лабораторной работе необходимо переместить персональный компьютер с одного порта коммутатора на другой и добавить новый PC в конфигурацию коммутатора.

Управление образами операционной системы и файлами конфигурации устройств

Файлы конфигурации сетевых устройств необходимо добавить в документацию по сети и в дальнейшем поддерживать в корректном состоянии. Настоятельно рекомендуется хранить резервные копии *файла текущей конфигурации (running-configuration)* на сервере или иметь отдельную копию на жестком диске. Эта важная документация может потребоваться при необходимости восстановлении конфигурации. Она также может быть использована при конфигурировании аналогичных коммутаторов. Резервную копию IOS следует создать на локальном сервере. Это позволяет при необходимости перезагрузить IOS во флэш-память.



Лабораторная работа: работа с образом операционной системы коммутатора

В этой лабораторной работе требуется сделать резервную копию файла образа IOS на сервере TFTP, а затем восстановить операционную систему на коммутаторе



Лабораторная работа: работа с файлом начальной конфигурации коммутатора

В этой лабораторной работе требуется сделать резервную копию файла начальной конфигурации на сервере TFTP, а затем восстановить операционную систему на коммутаторе

Восстановление пароля на коммутаторах серий 1900/2950

Все операции управления коммутатором должны проводиться при установленных паролях на канале консоли и на канале виртуального терминала. Также устанавливается обычный пароль и секретный пароль. Это приводит к тому, что доступ к ехес-режиму пользователя и к привилегированному режиму коммутатора будут иметь только санкционированные пользователи.

Однако бывают случаи, когда пользователь имеет физический доступ к коммутатору, но не имеет доступа к ехес-режиму пользователя или к привилегированному режиму, поскольку не знает соответствующих паролей или забыл их. В этих случаях необходимо выполнить процедуру восстановления пароля.



Лабораторная работа: процедура восстановления пароля для коммутаторов Catalyst серии 29XX

В этой лабораторной работе пользователь восстанавливает свой доступ к коммутатору Catalyst 2900 после утраты пароля.

Обновление микропрограммы и IOS коммутаторов 1900/2900

Версии образа операционной системы IOS Cisco и образов микропрограммы аппаратного обеспечения периодически обновляются после устранения обнаруженных ошибок, введения новых функций и повышения производительности. Новая версия IOS может сделать работу сети более безопасной и более производительной. Для этого необходимо обновить используемую версию IOS.

Для обновления версии IOS необходимо получить копию нового образа путем загрузки его с сервера Центра программного обеспечения Cisco (www.cisco.com) на локальный сервер. Для этого следует ввести имя и пароль пользователя. После загрузки образа его можно установить на коммутаторе.



Лабораторная работа: Обновление IOS коммутаторов 1900/2900

В этой лабораторной работе требуется обновить на коммутаторе файлы IOS и HTML.

Резюме

В данной главе были рассмотрены следующие вопросы:

- Мотивы использования коммутаторов для сегментации сети и предоставляемые ими преимущества;
- Способы изучения адресов коммутаторами;
- Различные способы пересылки данных коммутаторами;
- Стандартные установки (установки по умолчанию) коммутаторов Catalyst;

- Задание коммутатору IP-адреса и назначение стандартного шлюза для обеспечения соединений с другими устройствами сети и для управления сетью;
- Просмотр установок коммутатора с помощью Web-браузера;
- Конфигурирование интерфейсов для скоростной и дуплексной передачи;
- Как просмотреть содержимое таблицы MAC-адресов и, при необходимости, внести в нее изменения;
- Как сконфигурировать меры безопасности на порте;
- Управление файлами конфигурации и образами IOS;
- Восстановление пароля на коммутаторе;
- Обновление версии операционной системы, установленной на коммутаторе.

В дополнение к уже изученному материалу данной главы рекомендуется ознакомиться с лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

Адресуемая по содержимому память (content-addressable memory — CAM). Память устройства, доступ к которой осуществляется по характеру требуемой информации, а не по адресу в памяти.

Асимметричная коммутация (asymmetric switching). Метод коммутации, обеспечивающий коммутируемые соединения между портами с разной полосой пропускания, такими, например, как порты 10 Мбит/с и 100 Мбит/с.

Буферизация памяти (memory buffering). Метод буферизации, при котором пакеты перед пересылкой при необходимости хранятся в памяти.

Быстрая коммутация (fast-forward switching). Метод коммутации, при использовании которого коммутация фактически начинается еще до полного поступления всего пакета на коммутатор.

Коллизионный домен (collision domain). В сетях Ethernet область сети, в которой распространяются испытывавшие коллизию фреймы. Повторители распространяют коллизии, а коммутаторы LAN, мосты и маршрутизаторы прекращают их распространение.

Коммутация без фрагментации (fragment-free switching). Метод коммутации, при использовании которого коммутатор перед пересылкой отфильтровывает фрагменты испытывавших коллизию фреймов, которые составляют большинство пакетов с ошибками.

Коммутация с промежуточным хранением (store-and-forward switching). Метод коммутации пакетов, при использовании которого содержимое пакета полностью анализируется перед отправкой его на соответствующий выходной порт. Этот анализ включает в себя вычисление контрольной суммы (cyclic redundancy check — CRC) и проверки адреса получателя. Кроме этого, перед отправкой фреймы могут временно храниться до освобождения сетевых ресурсов, таких как неиспользуемые каналы.

Микросегмент (microsegment). Часть сети, которая образуется в результате разделения (дробления) сети на сегменты меньшего размера, обычно с целью увеличения для отдельных сетевых устройств доступной им полосы пропускания.

Симметричная коммутация (symmetric switching). Метод коммутации, при использовании которого коммутатор обеспечивает соединения только между портами с одинаковой полосой пропускания, таких как порты 10 Мбит/с или порты 100 Мбит/с.

Сквозная коммутация (cut-through switching). Метод коммутации, при использовании которого головная часть пакета начинает отправляться с выходного порта до того, как весь пакет полностью поступит на входной порт. Устройство, осуществляющее сквозную коммутацию, обрабатывают и пересылают пакеты сразу после считывания адреса получателя и определения выходного порта. Сквозная коммутация иногда также называется “коммутацией на лету”.

Широковещательный домен (broadcast domain). Набор устройств, каждый из которых получает широковещательные фреймы, рассылаемые любым устройством из этого набора. Широковещательные домены обычно ограничены маршрутизаторами, поскольку маршрутизаторы не пересылают далее широковещательные фреймы.

Контрольные вопросы

1. Какие из приведенных ниже характеристик связаны с миросегментацией? Следует выбрать все правильные ответы.
 - A. Выделенные маршруты между отправителем и получателем
 - B. Несколько маршрутов передачи данных внутри коммутатора
 - C. Увеличение числа коллизий
 - D. Создание одного широковещательного домена для всей локальной сети LAN
2. Как можно назвать коммутатор локальной сети LAN?
 - A. Многопортовый повторитель, функционирующий на 1-м уровне
 - B. Многопортовый концентратор, функционирующий на 2-м уровне
 - C. Многопортовый маршрутизатор, функционирующий на 3-м уровне
 - D. Многопортовый мост, функционирующий на 2-м уровне
3. С какой целью оптимизируется симметричная коммутация?
 - A. Для передачи данных в сети типа “клиент-сервер”, к которой подсоединен “быстрый” порт коммутатора
 - B. Для равномерного распределения потоков данных в сети
 - C. Для повышения эффективности работы коммутаторов с недостаточным объемом буферной памяти
 - D. Для перераспределения нагрузки между каналами
4. При одном типе коммутации коммутатор просматривает адрес получателя и немедленно начинает пересылку фрейма, при втором типе коммутации сначала происходит получение всего фрейма и лишь после этого начинается пересылка. Каковы эти типы коммутации?
 - A. С промежуточным хранением; симметричная
 - B. Сквозная; с промежуточным хранением
 - C. С промежуточным хранением; сквозная
 - D. С буферизацией в памяти; сквозная

5. При каком типе коммутации используются пересылка без фрагментации и быстрая пересылка?
 - A. Сквозная коммутация
 - B. Коммутация с буферизацией в памяти
 - C. Сквозная коммутация
 - D. Симметричная коммутация
6. Какой кабель следует использовать для подключения рабочей станции к коммутатору?
 - A. Straight-through
 - B. Cross-over
 - C. Нуль-модемный кабель
 - D. Стандартный телефонный кабель
7. При каком типе коммуникации только один узел является отправителем и только один получателем?
 - A. Широковещание
 - B. Одноадресатная пересылка
 - C. Многоадресатная рассылка
 - D. Ни один из вышеперечисленных



В этой главе...

- Описаны цели использования топологий с избыточными маршрутами
- Описан протокол связующего дерева (Spanning Tree Protocol — STP)
- Описаны различные состояния портов связующего дерева и выбор назначенных портов
- Описаны различные этапы выбора корневого моста
- Описано назначение оценки маршруту
- Описана установка таймеров STP
- Описано, как протокол STP содействует ускорению конвергенции
- Описан быстрый протокол связующего дерева (Rapid Spanning Tree Protocol — RSTP)

Протокол связующего дерева STP

В настоящей главе описываются топологии с избыточностью и объясняется их важность для поддержки устойчивой работы сетей. Кроме того, в ней описаны функции двух протоколов: протокола связующего дерева (Spanning Tree Protocol — STP) и протокола RSTP.

Рекомендуется также выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Обзор топологий с избыточностью

Наличие избыточности в сети является важным фактором. Избыточность делает сеть устойчивой к возможным сбоям. Избыточность топологии защищает сеть и обеспечивает ее функционирование в случае сбоя в отдельном канале, на порте или в сетевом устройстве. Однако топологии сетей, построенных на использовании коммутаторов и мостов, обладающие избыточностью, подвержены широковещательным штормам (broadcast storms), множественным передачам фреймов и неустойчивости баз данных, в которых находятся адреса управления доступом к среде передачи (*Media Access Control* — *MAC*), называемые также MAC-адресами.

Что понимается под избыточностью в сети

В настоящее время частные компании и государственные организации в своей деятельности все более полагаются на компьютерные сети. Доступ к файловым серверам, базам данных, к сети Internet, к интранет- и экстранет-сетям является критически важным для успешной работы компаний. В случае неработоспособности сети резко падает производительность работы компании, а потребители выражают неудовлетворенность. Поэтому компании стремятся добиться круглосуточной работоспособности сети на протяжении всей рабочей недели.

Достижение 100% работоспособности сети, вероятно, невозможно, однако обеспечение работоспособности сети на 99,999% (такой уровень надежности называется “пятью девятками”) — цель, которую ставят перед собой компании и организации. Это значение можно представить в среднем как один день простоя сети за 30 лет, один час простоя за 4000 дней или 5,25 минут простоя за год. Эта оценка применима и к другим важным службам, таким как финансовые операции, больницы, работа провайдеров служб Internet и т.д. Цена простоев оказывается весьма высокой. Многим другим предприятиям для уменьшения расходов приходится жертвовать надежностью сети.

Достижение уровня надежности 99,999% требует исключительной надежности от сети. Эта надежность достигается за счет использования надежного оборудования и путем проектирования сети, устойчивой к сбоям и ошибкам. Для этого сеть проектируется таким образом, чтобы в ней быстро происходила реконвергенция и при передаче данных обходился участок со сбоем.

Устойчивость к сбоям достигается за счет создания избыточности в сети. Избыточность означает наличие в сети средств, которые превышают требования обычной ситуации при работе сети. Как избыточность помогает обеспечить надежность?

Предположим, что единственным способом добраться до работы является ваш личный автомобиль. Если в нем произошла поломка, которая сделала его неработоспособным, то добраться до работы станет невозможным до тех пор пока автомобиль не будет отремонтирован.

Если в автомобиле происходит поломка, которая делает его неработоспособным, один раз в десять дней, то процент использования автомобиля составляет 90%. Возможность поехать на работу при этом обеспечивается в 9 днях из 10. Соответственно, надежность составляет 90%.

Покупка еще одного автомобиля улучшает ситуацию, однако для того, чтобы в обычной ситуации просто добраться до работы, двух автомобилей не требуется. Один из них является лишним, однако он доступен в том случае, когда имеются проблемы с первым автомобилем. Это обеспечивает дополнительную надежность.

Топологии с избыточностью

Целью создания избыточности в сети является предотвращение простоя в сети в тех случаях, когда в отдельной точке сети происходит сбой. Для повышения надежности все сети должны обладать избыточностью. Примером сети с избыточностью может служить сеть автомобильных дорог. Если одна трасса закрыта для ремонта, то имеются другие маршруты к требуемому месту.

Предположим, что у крупного города есть небольшой пригород, который отделен от центральной части города рекой. Если через эту реку существует только один мост, то, соответственно, имеется лишь один маршрут к центру города. При такой топологии избыточность отсутствует.

Если на мосту возникла “пробка” или он поврежден в результате дорожного происшествия, то поездка в город через этот мост становится невозможной. Построение второго моста через эту реку создает избыточность в такой автомобильной сети. В этом случае пригород не оказывается отрезанным от центра города в том случае, если по одному из мостов проехать нельзя.

Избыточность в сетях с коммутацией

Сети, в которых имеется избыточность маршрутов и устройств, позволяют сети поддерживать работоспособное состояние в течение более длительного времени. Как показано на рис. 8.1, топологии с избыточностью устойчивы по отношению к отдельным точкам сбоев. Если какой-либо маршрут или устройство выходят из строя, то избыточный маршрут или устройство могут принять на себя выполнение их функций.

Если коммутатор А выходит из строя, то потоки данных по прежнему могут передаваться из сегмента 2 в сегмент 1 и далее в канал маршрутизатора через коммутатор В.

Если на порте 1 коммутатора А происходит сбой, то потоки данных могут по-прежнему пересылаться через порт 1 коммутатора В.

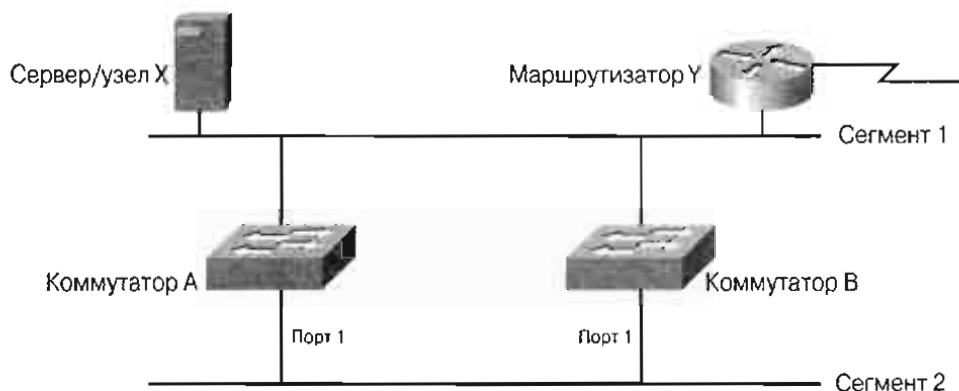


Рис. 8.1. Избыточность топологии коммутатора

Коммутаторы изучают *MAC-адреса* устройств, подсоединенных к их портам для того, чтобы соответствующим образом передать данные получателю. До тех пор, пока не стали известны все *MAC-адреса* устройств, одним из решений является отправка фреймов с неизвестным адресом получателя методом лавинной рассылки (*to flood frames*), т.е. всем устройствам, кроме того, от которого эти фреймы поступили. Широковещательные и многоадресные сообщения также рассылаются методом лавинной рассылки.

В сети, использующей коммутацию, и обладающей избыточной топологией, происходят широковещательные штормы (*broadcast storms*), многократное копирование фреймов и возникают проблемы, связанные с неустойчивостью таблиц *MAC-адресов*.

Широковещательные штормы

Широковещательные и многоадресные сообщения являются причиной потенциальных проблем в сети с коммутацией. Коммутаторы обращаются с многоадресными сообщениями как с широковещательными. Широковещательные и многоадресные сообщения рассылаются методом лавинной рассылки. В этом случае фрейм рассылается со всех портов коммутатора, за исключением того, на котором он был получен.

Как показано на рис. 8.2, если узел X посылает широковещательное сообщение, такое, например, как запрос протокола преобразования адресов (*Address Resolution Protocol — ARP*) относительно адреса 2-го уровня для маршрутизатора, то коммутатор А рассылает это сообщение со всех своих портов. Поскольку коммутатор В сам находится в этом же сегменте, то и он также получает все широковещательные сообщения. Коммутатор В получает все широковещательные сообщения, рассылаемые коммутатором А, а коммутатор А, в свою очередь, получает все широковещательные сообщения, рассылаемые коммутатором В. Коммутатор А получает эти новые широковещательные сообщения и вновь широковещательно рассылает их, как и коммутатор В. Пример такой ситуации приведен на рис. 8.2.

Таким образом, коммутаторы непрерывно рассылают одни и те же широковещательные фреймы. Такое явление называется широковещательным штормом и оно продолжается до тех пор, пока один из коммутаторов не будет отсоединен от сети. При этом коммутаторы и конечные устройства настолько заняты обработкой широковещательных сообщений, что передача данных пользователей становится маловероятной. Передача полезных данных по сети при этом либо происходит крайне медленно, либо вообще не функционирует.

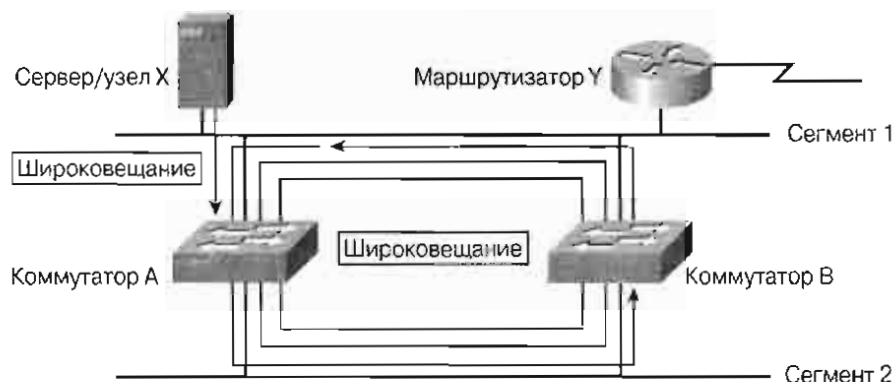


Рис. 8.2. Широковещательный шторм

Множественная передача фреймов

В сети с избыточной топологией конечное устройство может получить несколько копий одного и того же фрейма (рис. 8.3).

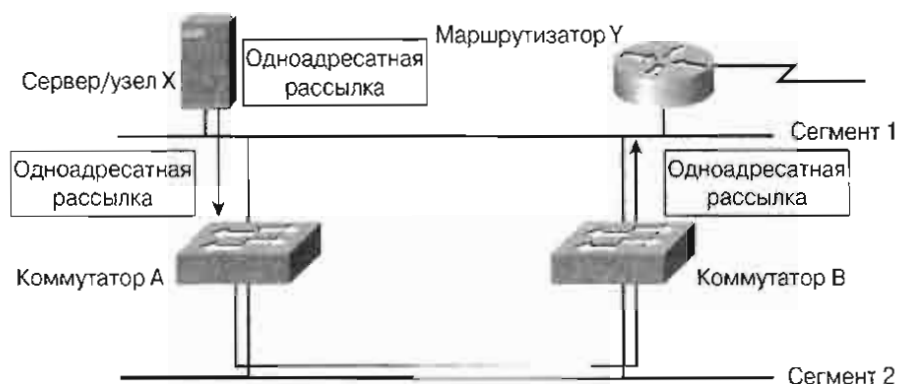


Рис. 8.3. Множественная передача фрейма

Большинство протоколов устроены таким образом, что они игнорируют множественные передачи или выдерживают их без существенного нарушения работы сети. В целом протоколы, использующие механизм последовательной нумерации, предполагают, что множественная передача закончена и нумерация в последовательности вновь начинается с нуля. Другие протоколы пытаются передать фреймы, дублирующие друг друга, соответствующему протоколу более высокого уровня, часто с непредсказуемыми результатами. Для того, чтобы понять, как возникает множественная передача, рассмотрим ситуацию, показанную на рис 8.3, в которой происходят описанные ниже действия.

- Когда узел X посылает одноадресный фрейм маршрутизатору Y, одна его копия принимается через непосредственное соединение Ethernet в сегменте 1, в то время как коммутатор A также получает его копию и помещает ее в свой буфер.
- Если коммутатор A просматривает поле адреса получателя в этом фрейме и не обнаруживает соответствующей позиции для маршрутизатора Y в своей таблице MAC-адресов, то он лавинным образом рассылает этот фрейм со всех своих портов, за исключением порта, на который этот фрейм поступил.

- Если коммутатор В получает копию этого фрейма через коммутатор А в сегменте 2 и также не находит соответствующей записи в своей таблице MAC-адресов, то он так же пересылает копию этого фрейма в сегмент 1.
- Маршрутизатор Y получает вторую копию того же самого фрейма.

Решением, позволяющим избежать появления петель и решить проблему множественной передачи одних и тех же фреймов, является логический разрыв петли и предотвращение рассылки фреймов с одного из четырех интерфейсов при нормальной работе сети.

Неустойчивость базы данных MAC-адресов

В сети, использующей коммутацию и обладающей избыточностью, коммутаторы могут получить неправильную информацию. Возможна ситуация, когда коммутатору поступает информация о том, что порту соответствует некоторый MAC-адрес, что на самом деле не соответствует действительности. Пример неустойчивости базы данных MAC-адресов показан на рис. 8.4.

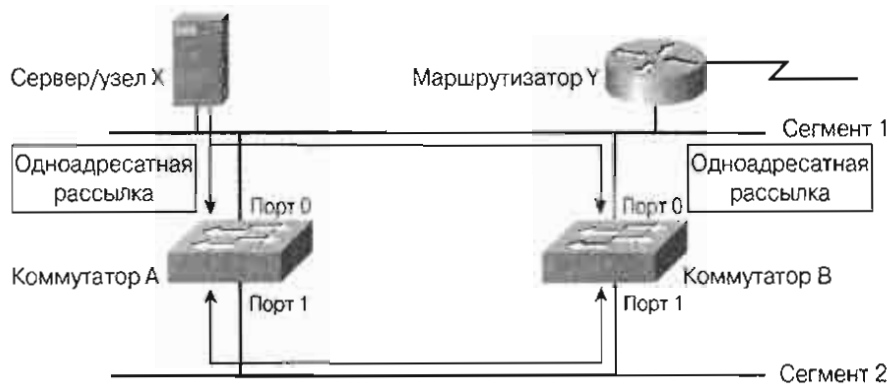


Рис. 8.4. Неустойчивость базы данных MAC-адресов

В этом примере коммутатор В устанавливает соответствие между MAC-адресом узла X и портом 0, который подсоединяется к сегменту 1 при поступлении первого фрейма. Несколько позже, когда копия этого фрейма, переданная через коммутатор А, поступает на порт 1 коммутатора В, этот коммутатор должен удалить первую запись и создать новую, в которой будет ошибочно указано, что MAC-адресу станции X соответствует порт 1, подсоединенный к сегменту 2.

В зависимости от внутренней архитектуры рассматриваемого коммутатора последний может успевать или не успевать за быстрыми изменениями базы данных MAC-адресов. В данном случае решением, позволяющим решить проблему, вызванную тем, что коммутатор не успевает за быстрыми изменениями базы данных MAC-адресов, является логический разрыв петли и предотвращение рассылки фреймов с одного из четырех интерфейсов при нормальной работе сети.

Обзор протокола связующего дерева

Протокол связующего дерева (Spanning Tree Protocol — STP) является протоколом управления каналом 2-го уровня, который используется для поддержки такого состояния сети, в котором в ней отсутствуют петли. Первоначальная версия протокола STP

была разработана корпорацией Digital Equipment (Digital). Впоследствии комитет IEEE 802 модернизировал алгоритм связующего дерева и опубликовал его в виде спецификации IEEE 802.1d. Алгоритмы корпорации Digital и комитета IEEE отличаются друг от друга и несовместимы. Коммутаторы Cisco, такие как Catalyst 1900 и 2950, используют версию протокола STP спецификации IEEE 802.1d.

Назначение протокола STP состоит в поддержке такого состояния сети, в котором в ней отсутствуют петли. Для того, чтобы сеть была свободна от петель, при ее обнаружении мост или коммутатор автоматически осуществляет логическую блокировку одного или нескольких избыточных портов.

Протокол STP постоянно проверяет сеть на предмет появления нового канала или сбоя в уже существующих; в этом случае коммутатор или мост получает информацию о таком событии. Пример работы протокола STP показан на рис. 8.5. В случае изменения топологии сети коммутаторы и мосты, на которых функционирует протокол STP, автоматически реконфигурируют свои порты для того, чтобы предотвратить потерю связи в каналах и возникновение петель.



Рис. 8.5. Протокол связующего дерева

В объединенных сетях на основе коммутаторов петли на физическом уровне могут вызвать серьезные проблемы. Широковещательные штормы, множественная передача фреймов и нестабильность баз данных MAC-адресов могут сделать такие сети неработоспособными.

Сетям на основе коммутации присущи такие преимущества, как малый размер коллизийных доменов, микросегментация и дуплексный режим работы. Проще говоря, преимуществом таких сетей является высокая производительность. Протокол STP используется в сетях с коммутацией для создания логической топологии, свободной от петель, из физической топологии, в которой петли присутствуют. Каналы, порты и коммутаторы, которые не являются элементами активной, свободной от петель топологии не участвуют в пересылке фреймов данных.

Если какой-либо элемент активной топологии выходит из строя, то необходимо определить новую свободную от петель топологию. Вычислить новую свободную от петель топологию или выполнить конвергенцию сети необходимо как можно быстрее для того, чтобы свести к минимуму время, в течение которого конечные станции не имеют доступа к сетевым ресурсам.

Для современных сетей версия протокола STP, определенная в стандарте IEEE 802.1d, осуществляет конвергенцию к новой топологии слишком медленно. Для преодоления этих ограничений был разработан новый стандарт — IEEE 802.1w или RSTP. В настоящей главе рассматривается как протокол STP, так и протокол RSTP.

Работа протокола связующего дерева

После того, как работа сети стабилизирована и в ней произошла конвергенция, каждая сеть имеет одно связующее дерево. В результате этого для каждой сети использующей коммутацию, будут выполнены следующие условия:

- В каждой сети существует один корневой мост;
- У каждого моста, который не является корневым, имеется один корневой порт;
- В каждом сегменте имеется один назначенный порт;
- Порты, которые не являются назначенными, не используются.

Для пересылки (forwarding — F) используются только корневые и назначенные порты. Порты, которые не являются назначенными, отбрасывают поступающие на них фреймы. Такие порты называются блокирующими (blocking — B) или отбрасывающими. Корневым портом моста называется порт, ближайший к корневому мосту. Для каждого некорневого моста должен быть выбран один корневой порт. На рис. 8.6 показана работа алгоритма связующего дерева.

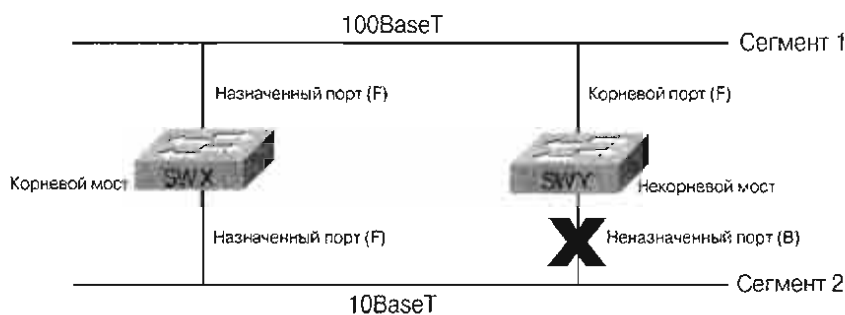


Рис. 8.6. Функционирование алгоритма связующего дерева

Сначала протокол STP осуществляет конвергенцию сети к свободной от петель логической топологии, путем выполнения описанных ниже трех этапов.

- 1. Выбор корневого моста.** В протоколе STP имеется механизм выбора корневого моста. В одной конкретной сети в качестве корневого может выступать только один мост. У корневого моста все порты являются назначенными. Назначенные порты в обычном режиме осуществляют пересылку фреймов. Когда порт находится в таком состоянии, он может получать и отправлять потоки данных. В данном примере в качестве корневого моста выбирается коммутатор X.
- 2. Выбор корневого порта на некорневых мостах.** Для каждого некорневого моста протокол STP устанавливает один корневой порт. В качестве корневого порта выбирается маршрут от некорневого моста до корневого моста с наименьшей оценкой. Корневые порты в обычном состоянии осуществляют пересылку данных. Оценка маршрута в алгоритме связующего дерева представляет собой аккумулярованную оценку, которая вычисляется на основе ширины полосы пропускания. Например, от коммутатора Y маршрутом к корневому мосту с наименьшей оценкой является маршрут через канал 100BaseT Fast Ethernet.
- 3. Выбор назначенного порта в каждом сегменте сети.** В каждом сегменте протокол STP выбирает один назначенный порт. В качестве назначенного порта выбира-

ется порт моста, который имеет наименьшую оценку маршрута к корневому мосту. Назначенные порты в обычном состоянии осуществляют пересылку данных для данного сегмента. В данном примере назначенный порт для обоих сегментов находится на корневом мосту, поскольку корневой мост непосредственно подсоединен к обоим сегментам. Порт 10BASE-T Ethernet на коммутаторе Y не является назначенным портом, поскольку для каждого сегмента имеется только один назначенный порт. Порты, которые не являются назначенными, в обычной ситуации находятся в состоянии блокировки для осуществления логического разбиения топологии, содержащей петли. Когда порт находится в состоянии блокировки, он не пересылает данные, однако может их получать.

Использование связующего дерева для создания свободной от петель топологии сети

Стевые топологии с избыточностью создаются для того, чтобы обеспечить функционирование сети в случае сбоев в отдельных точках сети. В таких случаях пользователи менее болезненно воспринимают нарушения своей работы, поскольку сеть продолжает функционировать. Любое нарушение работы сети, вызываемое сбоем, необходимо сделать как можно более кратковременным.

Избыточность повышает надежность сети. В сетях, построенных на использовании коммутаторов или мостов, наличие избыточных каналов между коммутаторами и мостами помогает преодолеть последствия сбоя на каком-либо из каналов. Эти соединения создают в сети физические петли. Пример такой ситуации приведен на рис. 8.7.

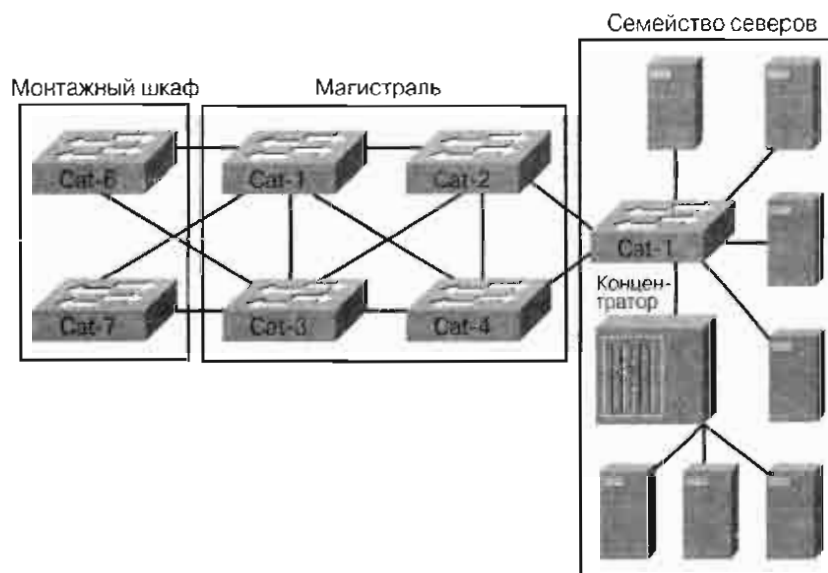


Рис. 8.7. Петли в мостовых соединениях

Петли в мостовых соединениях создаются таким образом, чтобы в случае сбоя в каком-либо из каналов его функции по пересылке данных мог выполнить другой канал. Коммутаторы функционируют на 2-м уровне эталонной модели OSI и решения о пересылке принимаются на этом уровне. Следствием этого является недопустимость существования петель в сетях с коммутацией.

В случае, когда получатель еще не известен, коммутаторы выполняют лавинную рассылку фреймов со всех своих портов. Широковещательные и многоадресные сообщения рассылаются со всех портов, кроме того, на который эти сообщения поступают (лавинная рассылка). Такие фреймы могут попасть в петлю. В заголовке 2-го уровня отсутствует поле *времени существования (time to live — TTL)*. Если фрейм посылается в сеть, топология 2-го уровня которой содержит петли, то он может попасть в такую петлю и двигаться по ней бесконечно, в результате чего напрасно затрачивается полоса пропускания и сеть становится неработоспособной.

На 3-м уровне модели OSI имеется поле времени существования пакета. При движении пакета по петле его значение последовательно уменьшается и когда оно становится равным нулю, пакет отбрасывается. Однако в этом случае возникает дилемма. Физическая топология, в которой имеются петли через коммутаторы или мосты, необходима для обеспечения надежности сети, однако сеть с коммутацией не должна иметь петель. Решением этой дилеммы является допустимость физических петель, но создание свободной от петель логической топологии.

Создаваемая при этом свободная от петель логическая топология называется деревом. Такая топология, которая является звездообразной или расширенной звездообразной логической топологией, представляет собой связующее дерево сети. Такая топология является связующим деревом, поскольку по этому дереву достижимы все устройства сети. Алгоритм, используемый для создания свободной от петель логической топологии, называется алгоритмом связующего дерева. Для конвергенции всей сети такому алгоритму требуется относительно большое время.

Расширенные функции протокола STP

Протокол STP выбирает корневой узел, называемый корневым мостом, а затем строит топологию сети, в которой к каждому сетевому узлу существует только один маршрут. Образующееся при этом дерево исходит из корневого моста. Избыточные каналы, которые не являются частью дерева кратчайших маршрутов, блокируются. Создание свободной от петель топологии становится возможным именно из-за того, что некоторые маршруты блокируются. Фреймы данных, поступающие в заблокированный канал, отбрасываются.

Протокол STP требует чтобы сетевые устройства обменивались сообщениями для обнаружения петель в мостовых соединениях. Каналы, которые вызывают появление петли, переводятся в заблокированное состояние. Сообщения, которые посылают коммутаторы для того, чтобы можно было создать свободную от петель логическую топологию, называются *модулями данных мостового протокола (bridge protocol data units — BPDU)*. Эти модули BPDU продолжают приниматься на заблокированных портах, что обеспечивает возможность построения нового связующего дерева в случае, если происходит сбой в устройстве или на активном маршруте.

Модули BPDU содержат достаточное количество информации для того чтобы коммутаторы могли выполнить описанные ниже действия.

- Выбрать один коммутатор который будет выполнять функции корня связующего дерева;
- Вычислить кратчайший путь от себя до корневого коммутатора;

- Для каждого сегмента LAN-сети назначить один из коммутаторов ближайшим к корневому коммутатору. Этот мост называется назначенным коммутатором. Назначенный коммутатор обрабатывает все данные, пересылаемые из этой LAN-сети корневому мосту.
- Каждый некорневой коммутатор выбирает один из своих портов в качестве корневого порта. Этот интерфейс обеспечивает наилучший маршрут к корневому коммутатору.
- Выбрать порты, которые являются частью связующего дерева (назначенные порты). Порты, которые не являются назначенными, блокируются.

Когда связующее дерево создает свободную от петель логическую топологию, оно всегда использует описанную ниже последовательность принятия решений, состоящую из четырех этапов.

1. Выбор наименьшего идентификатора (ID) корневого моста (bridge ID — BID);
2. Вычисление наименьшей оценки маршрута к корневому мосту.
3. Выбор наименьшего идентификатора (ID) моста-отправителя (bridge ID — BID);
4. Выбор наименьшего идентификатора (ID) порта.

Мост использует эту состоящую из четырех этапов последовательность принятия решений для того, чтобы сохранить копию “наилучшего” модуля BPDU на каждом порте. Когда мост выполняет эту оценку маршрутов, он рассматривает все модули BPDU, которые были получены на данном порте, а также BPDU, которые были бы посланы на этот порт. При поступлении каждого модуля BPDU для него выполняется описанная выше четырехэтапная проверка с целью выяснить, не является ли он более привлекательным (т.е. имеет меньшее значение оценки), чем существующий BPDU, сохраненный для этого порта. Если новый BPDU (или локально сгенерированный BPDU) более привлекательный, то он заменяет прежнее значение.

Кроме того, этот процесс “сохранения наилучшего BPDU” управляет отправкой модулей BPDU. Когда мост в первый раз становится активным, все его порты посылают модули BPDU каждые 2 секунды (если используются значения таймеров по умолчанию). Однако если порт получает от другого моста BPDU, который более привлекателен, чем BPDU, который он сам отправляет, то этот локальный порт прекращает рассылку BPDU. Если от соседнего устройства в течение определенного времени (по умолчанию 20 секунд) не поступает более привлекательного модуля BPDU, то локальный порт возобновляет рассылку.

Выбор корневого моста

При использовании протокола STP в качестве корневого выбирается мост с наименьшим значением идентификатора ID. Параметр BID включает в себя приоритет и MAC-адрес моста.

Коммутаторы и мосты, выполняющие алгоритм связующего дерева, регулярно обмениваются сообщениями о конфигурации с другими коммутаторами и мостами (по умолчанию каждые две секунды) с помощью сообщений BPDU. Частью информации, включаемой в BPDU является идентификатор BID.

Протокол STP требует, чтобы каждому мосту был назначен уникальный идентификатор (BID). Обычно этот идентификатор BID состоит из значения приоритета (два

байта) и MAC-адреса моста (шесть байтов). Приоритетом по умолчанию, в соответствии со спецификацией IEEE 802.1d, является значение 32768 (1000 0000 0000 0000 в двоичной записи или 0x8000 в шестнадцатеричной), которое является значением из среднего диапазона. На рис. 8.8. оба коммутатора имеют одно и то же значение приоритета по умолчанию, поэтому корневым станет коммутатор, который имеет меньшее значение MAC-адреса. В данном примере коммутатор X (SW X) является корневым и его ID моста равен 0x8000 (0c00.1111.1111).

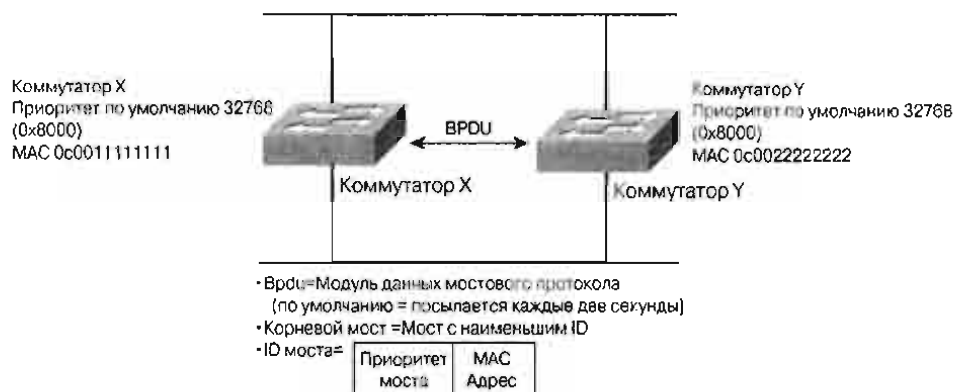


Рис. 8.8. Выбор корневого моста

ID моста, показанного на рис. 8.9, состоит из приоритета моста, который по умолчанию равен 32568, и базового MAC-адреса коммутатора.

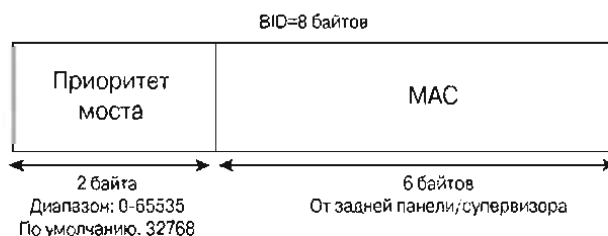


Рис. 8.9. Идентификатор ID моста

Когда коммутатор запускается впервые, он считает себя корневым и посылает минимальный BPDU. Он содержит MAC-адрес коммутатора и идентификаторы VID корневого маршрутизатора и отправителя. Все коммутаторы просматривают эти отсылаемые VID. Когда коммутатор получает BPDU, который имеет меньший корневой VID, он заменяет соответствующий VID в модулях BPDU. Все коммутаторы просматривают их и делают вывод, что мост с наименьшим значением VID будет корневым мостом.

Администратор может повлиять на это решение путем установки меньшего значения приоритета коммутатора, чем принимаемое по умолчанию. В этом случае ID моста становится меньше.

ПРИМЕЧАНИЕ

Коммутатор Catalyst Cisco использует MAC-адрес из пула MAC-адресов, назначенных либо задней панели, либо модулю супервизора, в зависимости от конкретной модели коммутатора.

Возможна ситуация, в которой сетевой администратор сочтет желательным повлиять на выбор корневого моста. Это часто происходит в том случае, когда характер передачи потоков данных по сети хорошо известен.



Лабораторная работа: выбор корневого моста

В этой лабораторной работе требуется определить, какой коммутатор выбран в качестве корневого с заводскими установками по умолчанию. После этого требуется сделать так, чтобы в качестве корневого был выбран другой коммутатор.

Последовательность состояний порта в протоколе связующего дерева

При использовании протокола STP каждый мост сети при включении питания проходит через состояние блокировки и промежуточное состояние изучения адресов и состояний других коммутаторов. Если порты соответствующим образом сконфигурированы, то происходит стабилизация и они переходят в состояние пересылки или блокировки. В состоянии пересылки порты обеспечивают маршрут к корневому мосту с наименьшей оценкой. Два промежуточных состояния имеют место в том случае, когда мост узнает об изменении в сетевой топологии. Во время изменения топологии порт временно находится в состояниях прослушивания и изучения топологии сети. На рис. 8.10 показаны состояния порта, на котором работает протокол связующего дерева.

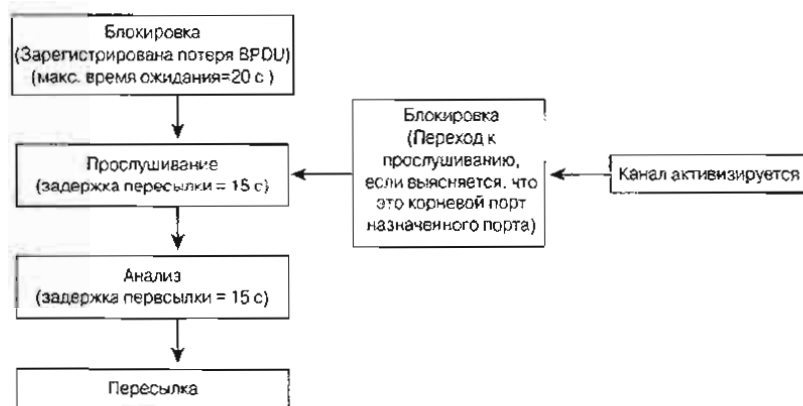


Рис. 8.10. Состояния порта, на котором функционирует протокол связующего дерева

Первоначально все порты моста находятся в состоянии блокировки, в котором они прослушивают модули BPDU. При первой загрузке моста он считает себя корневым мостом и переходит в состояние прослушивания. Отсутствие модулей BPDU в течение определенного периода времени (максимальный возраст) может вызвать переход от состояния блокировки к состоянию прослушивания. Когда порт находится в промежуточном состоянии прослушивания, он может отправлять и получать BPDU для определения текущей топологии. В этом состоянии передача данных пользователей не происходит. Именно в состоянии прослушивания мост выполняет операции по выбору корневого моста, корневых портов на некорневых мостах и выбора назначенных портов для каждого сегмента. Порты, которые остаются назна-

ченными или корневыми в течение 15 секунд (задержка пересылки), переходят в состояние изучения топологии. Порты, которые не являются назначенными или корневыми, возвращаются в состояние блокировки. При переходе порта в состояние изучения топологии он может заполнять свою таблицу MAC-адресов адресами, полученными на его портах, однако не пересылает фреймы пользователя. По умолчанию состояние изучения продолжается 15 секунд (такое время, равное задержке пересылки). В это время мост все еще не передает данных пользователя.

Ниже приводятся состояния протокола STP.

- **Состояние блокировки.** Фреймы пользователей не пересылаются, прослушиваются модули BPDU.
- **Состояние прослушивания.** Фреймы пользователей не пересылаются, но прослушиваются.
- **Состояние изучения топологии.** Фреймы пользователей не пересылаются, изучаются адреса других устройств.
- **Состояние пересылки.** Пересылаются фреймы пользователей и изучаются адреса других устройств.
- **Состояние отключения.** Фреймы пользователей не пересылаются, модули BPDU не прослушиваются.

В состоянии изучения топологии уменьшается объем лавинной рассылки, которая требуется в начале пересылки. Если какой-либо порт по-прежнему является назначенным или корневым портом в заключительной фазе состояния изучения топологии, то он переходит в состояние пересылки. Порты, которые не являются назначенными или корневыми, возвращаются в состояние блокировки. В состоянии пересылки порт может отправлять и получать данные пользователей.

Обычно время, требуемое порту для перехода из состояния блокировки в состояние пересылки, составляет от 30 до 50 секунд. Это время таймеров протокола связующего дерева может быть изменено сетевым администратором. Обычно эти периоды таймеров устанавливаются со стандартным значением. Значения по умолчанию устанавливаются для того, чтобы у сети была возможность собрать правильную информацию о сетевой топологии.

Время, требуемое порту для перехода из состояния прослушивания в состояние изучения или из состояния изучения топологии в состояние пересылки, называется задержкой пересылки и по умолчанию составляет 15 секунд. Максимальный возраст, который по умолчанию равен 20 секундам, равен времени хранения мостом модуля BPDU перед его отбрасыванием. Если порт находится в состоянии блокировки и не получает новых модулей BPDU за время максимального возраста, то он переходит из состояния блокировки в состояние прослушивания.

Если порт коммутатора подсоединен только к станциям конечных пользователей (не имеет соединений с другими коммутаторами или мостами), то на таких портах конечных пользователей следует включить функцию коммутатора Catalyst, называемую *“быстрым портом”* (*portfast*). При включенной функции быстрого порта в момент активизации порта он автоматически переходит из состояния блокировки в состояние пересылки. Это становится возможным потому, что в этом случае через эти порты не могут возникнуть петли, поскольку к ним не подсоединены другие коммутаторы или мосты. На рис. 8.11 приведен пример сети, порты которой находятся в различных состояниях.



Рис. 8.11. Пример сети с различными состояниями портов

Выбор назначенных портов

В сети, использующей коммутацию, каждый сегмент имеет один назначенный порт. Этот порт функционирует как единственный порт моста, который получает и отправляет все данные, поступающие в сегмент и отправляемые из него. Такой подход основывается на том, что если только один порт обрабатывает данные для всех каналов, то все петли оказываются разорванными. Мост, которому принадлежит назначенный порт данного сегмента называется *назначенным мостом* (*designated bridge*) этого сегмента. После окончания конкуренции за право быть корневым коммутатором все коммутаторы переключаются на выбор корневых портов. Корневым портом моста называется порт, ближайший к корневому мосту. Каждый некорневой мост должен выбрать один корневой порт. Для этого мосты вновь используют оценку в качестве меры близости к корневому коммутатору. В частности, мосты определяют величину, называемую оценкой корневого маршрута, которая является кумулятивной (суммарной) оценкой всех каналов, ведущих к корневому мосту. На рис. 8.12 приведен пример выбора корневых портов и показано, как вычисляется оценка при прохождении через несколько мостов и проиллюстрирован процесс окончательного выбора корневого порта.

Когда корневой мост Cat-A посылает модули BPDU, эти модули содержат оценку корневого маршрута, равную нулю (этап 1). Когда мост Cat-B получает эти модули BPDU, он добавляет оценку маршрута порта 1/1 к оценке корневого маршрута, которая содержится в полученном BPDU. Предположим, что в сети функционирует протокол Fast Ethernet. Коммутатор Cat-B получает оценку корневого маршрута, равную 0 и добавляет к оценке порта 1/1 значение, равное 19. После этого коммутатор Cat-B использует значение 19 для внутренних расчетов и посылает модули BPDU с оценкой корневого маршрута, равной 19, с порта 1/2 (этап 3).

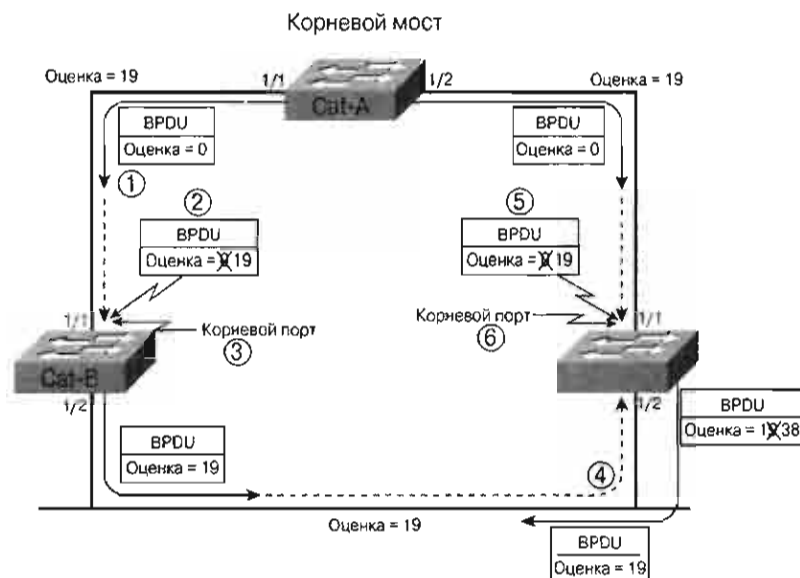


Рис. 8.12. Выбор корневых портов

Когда коммутатор Cat-C получает эти модули BPDU от коммутатора Cat-B (4-й этап), он увеличивает оценку корневого маршрута до 38 ($19 + 19$). Однако коммутатор Cat-C получает также модули BPDU от корневого моста на порте Port 1/1. Эти BPDU поступают на порт Port 1/1 коммутатора Cat-C с оценкой 0 и коммутатор Cat-C увеличивает внутреннюю оценку до 19 (этап 5). Теперь коммутатору Cat-C необходимо принять решение о выборе одного корневого порта — порта, ближайшего к корневому мосту. Коммутатор Cat-C имеет оценку корневого маршрута равную 19 на порте Port 1/1 и оценку 38 на порте Port 1/2. Следовательно, порт Port 1/1 коммутатора Cat-C становится корневым портом (этап 6). После этого коммутатор Cat-C начинает анонсировать оценку корневого маршрута, равную 19 коммутаторам, расположенным в нисходящем направлении (этап 7).

Хотя подробное описание этого процесса для коммутатора Cat-B на рис. 8.13 не приводится, в нем происходят аналогичные вычисления.

С порта Port 1/1 коммутатора Cat-B можно достичь корневой мост с оценкой 19, в то время как вычисления для порта Port 1/2 коммутатора Cat-B дают значение оценки, равное 38. Следовательно, порт Port 1/1 становится корневым портом коммутатора Cat-B. Следует обратить внимание на то, что при поступлении модулей BPDU на порт оценки увеличиваются.

Следует помнить о том, что оценки протокола STP увеличиваются при поступлении модулей BPDU на порт, а не при рассылке их с порта. Например, модули BPDU поступают на порт Port 1/1 коммутатора Cat-B с оценкой, равной 0 и эта оценка увеличивается до 19 “внутри” коммутатора Cat-B.

Действия протокола STP по предотвращению петель становятся наглядными на третьем этапе первоначальной конвергенции протокола STP при выборе назначенных портов. Каждый сегмент в сети с мостовыми соединениями имеет один назначенный порт. Этот порт функционирует как единственный порт моста, который осуществляет как отправку, так и получение данных для данного сегмента и корневого моста. В основе такого подхода лежит положение о том, что если для каждого

канала обработку данных выполняет только один порт, то все петли в сети разорваны. Мост, которому принадлежит назначенный порт для данного сегмента, называется *назначенным мостом (designated bridge)* данного сегмента.

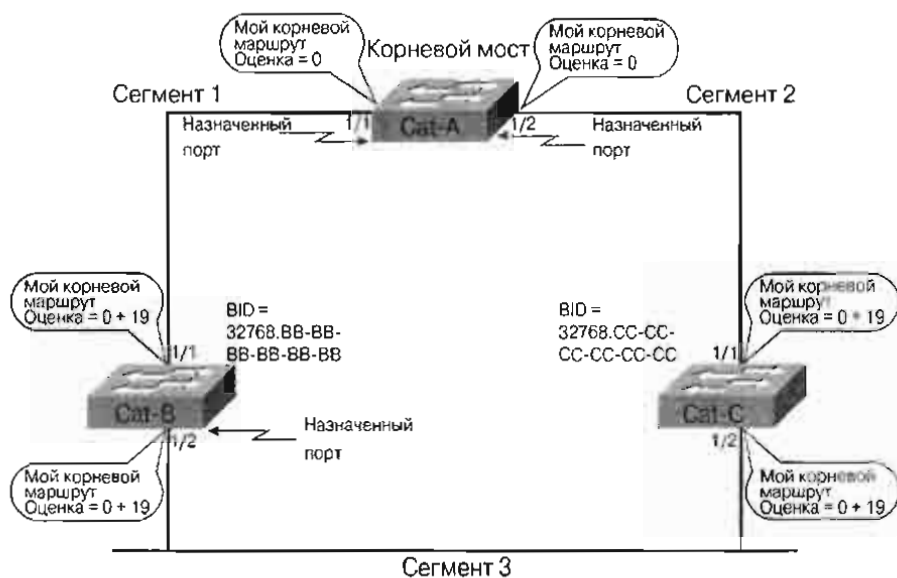


Рис. 8.13. Выбор назначенных портов

Как и при выборе корневого порта, назначенные порты выбираются на основе кумулятивной оценки корневого маршрута к корневому мосту, как показано на рис. 8.13. На рис. 8.13 рассмотрим назначенные порты и каждый сегмент по очереди. Сначала рассмотрим сегмент 1, который является каналом между коммутаторами Cat-A и Cat-B. В этом сегменте имеется два порта мостов: порт Port 1/1 коммутатора Cat-A и порт Port 1/1 коммутатора Cat-B. Порт Port 1/1 коммутатора Cat-A имеет оценку корневого маршрута равную 0 (все-таки это корневой мост), а порт Port 1/1 коммутатора Cat-B имеет оценку корневого маршрута равную 19 (значение 0 получено в модулях BPDU от коммутатора Cat-A плюс оценка маршрута, равная 19, назначенная порту Port 1/1 коммутатора Cat-B). Поскольку порт Port 1/1 коммутатора Cat-A имеет меньшую оценку корневого маршрута, он становится назначенным портом канала.

Для сегмента 2 (канал от коммутатора Cat-A к коммутатору Cat-C) имеет место аналогичная операция выбора. Порт Port 1/2 коммутатора Cat-A имеет оценку корневого маршрута, равную 0, в то время как порт Port 1/1 коммутатора Cat-C имеет оценку корневого маршрута, равную 19. Порт Port 1/2 коммутатора Cat-A имеет меньшую оценку и становится назначенным портом. Следует отметить, что каждый активный порт на корневом мосту становится назначенным портом. Единственным исключением из этого правила является физическая петля на 1-м уровне к корневому мосту. Примером является ситуация, в которой два порта корневого моста подсоединены к одному и тому же концентратору или когда два порта соединены перекрученным кабелем.

Теперь рассмотрим сегмент 3 (канал от коммутатора Cat-B к коммутатору Cat-C): как порт Port 1/2 коммутатора Cat-B, так и порт Port 1/2 коммутатора Cat-C имеют оценку корневого маршрута равную 19. В этом случае имеет место равенство оценок. Если протокол STP сталкивается с ситуацией равенства оценок, то при принятии

решения он использует четырехэтапную последовательность, обсуждавшуюся ранее в разделе “Протокол связующего дерева”. Напомним, что эти четыре этапа включают в себя:

- Выбор наименьшего корневого идентификатора BID
- Вычисление наименьшей оценки маршрута к корневому мосту
- Выбор наименьшего идентификатора BID отправителя
- Выбор наименьшего идентификатора ID порта.

В примере, показанном на рис. 8.13, все три моста соглашаются с тем, что коммутатор Cat-A является корневым мостом, что требует дать оценку корневому маршруту. Однако, как было показано выше, оба коммутатора — Cat-B и Cat-C имеют одинаковые оценки, равные 19. В этом случае решающим становится третий критерий — значение идентификатора BID. Поскольку идентификатор BID коммутатора Cat-B (32768.BB-BB-BBBB-BB-BB) меньше чем идентификатор BID коммутатора Cat-C (32768.CC-CC-CC-CC-CC-CC), порт Port 1/2 коммутатора Cat-B становится назначенным портом сегмента 3. Соответственно, Port 1/2 коммутатора Cat-C становится неназначенным портом.

Оценка маршрута

Оценка маршрута в протоколе связующего дерева представляет собой накопленную общую оценку маршрута, вычисленную на основе полосы пропускания всех каналов на маршруте. В табл. 8.1 приведены оценки маршрутов, определенные в спецификации IEEE 802.1D для различных сетевых технологий, таких как Token Ring, Ethernet и SONET. Мосты используют понятие оценки для выяснения степени своей близости к другим мостам. Стандарт 802.1D, первоначально определял оценку как частное от деления величины 1000 Мбит/с на полосу пропускания канала, выраженную в Мбит/с. С появлением технологии 10 Gigabit Ethernet применение этой формулы стало невозможным. В табл. 8.2 приведены использовавшиеся ранее оценки каналов для различных Ethernet-технологий и те, которые используются в настоящее время.

Таблица 8.1. Оценки маршрутов для различных сетевых технологий

Полоса пропускания	Оценка в протоколе STP
4 Мбит/с	250
10 Мбит/с	100
16 Мбит/с	62
45 Мбит/с	39
100 Мбит/с	19
155 Мбит/с	14
622 Мбит/с	6
1 Гбит/с	4
10 Гбит/с	2

Таблица 8.2. Пересмотренные оценки каналов для сетей Ethernet

Скорость канала	Оценка (Пересмотренная спецификация IEEE)	Оценка (Предыдущая спецификация IEEE)
10 Гбит/с	2	1
1 Гбит/с	4	1
100 Мбит/с	19	10
10 Мбит/с	100	100

Из таблицы видно, как мосты используют оценку маршрута для определения своей близости к другим мостам. Например, канал 10BASE-T имеет оценку 100 (1000/10), а каналы Fast Ethernet и Fiber Distributed Data Interface (FDDI) имеют оценку, равную 10 (1000/100). Этой схемой пользовался весь мир с того момента, когда Радия Перлман (Radia Perlman) начал работу над протоколом STP в 1983 году. Однако с появлением технологий Gigabit Ethernet и OC-48 ATM (2.4 Гбит/с) возникла проблема. Например, для OC-48 ATM вычисление оценки по этой формуле дает значение $1000 \text{ Мбит/с} / 2400 \text{ Мбит/с} = 0,41667$. Значение 0.41667 недействительно, поскольку его придется округлить до 1, как и для любой другой технологии с полосой пропускания 1 Гбит/с или более. Единственным выходом из этой ситуации является присвоение оценки 1 всем каналам с полосой пропускания большей или равной 1 Гбит/с. Однако в этом случае протокол STP не сможет выбирать оптимальный маршрут в гигабитных сетях. Для решения этой проблемы IEEE принял решение изменить способ вычисления оценки и использовать нелинейную шкалу.

Таймеры протокола STP

Время приветствия определяет временной интервал между регулярными рассылками модулей конфигурации BPDU. Стандарт 802.1D определяет стандартное значение этого интервала, равное 2 секундам. Однако это значение управляет только модулями конфигурации BPDU, которые генерируются корневым мостом. Остальные мосты распространяют модули BPDU по мере их получения. Иными словами, если в течение 2-20 секунд модули BPDU перестают поступать, то некорневые мосты прекращают рассылать регулярные BPDU. Если этот простой длится более 20 секунд, что является максимальным значением возраста по умолчанию, то мост делает недействительными сохраненные модули BPDU и начинает искать новый корневой порт. Максимальным возрастом считается время, в течение которого мост хранит BPDU перед их отбрасыванием.

Под задержкой пересылки понимается одно значение, которое определяет оба этих состояния. Первоначально в качестве значения по умолчанию принималось значение 15 секунд, которое определялось предположением, что максимальный размер сети определяется семью переходами, максимальное количество утерянных BPDU равно трем, а интервал приветствия равен двум секундам. Таймер задержки при пересылке также управляет периодом старения адресной таблицы моста после изменения активной сетевой топологии.

Раньше говорилось о том, что каждый порт сохраняет копию наилучшего BPDU, который он получал и просматривал. До тех пор, пока мост каждые 2 секунды получает модули BPDU, получающий их мост поддерживает постоянные копии значений

этих модулей. Однако если в устройстве, рассылающем эти модули BPDU с наилучшими маршрутами, происходит сбой, то должен заработать механизм, который позволит другим мостам выполнить функции этого вышедшего из строя устройства. В таблице 8.3 приведены некоторые значения таймеров протокола STP.

Таблица 8.3. Таймеры протокола STP

Таймер	Назначение	Значение по умолчанию
Время приветствия (Hello Time)	Промежуток времени между регулярными рассылками модулей BPDU корневым мостом	2 секунды
Задержка пересылки	Продолжительность состояний прослушивания и изучения топологии	15 секунд
Максимальный возраст (Max Age)	Время хранения модулей BPDU	20 секунд

В некоторых ситуациях коммутаторы могут обнаружить изменения топологии на непосредственно подсоединенных каналах и сразу перейти в состояние прослушивания, не ожидая истечения максимального возраста.

Например, предположим, что канал 3-го сегмента на рис. 8.14 использует концентратор и трансивер порта Port 1/2 коммутатора Cat-B вышел из строя. Коммутатор Cat-C не получает немедленного уведомления об этом сбое, поскольку он по-прежнему получает “канал” Ethernet от концентратора. Единственное, что знает коммутатор Cat-C, это то, что модули BPDU продолжают поступать. Через двадцать секунд после сбоя (время максимального возраста) порт 1/2 коммутатора Cat-C принимает решение считать устаревшей информацию модуля BPDU о том, что коммутатор Cat-B имеет наилучший назначенный порт в 3-м сегменте. Это вынуждает порт Port 1/2 коммутатора Cat-C перейти в состояние прослушивания в попытке стать назначенным портом. Поскольку порт Port 1/2 коммутатора Cat-C теперь предлагает наиболее привлекательный доступ от корневого моста к этому каналу, он в конечном итоге переходит в режим пересылки. На практике процесс перехода функций назначенного моста к коммутатору Cat-C занимает около 50 секунд (20 секунд [максимальный возраст] + 15 секунд режима прослушивания + 15 секунд режима изучения топологии).

В некоторых ситуациях коммутаторы могут обнаружить изменения топологии на непосредственно подсоединенных каналах и сразу перейти в состояние прослушивания, не ожидая истечения максимального возраста. Например, рассмотрим сеть, показанную на рис. 8.15.

В этом примере происходит сбой на порте Port 1/1 коммутатора Cat-C. Поскольку этот сбой происходит на канале к корневому порту, нет необходимости ожидать 20 секунд для того, чтобы считать прежнюю информацию устаревшей.

Вместо этого порт Port 1/2 коммутатора Cat-C немедленно переходит в состояние изучения топологии, пытаясь стать новым корневым портом. В результате этого процесс конвергенции протокола STP сокращается с 50 секунд до 30 секунд.

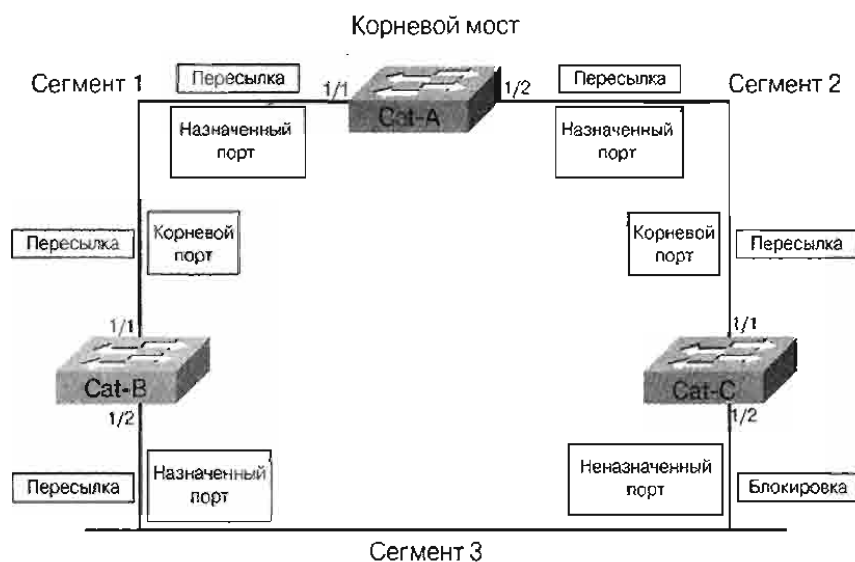


Рис. 8.14. Пример сети с идентифицированными состояниями портов

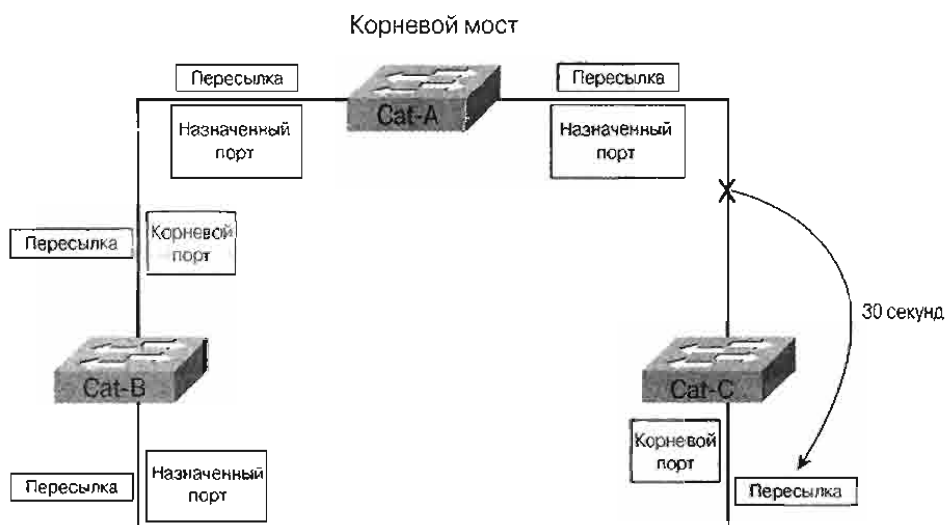


Рис. 8.15. Пример сети с идентифицированными состояниями портов

Следует помнить о двух ключевых моментах, касающихся использования таймеров протокола STP. Во-первых, не следует изменять значения таймеров, принимаемые по умолчанию, без тщательного анализа. При попытке максимизировать установки таймера следует изменять только значения таймеров на корневом мосту, поскольку модули BPDU содержат три поля, в которых значения таймеров могут быть переданы с корневого моста на все остальные мосты сети. Рассмотрим альтернативный вариант действий: если с конфигурировать каждый мост локально, то некоторые мосты пройдут последовательность состояний до состояния пересылки раньше, чем другие выйдут из состояния прослушивания. Такой хаотичный подход может быстро привести к нестабильности сети. Предоставляя поля значений таймеров в модулях BPDU, один мост, выступающий в качестве корневого, сможет диктовать параметры таймеров всем коммутаторам сети.

Перерасчет связующего дерева

Если в топологии сети происходят изменения, то протокол STP поддерживает соединения в сети путем перевода некоторых заблокированных портов в состояние пересылки. Если изменение топологии вызвано сбоем моста или канала, то связующее дерево перенастраивает топологию сети для обеспечения соединений путем перевода заблокированных портов в состояние пересылки.

В сети, показанной на рис. 8.16, в случае, когда коммутатор Switch X (корневой мост) выходит из строя и не посылает коммутатору Switch Y модулей BPDU в течение времени максимального возраста (по умолчанию в течение 20 секунд, что равно 10 пропущенным рассылкам модулей BPDU), коммутатор Switch Y обнаруживает отсутствие BPDU от корневого моста. В момент, когда истекает время таймера максимального возраста на коммутаторе Switch Y, а новый BPDU от коммутатора Switch X не поступил, начинается перерасчет связующего дерева. Коммутатор Switch Y переводит свой заблокированный порт (порт 1) из состояния блокировки в состояние прослушивания, а затем в состояние пересылки.



Рис. 8.16. Перерасчет связующего дерева

Примерно через 50 секунд после конвергенции сети коммутатор Switch Y становится корневым мостом и начинает пересылать данные между двумя сегментами.



Лабораторная работа: пересчет связующего дерева

В этой лабораторной работе можно увидеть, как работает алгоритм связующего дерева в случае изменений топологии в сети, использующей коммутацию.

Конвергенция сети

Конвергенция сети необходима для нормальной работы сети. Для сети, в которой используются коммутаторы или мосты, ключевым вопросом является время, которое требуется для конвергенции сети в случае изменения ее топологии. В протоколе STP под конвергенцией понимается состояние сети, в котором все порты коммутаторов и мостов перешли либо в состояние пересылки, либо в состояние блокировки.

Быстрая конвергенция является желательной, поскольку в этом случае уменьшается время нахождения портов коммутаторов и мостов в переходных состояниях, когда они не осуществляют пересылки пакетов. Обычно конвергенция занимает от 30 до 50 секунд.

Протокол RSTP

Протокол (*RSTP*) предназначен для того, чтобы значительно ускорить перерасчет связующего дерева в случае изменений в сетевой топологии. В протоколе RSTP определяются дополнительные роли портов: альтернативного и резервного и состояния портов: отбрасывания, изучения топологии и пересылки.

Протокол RSTP (спецификация IEEE 802.1w) значительно сокращает время конвергенции активной топологии сети в случае изменений физической топологии или изменения параметров конфигурации. Протокол RSTP выбирает один коммутатор в качестве корня связанной со связующим деревом активной топологии и назначает роли отдельным портам коммутатора в зависимости от того, являются ли они частью активной топологии.

Протокол RSTP обеспечивает быстрое восстановление соединений в случае сбоя на коммутаторе, порте коммутатора или в локальной сети LAN. Новый корневой порт и назначенный порт на другой стороне моста переходят в состояние пересылки путем явного квитирования (обмена сообщениями) между ними. Протокол RSTP позволяет сконфигурировать порты коммутатора таким образом, чтобы они могли перейти в состояние пересылки сразу после повторной инициализации коммутатора. Протокол RSTP, описанный в спецификации IEEE 802.1w, замещает протокол STP описанный в 802.1d, оставаясь совместимым с ним.

Для того, чтобы стало возможным использование функций протокола RSTP, необходимо, чтобы на коммутаторе была установлена новая версия образа программного обеспечения (enhanced software image — EI).

Четыре роли коммутатора в протоколе RSTP определяются как описано ниже.

- **Root (корневой)** Пересылающий порт, выбранный для топологии связующего дерева;
- **Designated (назначенный)**—пересылающий порт, выбираемый для каждого сегмента коммутируемой LAN-сети;
- **Alternate (альтернативный)**—Альтернативный маршрут к корневому мосту.
- **Backup (резервный)**—Резервный маршрут по отношению к тому, который обеспечивается назначенным портом и ведет к листьям связующего дерева. Резервные порты могут существовать только в том случае, когда два порта образуют петлю посредством канала типа “точка-точка” или с помощью моста, имеющего два или более соединения с общим сегментом LAN-сети.
- **Disabled (отключенный)** —порт, не участвующий в работе протокола связующего дерева.

Роль корневого порта или назначенного порта включает в себя порт в активной топологии. В роли альтернативного или резервного порт исключается из активной топологии сети.

Состояния портов в протоколе RSTP

Состояние порта управляет процессами пересылки и изучения топологии, а также предоставляет значения для отбрасывания, изучения топологии и пересылки. В табл. 8.4 сравниваются состояния портов в протоколе STP с состояниями портов в протоколе RSTP.

Таблица 8.4 Сравнение состояний портов в протоколе STP с состояниями портов в протоколе RSTP

Операционное состояние	Состояние порта в протоколе STP	Состояние порта в протоколе RSTP	Включен в активную топологию?
Включен	Блокировка	Отбрасывание	Нет
Включен	Прослушивание	Отбрасывание	Нет
Включен	Изучение топологии	Изучение топологии	Да
Включен	Пересылка	Пересылка	Да
Отключен	Блокирован	Отбрасывание	Нет

В условиях стабильной топологии протокол RSTP обеспечивает, переход каждого корневого порта и назначенного порта в состояние пересылки, в то время как все альтернативные порты и резервные порты постоянно находятся в состоянии отбрасывания.

Переход в состояние пересылки

Быстрый переход в состояние пересылки является наиболее важной функцией, введенной в спецификации IEEE 802.1w. До введения 802.1w алгоритм связующего дерева пассивно ожидал, пока произойдет конвергенция сети перед переходом порта в состояние пересылки. В новом протоколе RSTP активно подтверждается, что порт может безопасно перейти в состояние пересылки не полагаясь на конфигурацию таймера. Для достижения быстрой конвергенции на порте протокол использует две новых переменных — краевого (граничного) порта и типа канала.

Краевыми называются порты, непосредственно подсоединенные к конечным станциям. Они не могут создавать в сети петель, следовательно, они могут перейти непосредственно в состояние пересылки, минуя состояния прослушивания и изучения топологии. Краевой порт не создает изменений в топологии сети если он включается или выключается.

Протокол RSTP может обеспечить быстрый переход к состоянию пересылки только на краевых портах и на каналах типа “точка-точка”. В современных сетях с коммутацией это не является существенным ограничением. Тип канала автоматически определяется дуплексным режимом порта. Порт, работающий в дуплексном режиме, является каналом типа “точка-точка”, в то время как порт, функционирующий в полудуплексном режиме, по умолчанию рассматривается как совместно используемый. Эту автоматическую установку типа порта можно изменить явным ручным конфигурированием. На рис. 8.17 приведен пример быстрого перехода к состоянию пересылки.

Протокол RSTP (спецификация IEEE 802.1w) в конечном итоге, вероятно, заменит протокол STP (IEEE 802.1d).

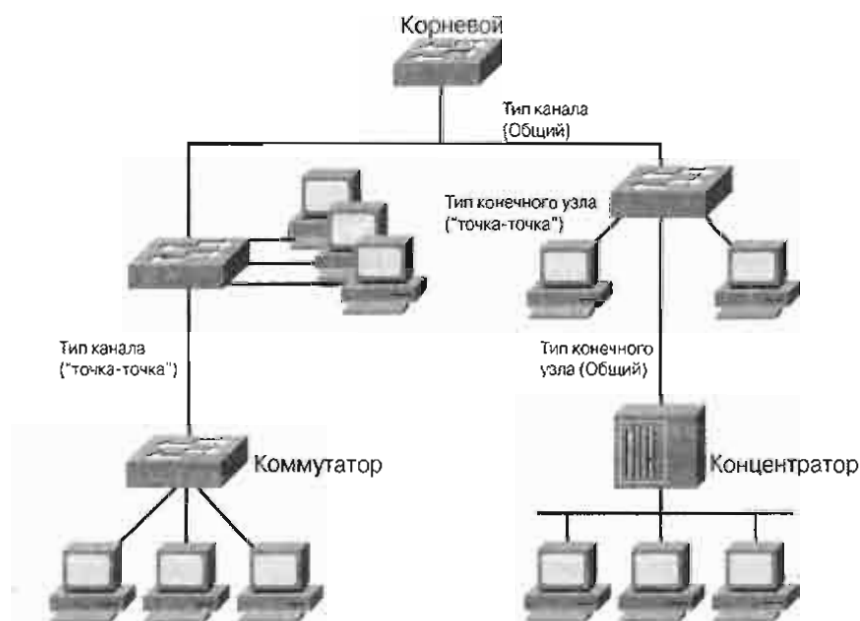


Рис. 8.17. Быстрый переход к состоянию пересылки

Резюме

В настоящей главе были рассмотрены следующие аспекты функционирования протокола STP.

- Избыточность топологии и коммутируемые сети с избыточной топологией, широковещательные штормы, множественная передача фреймов и нестабильность базы данных MAC-адресов.
- Топологии с избыточностью обеспечивают более надежные и устойчивые к отказам сети.
- Протокол STP и алгоритм связующего дерева обеспечивают свободную от петель логическую топологию в физической топологии, имеющей петли.
- Обсуждены важные для работы протокола STP понятия, такие как функционирование связующего дерева, структура связующего дерева, выбор корневого моста, последовательность состояний портов связующего дерева, выбор назначенных портов, оценка маршрута, таймеры протокола STP, перерасчет связующего дерева и конвергенция сети.
- Обсуждены вопросы, связанные с протоколом RSTP, состояния портов протокола RSTP и переход к состоянию пересылки.

В дополнение к материалу, изложенному в настоящей главе, рекомендуется ознакомиться с лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

Быстрый порт (portfast). Команда, переводящая порт протокола связующего дерева в состояние пересылки минуя состояния прослушивания и изучения топологии.

Быстрый протокол связующего дерева (Rapid Spanning Tree Protocol — RSTP). Протокол RSTP определяет дополнительные роли порта и определяет состояния порта: отбрасывание, изучение топологии и пересылка.

Время существования (time to live — TTL). Поле протокола IP, задающее количество переходов, которое может пройти пакет до того, как он будет отброшен или возвращен в обратном направлении.

Идентификатор моста (bridge ID — BID). Номер, который используется мостом или коммутаторами для идентификации приоритета и выбора корневого моста или коммутатора. Корневым становится мост, имеющий наименьшее значение идентификатора BID.

Модуль данных мостового протокола (bridge protocol data unit — BPDU). Пакет приветствия протокола связующего дерева (Spanning Tree Protocol) который регулярно рассылается (с конфигурируемым интервалом) для обмена информацией между мостами.

Назначенный мост (designated bridge) Мост, который имеет наименьшую оценку маршрута при отправке фрейма из сегмента на корневой мост.

Подуровень управления доступом к среде передачи (Media Access Control — MAC). Нижний из двух подуровней канального уровня, определенного организацией IEEE. MAC-подуровень управляет доступом к совместно используемой среде, например, в сетях с передачей маркера или конкурентным доступом к среде.

Протокол преобразования адресов ARP (Address Resolution Protocol — ARP). Internet-протокол, используемый для преобразования IP-адресов в MAC-адреса.

Протокол связующего дерева (Spanning Tree Protocol — STP). Протокол управления каналом 2-го уровня, используемый для поддержки в сети состояния, свободного от петель. Протокол STP постоянно анализирует состояние сети для того, чтобы в случае отказа или добавления канала, коммутатора или моста предпринять соответствующие действия.

Контрольные вопросы

1. Цель избыточной топологии состоит в устранении простоев в сети в случае когда в ней имеется _____ точек сбоя.
 - A. Одна
 - B. Две
 - C. Три
 - D. Четыре
2. Каково назначение протокола связующего дерева?
 - A. Поддержка маршрутов с одной петлей
 - B. Поддержка сети в состоянии свободном от петель
 - C. Поддержка сети в состоянии с несколькими петлями
 - D. Поддержка сети в состоянии с уменьшенным количеством петель
3. При изменении топологии сети _____
 - A. Необходимо инициировать повторное вычисление связующего дерева
 - B. Необходимо заново с конфигурировать верхний узел связующего дерева

- C. Необходимо заново сконфигурировать все устройства, принимающие участие в работе протокола связующего дерева
 - D. Протокол связующего дерева (Spanning Tree Protocol) реконфигурирует порты коммутатора или моста автоматически
4. У корневого моста все порты являются ____
- A. Корневыми портами
 - B. Заблокированными портами
 - C. Назначенными портами
 - D. Неназначенными портами
5. Как протокол связующего дерева выбирает корневой порт на мосту не являющемся корневым?
- A. Корневым портом становится порт с максимальной оценкой маршрута от некорневого моста к корневому мосту.
 - B. Корневым портом становится порт с наименьшей оценкой маршрута от некорневого моста к корневому мосту.
 - C. Корневым портом становится порт с минимальной оценкой маршрута от некорневого моста к резервному корневому мосту.
 - D. Корневым портом становится порт с максимальной оценкой маршрута от некорневого моста к резервному корневому мосту.
6. Какой мост выбирает протокол связующего дерева в качестве корневого?
- A. Мост, имеющий наименьший приоритет
 - B. Мост, имеющий наименьший идентификатор ID
 - C. Мост, имеющий максимальный идентификатор ID
 - D. Мост, имеющий максимальный MAC-адрес
7. Из чего состоит идентификатор BID протокола связующего дерева (Spanning Tree Protocol)?
- A. Из приоритета моста и его IP-адреса
 - B. Из приоритета моста и его MAC-адреса
 - C. Из MAC-адреса моста и его IP-адреса
 - D. Из MAC-адреса моста и номера порта Ethernet
8. В каком состоянии порт может заполнять свою таблицу MAC-адресов, но не пересылает фреймы пользователей?
- A. В состоянии изучения топологии
 - B. В состоянии блокировки
 - C. В состоянии прослушивания
 - D. В состоянии пересылки
9. Чему равна оценка канала 100 Мбит/с в пересмотренной спецификации IEEE?
- A. 4
 - B. 10
 - C. 19
 - D. 100

10. Что называется конвергенцией в протоколе связующего дерева?
 - A. Состояние сети, в котором все порты перешли в состояние блокировки.
 - B. Состояние сети, в котором все порты перешли в состояние пересылки.
 - C. Состояние сети, в котором все порты перешли в состояние прослушивания или в состояние пересылки.
 - D. Состояние сети, в котором все порты перешли в состояние пересылки или в состояние блокировки.
11. Чему равен по умолчанию максимальный возраст в протоколе связующего дерева?
 - A. 2 секунды
 - B. 15 секунд
 - C. 20 секунд
 - D. 30 секунд
12. Какое состояние быстрого протокола связующего дерева (Rapid Spanning Tree Protocol) эквивалентно состоянию блокировки протокола связующего дерева (Spanning Tree Protocol)?
 - A. Состояние блокировки
 - B. Состояние отбрасывания (dropping)
 - C. Состояние игнорирования (discarding)
 - D. Состояние пересылки
13. Какая роль порта характеризует пересылающий порт, выбираемый для каждого сегмента использующей коммутацию LAN-сети, при использовании протокола быстрого связующего дерева (Rapid Spanning Tree Protocol)?
 - A. Корневой порт
 - B. Резервный порт
 - C. Альтернативный порт
 - D. Назначенный порт
14. Каким образом протокол STP обеспечивает отсутствие петель в сети?
 - A. Путем перевода всех портов в состояние блокировки
 - B. Путем перевода всех мостов в состояние блокировки
 - C. Путем перевода некоторых портов в состояние блокировки
 - D. Путем перевода некоторых мостов в состояние блокировки



В этой главе...

- Дано определение виртуальной локальной сети
- Описаны причины создания сетей VLAN и описаны их преимущества
- Описаны способы реализации сетей VLAN
- Описано создание, тестирование и удаление конфигураций VLAN-сетей
- Описаны основные методы устранения ошибок в сетях VLAN

Виртуальные локальные сети

В настоящей главе приводятся начальные сведения о виртуальных локальных сетях (Virtual Local-Area Networks — VLAN) и описываются преимущества использования коммутируемой архитектуры VLAN. В ней также приведены основные понятия, используемые для описания работы VLAN-сетей и рассмотрены основные операции. Кроме того, в этой главе приведены инструкции по созданию, тестированию и удалению VLAN-сетей. В заключение описаны способы устранения ошибок, которые можно использовать для их нахождения и разрешения проблем, возникающих при реализации сетей VLAN.

Рекомендуется также выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Начальные сведения о сетях VLAN

Одной из важных функций, реализуемых в технологии Ethernet, являются *виртуальные локальные сети VLAN*, в которых для объединения рабочих станций и серверов в логические группы используются коммутаторы. Связь устройств, принадлежащих к одной VLAN-сети, возможна только с устройствами этой же сети, поэтому сеть с коммутацией функционирует как несколько индивидуальных, не соединенных друг с другом локальных сетей LAN. Трудно дать общее строгое определение сетей VLAN, поскольку разные производители используют различные подходы к созданию таких сетей.

Компании часто используют сети VLAN в качестве способа логической группировки пользователей. Это можно сравнить с традиционной организацией рабочих мест, в которой несколько отделов обычно группировались в локальный департамент и локальная сеть естественным образом решала задачи связи для этого департамента. В настоящее время сотрудники часто не связаны с конкретным физическим рабочим местом, поэтому сети VLAN создают не физическую, а логическую группу пользователей. Например, сотрудники, работающие в отделе маркетинга, объединены VLAN-сетью маркетинга, а сотрудники инженерного подразделения — VLAN-сетью инженерных служб.

Сети VLAN решают задачи масштабирования сети, обеспечения безопасности и сетевого управления. В сетях с топологией VLAN маршрутизаторы обеспечивают фильтрацию широковещания, решают задачи защиты сети и управления потоками данных.

Сеть VLAN представляет собой группу сетевых устройств и служб, не ограниченную физическим сегментом или коммутатором. На рис. 9.1. показано логическое группирование рабочих станций в сети VLAN, в сравнении с физическим группированием рабочих станций в традиционной сети LAN.

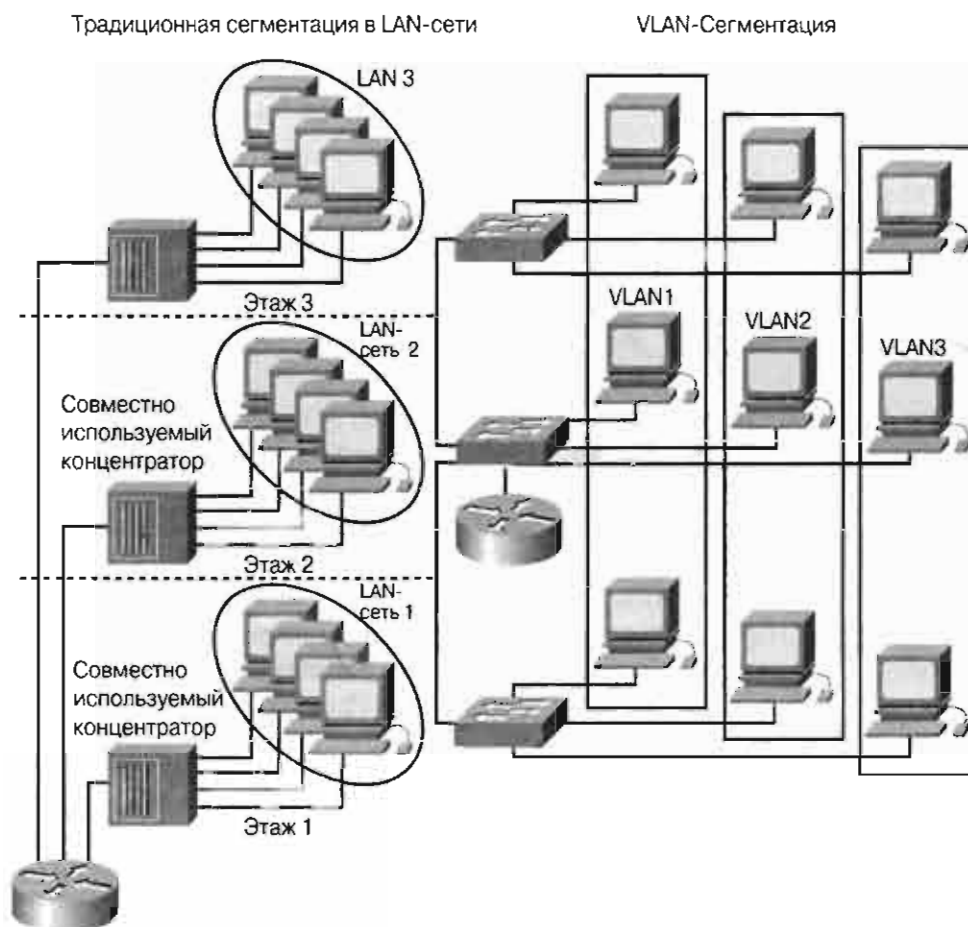


Рис. 9.1. Сети VLAN и физические границы

Сети VLAN логически сегментируют сети, использующие коммутацию, на основе их организационных функций, принадлежности к различным рабочим коллективам (группам) или используемым приложениям, а не на базе физического или географического расположения. Например, все рабочие станции и серверы, используемые некоторой рабочей группой, могут быть объединены в одну и ту же сеть VLAN, независимо от их физического подсоединения к сети или расположения на территории предприятия. На рис. 9.2 приведен пример проектирования сети VLAN в физической сети. В данном случае создаются три сети VLAN, в которых рабочие станции соединены друг с другом через коммутаторы, а сами коммутаторы соединены друг с другом через маршрутизатор. Реконфигурирование системы может быть выполнено программным способом, без физического перемещения устройств и изменения подключения кабелей.

На рис. 9.3 показано физическое проектирование сети VLAN, основанное на различных рабочих группах компании и их расположении на различных этажах офиса. В данном случае сеть VLAN создается для каждого отдела (инженерный отдел, отдел маркетинга и отдел учета), в каждом из которых имеется свой коммутатор.

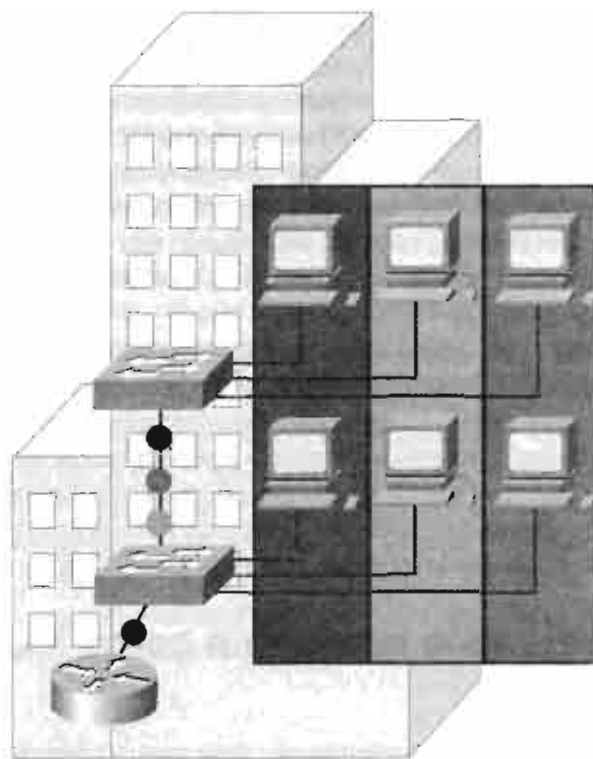


Рис. 9.2. Проектирование виртуальной локальной сети

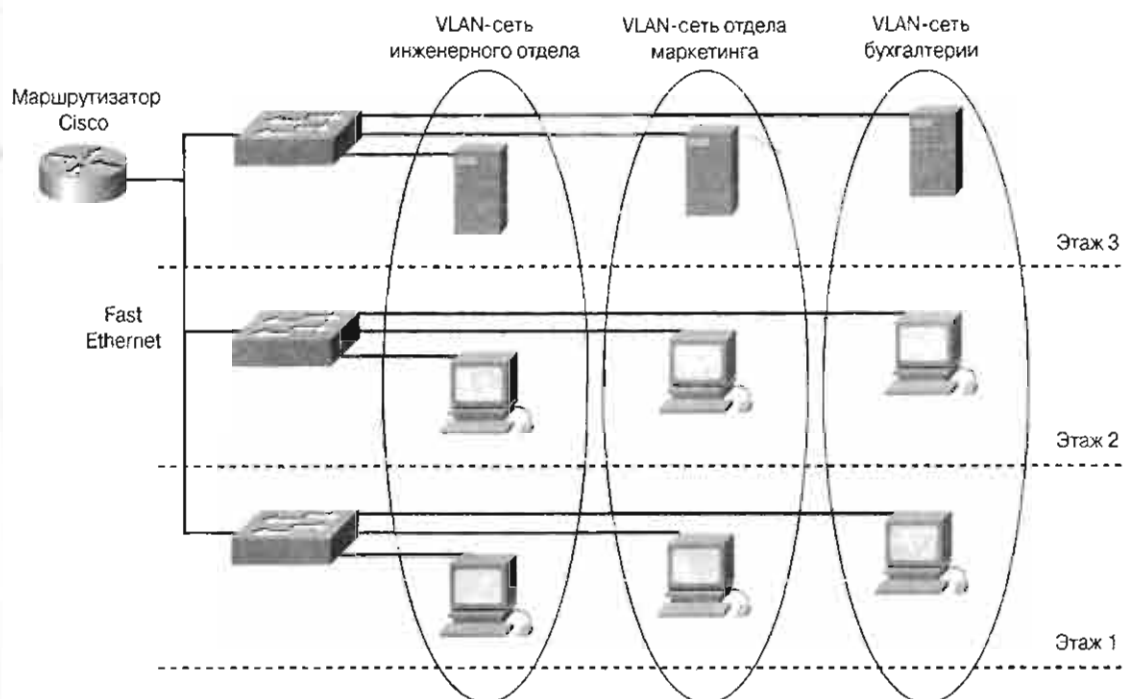


Рис. 9.3. Сети VLAN охватывают определенное физическое пространство

Как правило, соединения клиентской рабочей станции, находящейся в сети VLAN, ограничены только файловыми серверами, принадлежащими этой же сети VLAN. Сеть VLAN можно рассматривать как широковещательный домен, который существует в определенном наборе коммутаторов. Сети VLAN состоят из ряда конечных систем, таких как рабочие станции или сетевые устройства (мосты и маршрутизаторы), соединенных друг с другом через отдельный мостовой домен. Мостовой домен поддерживается различными сетевыми устройствами, такими, например, как коммутаторы сетей LAN, которые работают по мостовым протоколам; при этом для каждой сети VLAN имеется своя мостовая группа.

Сети VLAN создаются для реализации служб сегментации, которые в традиционных LAN-конфигурациях обычно обеспечиваются маршрутизаторами. В топологиях сетей VLAN маршрутизаторы обеспечивают фильтрацию *широковещания (broadcast)*, защиту сети и управление потоками данных. Коммутаторы не могут осуществлять мостовые соединения между сетями VLAN, поскольку это нарушило бы целостность широковещательного домена сети VLAN. Маршрутизация потоков данных должна происходить только при передаче данных между сетями VLAN.

Широковещательные домены в сетях VLAN и маршрутизаторы

Сеть VLAN является широковещательным доменом, который создается одним или более коммутаторами. В приводимом ниже сценарии при проектировании сети требуется создать два отдельных широковещательных домена. На рис. 9.4 два отдельных широковещательных домена создаются с помощью трех отдельных коммутаторов — по одному на каждый широковещательный домен. Следует отметить, что маршрутизатор позволяет осуществлять маршрутизацию пакетов между широковещательными доменами, которые в данном случае подобны отдельным группам устройств 3-го уровня.

Это может быть сделано путем установки одного или нескольких соединений с маршрутизатором.

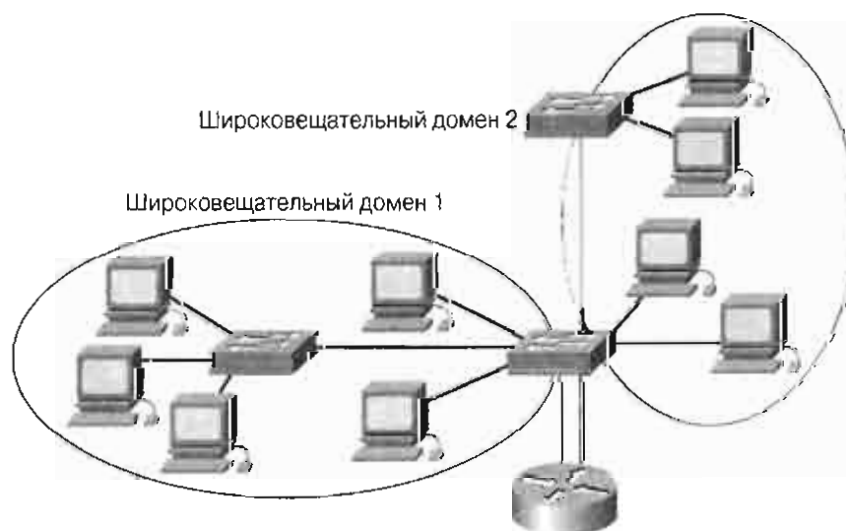


Рис. 9.4. Распределение широковещания в сети VLAN

Функционирование сети VLAN

Сеть VLAN представляет собой сеть коммутации, которая логически сегментируется в соответствии с выполняемыми функциями, объединением сотрудников в группы или согласно используемым приложениям, независимо от физического расположения пользователей. Сети VLAN может быть выделен любой порт коммутатора. Порты, выделенные одной и той же сети VLAN, имеют общее пространство широковещания.

Порты, не принадлежащие к этой сети VLAN, не получают эти широковещательные сообщения. Это повышает общую производительность сети, поскольку уменьшается количество ненужных широковещательных сообщений, которые потребляют полосу пропускания сети. Сети VLAN создаются двумя описанными ниже способами.

- **Статические сети** — этот способ также называется членством на базе порта. Назначение портов сетям VLAN создает статическое распределение VLAN. Когда устройство подсоединяется к порту, оно автоматически попадает во VLAN-сеть этого порта. Если устройство меняет порт своего подключения, но ему требуется доступ к той же самой сети VLAN, то сетевой администратор должен сделать назначение порта сети VLAN для нового соединения. Пример такого назначения приведен на рис. 9.5.

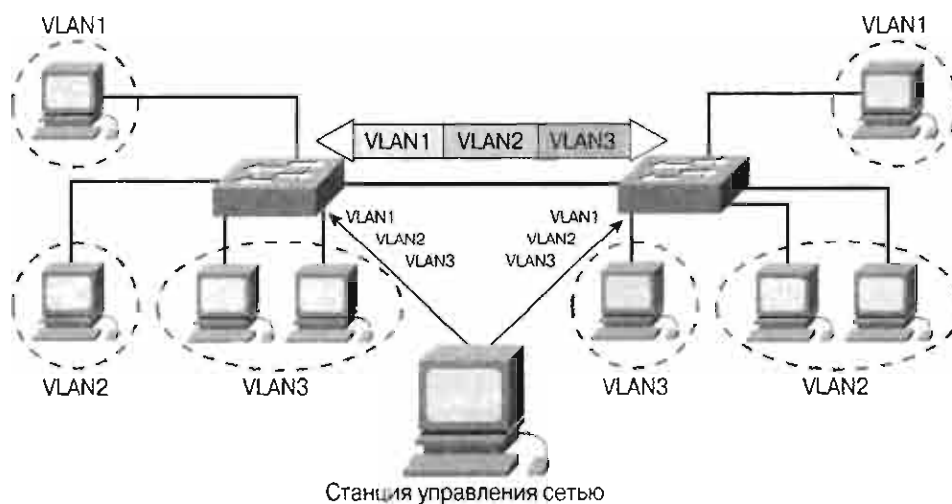


Рис. 9.5. Статические сети VLAN

- **Динамические сети VLAN** — динамические сети VLAN создаются с использованием пакетного программного обеспечения, такого как CiscoWorks 2000. С помощью сервера политик управления сетями VLAN (VLAN Management Policy Server — VMPS) можно назначать порты коммутатора сетям VLAN динамически, на основе MAC-адреса устройства-источника, подсоединенного к данному порту. В настоящее время динамические VLAN позволяют присоединять к себе устройства на основе MAC-адреса источника. Когда устройство присоединяется к сети, оно делает запрос в базу данных на сервере VMPS относительно своей принадлежности к данной сети VLAN. Этот процесс показан на рис. 9.6, где каждый коммутатор имеет свой уникальный MAC-адрес.

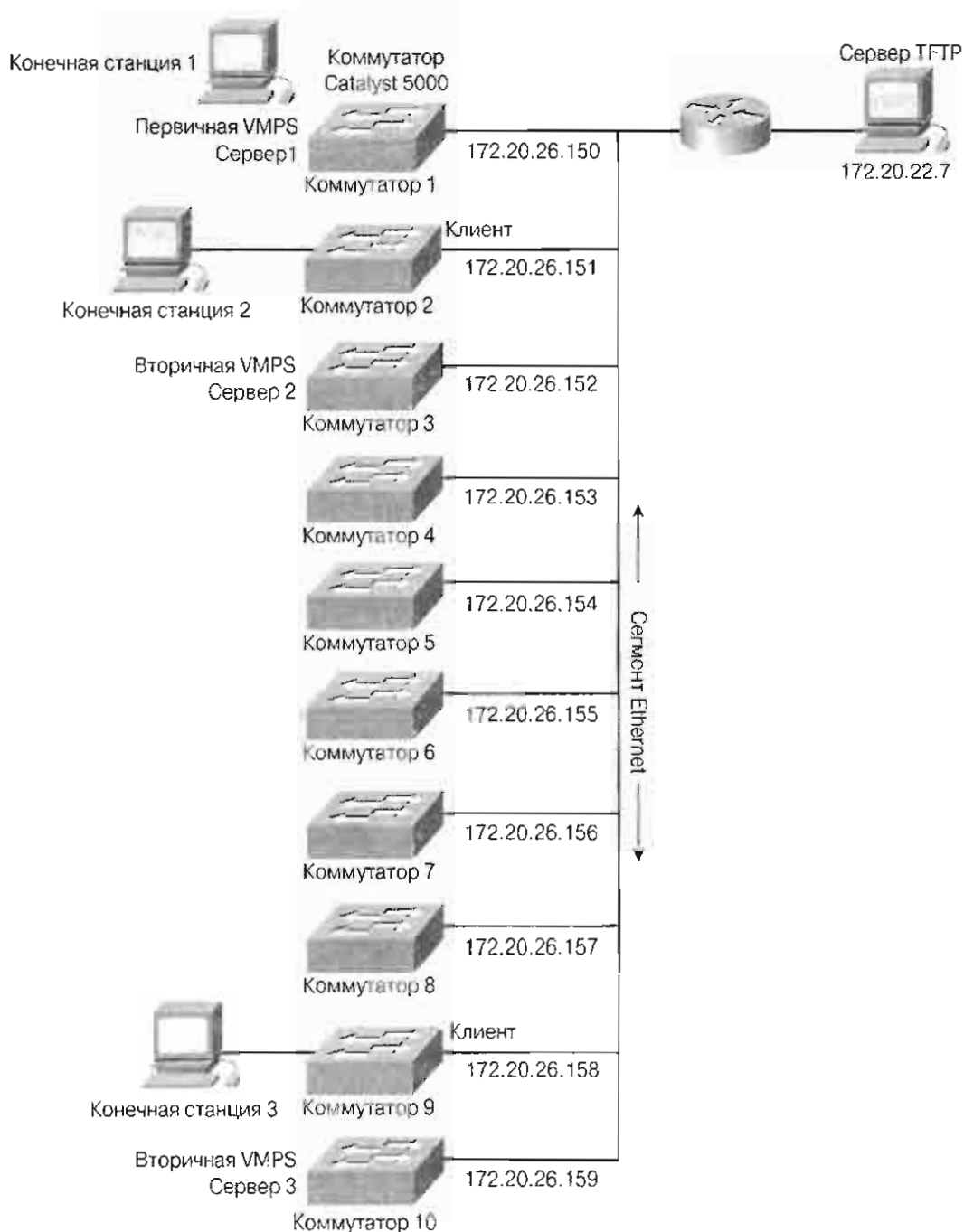


Рис. 9.6. Динамические сети VLAN

Принадлежность устройства к статической сети VLAN на основе портов проиллюстрировано на рис. 9.7. Конкретной сети VLAN назначается порт, который не зависит от пользователя или системы, подсоединенной к данному порту. Это означает, что все пользователи, подсоединенные к данному порту, должны быть членами одной и той же сети VLAN. Отдельная рабочая станция пользователя или концентратор, к которому подсоединены несколько рабочих станций, могут быть подсоединены к отдельному порту коммутатора. Назначение портов сетям VLAN обычно осуществляет сетевой администратор. Конфигурация порта в этом случае является статической и переключе-

ние порта на другую VLAN не может быть выполнено автоматически без реконфигурирования коммутатора. Следует обратить внимание на то, что каждая сеть VLAN находится в отдельной подсети, а маршрутизатор используется для связи между этими подсетями.

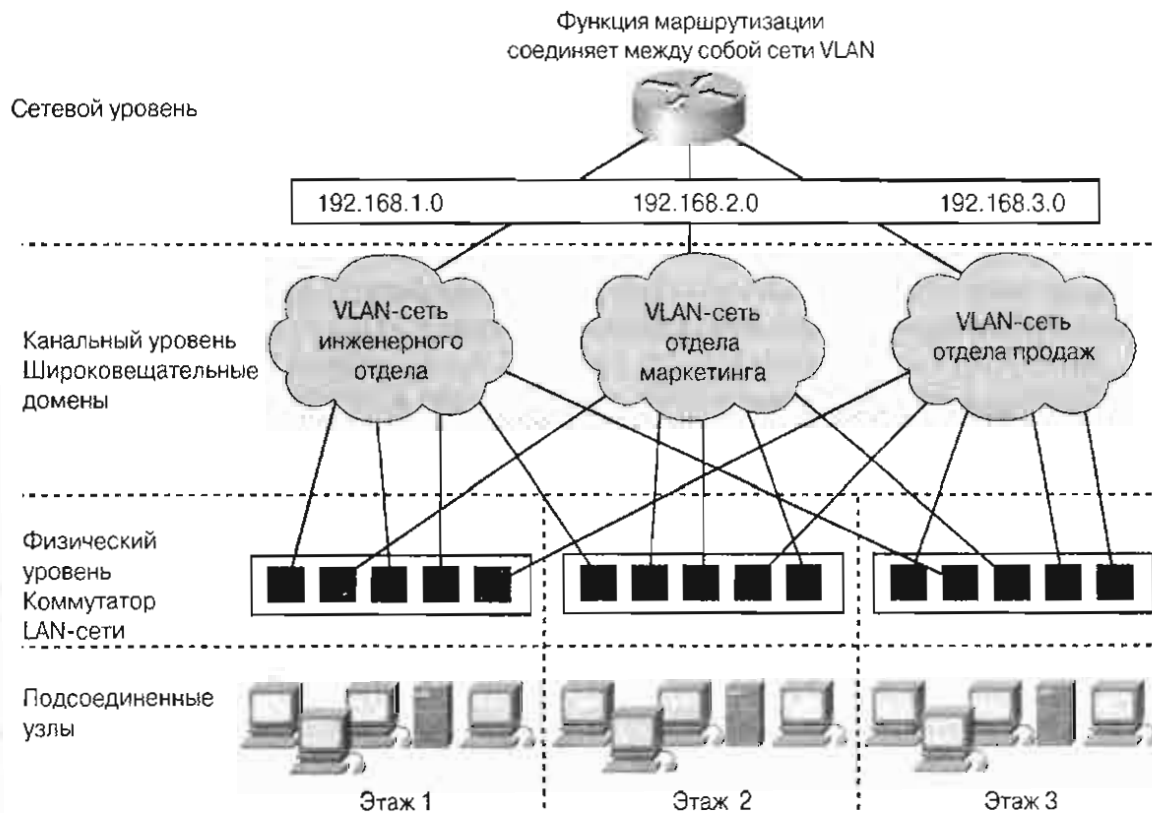


Рис. 9.7. Статические виртуальные сети на основе портов

Когда пользователи подсоединяются к этому совместно используемому сегменту, как это происходит в традиционных основанных на концентраторах сетях LAN, все они после этого используют общую полосу пропускания. На каждого дополнительного пользователя, который подсоединяется к совместно используемой среде передачи, приходится меньше доступной полосы пропускания, поскольку все пользователи находятся в одном и том же коллизийном домене. Если количество пользователей, использующих одну и ту же полосу пропускания становится слишком большим, то начинаются частые коллизии и работа приложения пользователя становится малопродуктивной. Коммутаторы уменьшают вероятность коллизий за счет обеспечения выделенной полосы пропускания между устройствами с помощью микросегментации; однако коммутаторы по-прежнему рассылают всем пользователям широковещательные сообщения, такие, как сообщения протокола ARP. Сети VLAN обеспечивают пользователям большую полосу пропускания в совместно используемой сети путем создания отдельных широковещательных доменов.

По умолчанию на каждом порте коммутатора имеется сеть VLAN1 или сеть VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

Следует помнить о том, что каждый интерфейс коммутатора ведет себя как порт моста и в целом коммутатор можно рассматривать как многопортовый мост. Мосты отфильтровывают потоки данных, которые не требуется направлять в иные сегменты, кроме того, из которого они поступили. Если фрейм необходимо переслать через мост и MAC-адрес получателя известен, то мост направляет этот фрейм на соответствующий интерфейс и не направляет на все остальные. Если мосту или коммутатору не известно расположение получателя, то происходит лавинная рассылка фрейма со всех портов в данный широковещательный домен (VLAN), за исключением того порта, с которого этот фрейм поступил.

Каждой виртуальной сети VLAN должен быть присвоен уникальный адрес 3-го уровня (сети или подсети). Это помогает осуществлять коммутацию пакетов между сетями VLAN, в которых имеются маршрутизаторы. Сети VLAN могут выступать в качестве сквозных сетей (end-to-end network), которые охватывают всю среду коммутатора, или существовать в определенных географических границах.

Сквозные VLAN-сети

Сквозные сети VLAN позволяют группировать устройства на основе использования ресурсов. Оно включает в себя уровень использования сервера, рабочие группы по выполняемым проектам и отделы. Цель сквозных сетей VLAN состоит в том, чтобы не менее 80% данных передавались внутри локальной сети VLAN. На рис. 9.8 приведен пример сквозных сетей VLAN. Сквозная VLAN-сеть обладает следующими характеристиками:

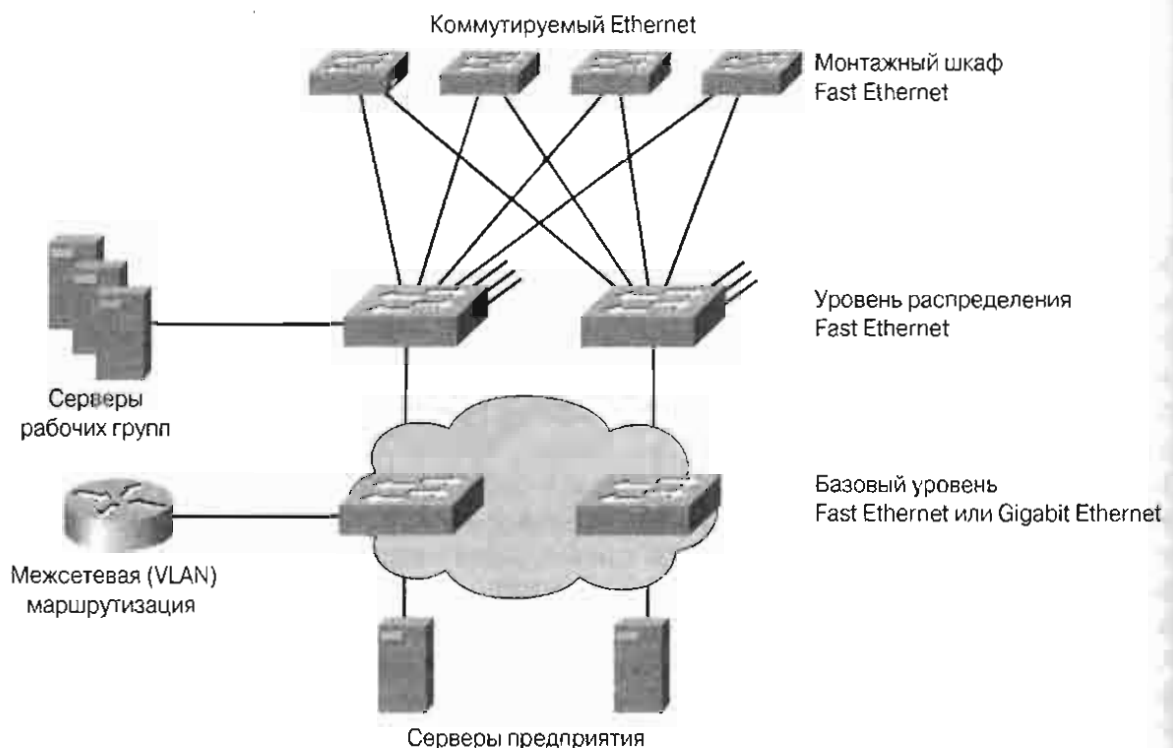


Рис. 9.8. Сквозные VLAN-сети

Пользователи группируются в сети VLAN независимо от их физического расположения, но в соответствии с исполняемыми ими рабочими функциями или с принадлежностью к разным рабочим группам.

У всех пользователей соотношение передачи данных внутри VLAN-сети и за ее пределы должно быть одним и тем же и составлять 80:20.

При перемещении пользователя в пределах сети кампуса его членство в сети VLAN не должно изменяться.

В каждой VLAN-сети для всех ее членов должны действовать общие правила безопасности

Географические VLAN-сети

По мере того, как корпоративные сети централизовали свои ресурсы, становилось все сложнее поддерживать сквозные VLAN-сети. Пользователям требовались различные ресурсы, многие из которых уже не находились в их VLAN-сетях. По причине такого изменения в размещении и использования ресурсов в настоящее время VLAN-сети все чаще создаются в определенных географических границах, а не в границах сообщества. Эти географические границы могут быть целым зданием или всего лишь одним коммутатором в монтажном шкафу. В такой географической VLAN-структуре типичным является случай соотношения обмена данными 20% для локального использования и 80% — для удаленных соединений. Это соотношение прямо противоположно тому, которое обычно устанавливается при проектировании сквозных VLAN. Хотя такая топология означает, что пользователю приходится пересекать устройство 3-го уровня (маршрутизатор) для получения доступа к 80% ресурсов, она позволяет использовать в сети последовательный детерминистический способ получения доступа к ресурсам.

Географическими сетями VLAN также значительно легче управлять и концептуализировать их, чем VLAN-сетями, устройства которых находятся в географически различных областях.

Преимущества сетей VLAN

Коммерческие компании постоянно реорганизуются. В среднем 20-40% рабочей силы физически меняют место проживания каждый год. Эти переезды, добавление новых пользователей, и другие изменения являются одними из главных головных болей сетевых менеджеров и составляют одну из самых больших статей расходов, связанных с управлением сетью. Многие перемещения пользователей требуют прокладки новых кабелей и почти все перемещения требуют новой адресации станций и реконфигурирования концентраторов и маршрутизаторов.

Изменения в системе управления сетью

Сети VLAN предоставляют эффективный механизм для управления изменениями в топологии сети и значительно снижают затраты, связанные с реконфигурированием концентраторов и маршрутизаторов. Пользователи сети VLAN могут использовать одно и то же сетевое адресное пространство (т.е. IP-подсеть), независимо от их физического расположения. Когда пользователи сети VLAN перемещаются из одного места в другое, до тех пор пока они остаются в одной и той же VLAN и подсоединены к од-

ному и тому же порту коммутатора, их сетевые адреса не изменяются. Изменение расположения пользователя требует лишь таких простых действий как включение штекера пользователя в соответствующий порт VLAN-коммутатора и конфигурирование порта коммутатора, к которому подсоединена данная VLAN. В динамических сетях VLAN при просмотрении MAC-адреса сетевого адаптера переместившейся рабочей станции в VMPS, коммутатор автоматически конфигурирует порт таким образом, чтобы он оказался в требуемой сети VLAN.

VLAN-сети и безопасность

VLAN сети являются эффективным механизмом расширения сферы действия брандмауэра от маршрутизаторов к среде коммутатора и защиты сети от потенциально опасных проблем, связанных с широковещанием. Кроме того, сети VLAN сохраняют все преимущества высокопроизводительной коммутации.

Брандмауэры создаются путем назначения портов коммутатора или пользователей в конкретные группы VLAN как на одном коммутаторе, так и на нескольких соединенных друг с другом коммутаторах. Широковещательные потоки данных не передаются за пределы сети VLAN. На рис. 9.9 приведен пример широковещательных доменов. В свою очередь смежные порты не получают широковещательных данных, которые генерируются другими сетями VLAN. Такой тип конфигурации значительно уменьшает общий объем широковещательных данных, освобождает полосу пропускания для действительно полезных данных и снижает общий уровень уязвимости сети в отношении широковещательных штормов. На рис. 9.10 показано как маршрутизатор может выполнять функции брандмауэра между сетями VLAN.

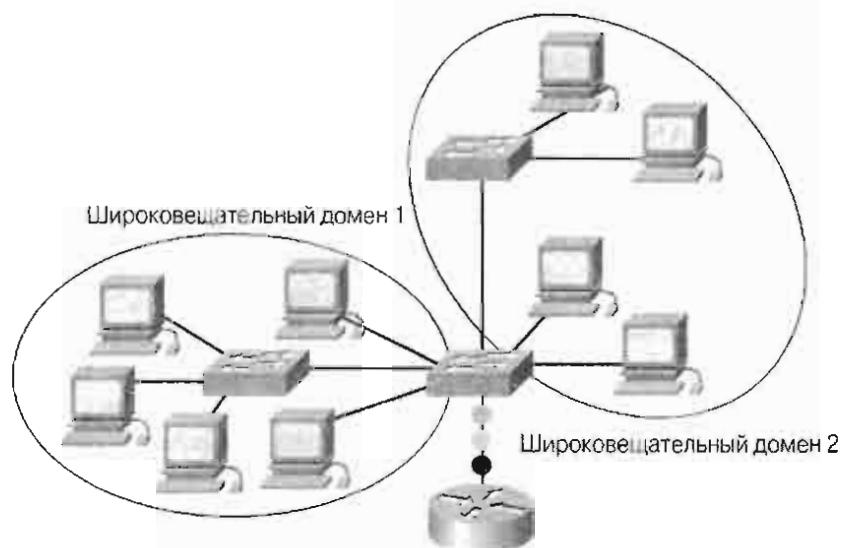


Рис. 9.9. Широковещательные домены

Одной из проблем совместно используемых сетей LAN является относительная легкость проникновения в них. Подключаясь к работающему порту несанкционированный пользователь получает доступ ко всем данным, передаваемым в сегменте. Чем больше группа пользователей, тем большие возможности создаются для потенциального несанкционированного доступа.



Рис. 9.10. Брандмауэр для широковещательных данных

Одним из экономически эффективных и легко административно реализуемых способов повышения уровня безопасности в сети является сегментация сети на несколько широковещательных групп. Это позволяет сетевому менеджеру решить следующие задачи:

- ограничить количество пользователей во VLAN-группе;
- предотвратить присоединение других сетей без предварительного получения разрешения от приложения, управляющего сетью VLAN;
- сконфигурировать все неиспользуемые порты на принимаемую по умолчанию службу нижнего уровня VLAN.

Реализация такого типа сегментации относительно проста. Порты коммутатора объединяются в группы на основе типа приложения и привилегий при доступе. Ограниченные приложения и ресурсы обычно размещаются в защищенных VLAN-группах. В защищенных сетях VLAN коммутатор ограничивает доступ пользователей к группе. Ограничения могут основываться на адресах станций, типах приложений или типах протокола. Пример обеспечения безопасности в сети VLAN показан на рис. 9.11.

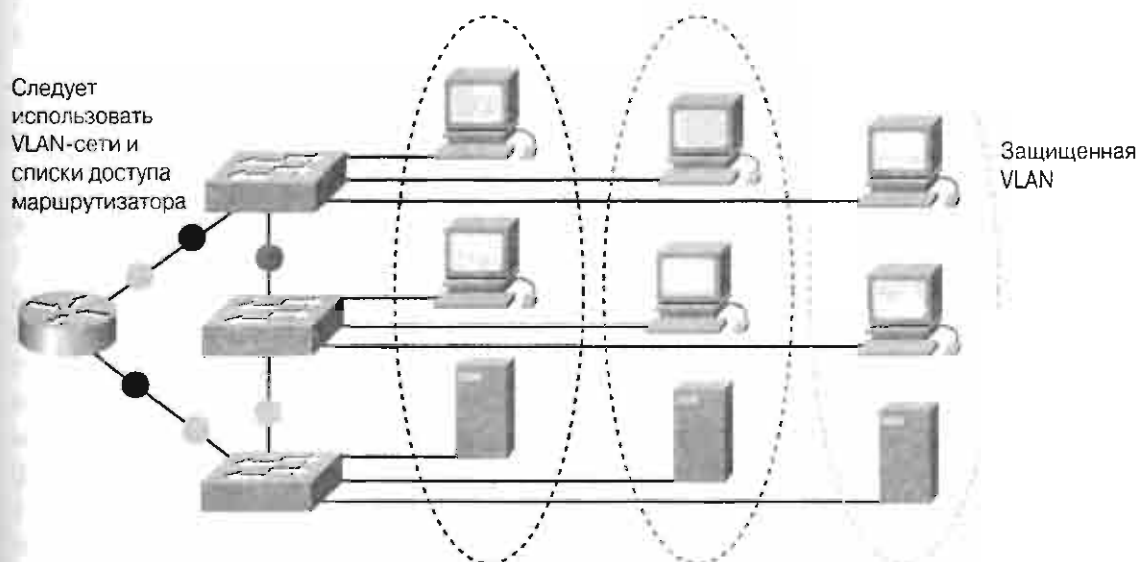


Рис. 9.11. Защищенная VLAN-сеть

Использование концентраторов в сетях VLAN

За последние несколько лет сетевые администраторы установили большое количество концентраторов. Многие из этих устройств заменяются настоящее время коммутирующими технологиями.

Поскольку приложениям требуется все большая выделенная полоса пропускания и производительность непосредственно на рабочем столе, эти концентраторы по-прежнему выполняют полезные функции по многим уже существующим сетям. Сетевые менеджеры могут сэкономить средства. Подсоединив существующие концентраторы к коммутаторам. Пример такого использования концентраторов приведен на рис. 9.12. каждый сегмент концентратора, подсоединенный к порту коммутатора, может быть назначен только одной сети VLAN. Все станции, совместно использующие сегмент концентратора, становятся членами одной и той же группы VLAN. Коммутатор поддерживает несколько адресов доступа к среде передачи или MAC-адресов (Media Access Control — MAC), по одному на каждую станцию, которые логически связаны с портом, к которому подсоединен концентратор. Если требуется переназначить отдельную станцию в другую VLAN-сеть, то станцию необходимо подсоединить к соответствующему концентратору. Соединенные между собой коммутаторы обрабатывают передачу данных между портами коммутатора и автоматически определяют соответствующие принимающие сегменты. Чем больше мелких групп будет образовано на совместно используемом концентраторе, тем больше степень микросегментации и тем большая гибкость обеспечивается для назначения индивидуальных пользователей в группы VLAN. Путем подсоединения концентраторов к коммутаторам можно сконфигурировать концентраторы в качестве части архитектуры VLAN. Можно также обеспечить совместное использование передачи данных и сетевых ресурсов, непосредственно подсоединенных к коммутирующим портам с получателями VLAN.

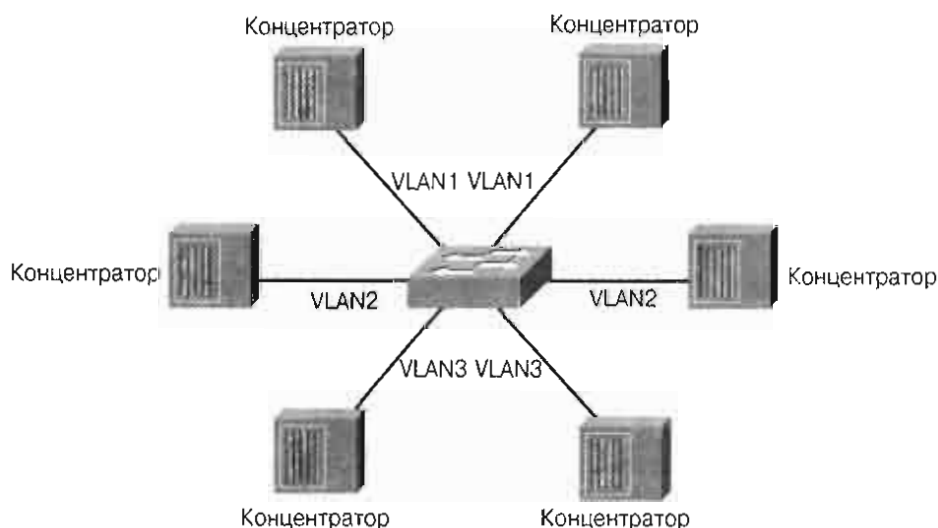


Рис. 9.12. Использование существующих концентраторов в среде коммутации сети VLAN

Типы VLAN-сетей

Три приведенных ниже базовых модели определяют назначение пакета сети VLAN и управляют его передачей.

- Сети VLAN, базирующиеся на портах (статические).
- VLAN-сети на основе MAC-адресов (динамические).
- Основанные на протоколах VLAN-сети.

Количество образованных на одном коммутаторе VLAN-сетей может изменяться в широких пределах, в зависимости от нескольких факторов. Среди этих факторов можно выделить типичный характер передачи данных, типы приложений, потребности сетевого управления и общей группы. Кроме того, важным фактором, определяющим количество VLAN-сетей на коммутаторе, является используемая схема IP-адресации. Например, предположим, что сеть использует 254-битовую маску для определения подсетей. В этом случае в одной подсети можно использовать до 254 адресов для рабочих станций. Поскольку настоятельно рекомендуется устанавливать взаимно однозначное соответствие между сетями VLAN и IP-подсетями, в одной VLAN-сети может быть не более 254 устройств.

Идентификация фреймов в сетях VLAN

В сетях VLAN с несколькими коммутаторами заголовки фреймов инкапсулируются или модифицируются для указания идентификатора ID сети VLAN до того, как фрейм будет отправлен в канал между коммутаторами. Перед отправкой фрейма конечному устройству заголовок фрейма изменяется и приобретает первоначальный вид.

Идентификация VLAN логически идентифицирует принадлежность пакета к определенной группе VLAN. Существует несколько магистральных методологий, включая IEEE 802.1Q, ISL, 802.10 и LANE.

Теги фреймов в спецификации IEEE 802.1Q

Протокол 802.1Q является стандартным методом идентификации VLAN-сетей путем вставки идентификатора VLAN в заголовок фрейма. Это процесс называется добавлением тега. На рис. 9.13 показан формат фрейма 802.1Q с идентификатором ID сети VLAN. Каждому порту 802.1Q назначается магистраль, а все порты магистрали оказываются в одной изначальной сети VLAN. Все фреймы без тегов назначаются в LAN-сеть, указанную в параметре ID. Ассоциированные магистральные порты 802.1Q имеют изначальное значение VLAN. В спецификации 802.1Q фрейма для изначальной VLAN теги не добавляются. Следовательно обычные рабочие станции могут прочитать изначальные фреймы без тегов, но не могут прочитать другие фреймы, потому что они имеют теги. Добавление тегов к фреймам в IEEE 802.1Q является предпочтительным методом обмена информацией о сетях VLAN между коммутаторами.

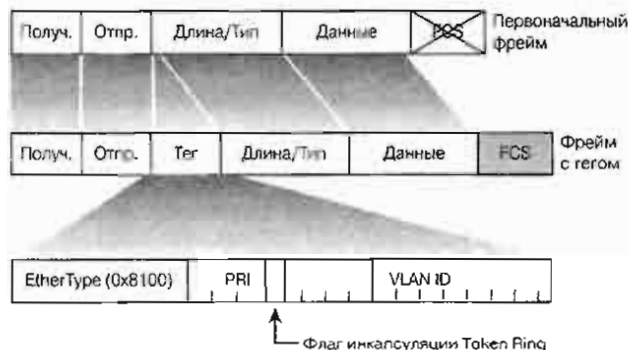


Рис. 9.13. Формат фрейма 802.1Q

Протокол межкоммутаторного канала

Протокол межкоммутаторного канала (Inter-Switch Link — ISL) представляет собой фирменный протокол инкапсуляции Cisco, используемый для связи между собой нескольких коммутаторов. На рис. 9.14 показан формат фрейма протокола ISL.

Для присвоения фреймов, которое используется коммутаторами серии Catalyst Cisco используется обладающий низкой задержкой механизм мультиплексирования потоков данных от нескольких сетей VLAN в один физический канал. Этот протокол был реализован для соединений между коммутаторами, маршрутизаторами и сетевыми адаптерами, используемыми на сетевых узлах, таких как серверы. Для поддержки функций протокола ISL на каждом подсоединенном устройстве должен быть сконфигурирован протокол ISL. Маршрутизатор, на котором сконфигурирован протокол ISL может быть использован для коммуникации между VLAN-сетями. Этот процесс описан более подробно в главе 10. Устройство, на котором не функционирует протокол ISL, при получении инкапсулированного ISL-фрейма Ethernet рассматривает его как ошибку протокола, если размер заголовка вместе с данными фрейма превосходит размер максимального модуля передачи (maximum transmission unit — MTU). Администраторы используют протокол ISL для поддержки избыточных каналов и перераспределения нагрузки между параллельными каналами с использованием протокола связующего дерева (Spanning Tree Protocol).

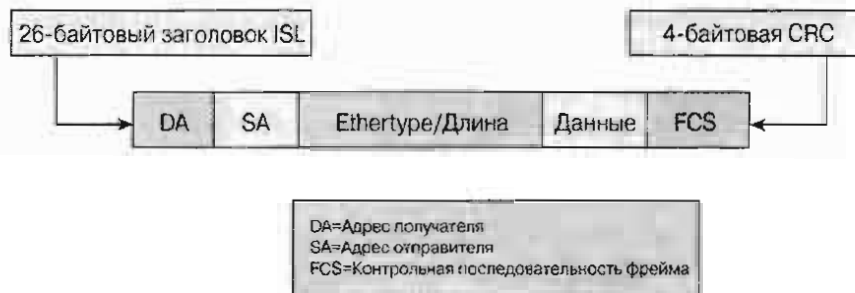


Рис. 9.14. Формат фрейма протокола ISL

Спецификация FDDI 802.10

Спецификация FDDI 802.10 является фирменным методом Cisco для передачи информации о VLAN-сетях во фрейме стандарта IEEE 802.10 (FDDI). Информация VLAN записывается в поле идентификатора ассоциации безопасности (security asso-

ciation identifier — SAID) фрейма 802.10. Этот метод, как правило, используется для передачи данных VLAN по магистрали распределенного оптоволоконного интерфейса данных (Fiber Distributed Data Interface — FDDI).

Эмуляция локальной сети

Эмуляция локальной сети (LAN Emulation — LANE) представляет собой стандарт, определенный форумом ATM и предоставляющий возможность двум станциям, подсоединенным через магистраль ATM те же возможности, которые они бы имели в обычных локальных сетях, таких как Ethernet или Token Ring. Как показывает само название, функцией протокола LANE является эмуляция LAN-сети в сети асинхронного режима передачи (Asynchronous Transfer Mode — ATM). В частности, протокол LANE определяет механизмы эмуляции по спецификации IEEE 802.3 Ethernet или 802.5 Token Ring LAN. Протокол LANE определяет интерфейс службы для протоколов более высокого уровня (т.е. для сетевого уровня), аналогично тому, как это происходит в существующих сетях LAN. Данные, пересылаемые по сети ATM, инкапсулируются в соответствующий MAC-формат LAN-сети. Иными словами, протоколы LANE принуждают ATM-сеть выглядеть и вести себя как LAN сеть Ethernet или Token Ring. Пример LANE-сети приведен на рис. 9.15.



Рис. 9.15. Сеть LANE

В табл. 9.1 перечислены методы присвоения тегов и инкапсуляции.

Таблица 9.1. Методы присвоения тегов и инкапсуляции

Метод идентификации	Инкапсуляция	Присвоение тегов	Среда передачи
802.1Q	Нет	Да	Ethernet
ISL	Да	Нет	Ethernet
802.10	Нет	Нет	FDDI
LANE	Нет	Нет	ATM

Конфигурирование VLAN

Первоначально сетевые администраторы полагали, что сети VLAN упростят их работу и сделают ненужными маршрутизаторы. К сожалению для них, эти надежды не оправдались. Сети VLAN не устранили проблем, связанных с 3-м уровнем модели OSI. Сети VLAN позволяют легче решать задачи 3-го уровня, такие, например, как разработка более простых списков доступа, однако необходимость в маршрутизации на 3-м уровне не исчезла.

Конфигурирование статических VLAN-сетей

Под статическими VLAN понимаются порты коммутатора, которым вручную назначаются сети VLAN путем использования управляющего программного обеспечения или непосредственным конфигурированием коммутатора. Эти порты поддерживают назначенную им конфигурацию VLAN сетей до тех пор пока она не будет изменена системным администратором. Хотя статические VLAN требуют в несения изменений вручную, они безопасны, легко конфигурируются и удобны для мониторинга. Этот тип VLAN хорошо работает в сетях, в которых соблюдаются следующие условия:

- перемещения станций легко контролируются и управляются;
- имеется надежное управляющее программное обеспечение для конфигурирования портов коммутатора;
- нежелательная дополнительная служебная нагрузка, требуемая для поддержки MAC-адресов конечных станций и типовых таблиц фильтрации.

Динамические VLAN, в отличие от статических, не полагаются на порты, которым назначаются конкретные VLAN сети. Вместо этого назначение VLAN-сетей портам основывается на MAC-адресах, логической адресации или типе протокола. При конфигурировании статических VLAN-сетей на маршрутизаторах Cisco 29xx следует помнить следующие основные положения:

- максимальное количество подключаемых VLAN-сетей зависит от типа коммутатора и ограничивается количеством его портов;
- сеть VLAN1 является одной из VLAN-сетей, создаваемых по умолчанию производителем;
- по умолчанию VLAN1 является VLAN-сетью;
- по сети VLAN1 рассылаются анонсы маршрутов протокола обнаружения устройств Cisco (*Cisco Discovery Protocol — CDP*) и магистрального протокола VLAN (*VLAN Trunking Protocol — VTP*);

- на всех коммутаторных магистралях, принимающих участие в работе VLAN-сетей, должен быть сконфигурирован один и тот же протокол инкапсуляции, такой как 802.1Q или ISL;
- команды конфигурирования VLAN-сетей зависят от номера модели;
- IP-адреса для моделей Catalyst 29xx находятся в широковещательном домене VLAN;
- при создании, добавлении и удалении VLAN-сетей коммутатор должен находиться в режиме VTP-сервера.

Создание на коммутаторе статической VLAN-сети является несложной задачей. При использовании коммутатора, работающего с командами IOS Cisco, следует войти в режим конфигурирования VLAN с помощью команды привилегированного EXEC-режима **vlan database**. Для создания VLAN-сети следует выполнить приведенные ниже команды.

```
Switch#vlan database
Switch(vlan)vlan vlan_number { vlan_name}
Switch(vlan)exit
```

При необходимости следует также сконфигурировать имя VLAN-сети.

После выхода из режима конфигурирования на коммутаторе создается VLAN-сеть. Следующим этапом является назначение данной VLAN одному или более интерфейсам.

```
Switch(config)#interface fastethernet 0/3
```

Коммутатор Catalyst 2900:

```
Switch(config-if)#switchport access vlan 2
```

Коммутатор Catalyst 1900:

```
(config-if)#vlan-membership static 2
```

Протестировать конфигурацию можно с помощью команды **show running-config**, как показано в примере 9.1.

Пример 9.1. show running-configuration

```
Switch#show running-config
Hostname Switch
!
ip subnet-zero
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 2
--- output omitted ---
```

**Лабораторная работа: конфигурирование статической VLAN-сети**

В этой лабораторной работе требуется сконфигурировать базовую конфигурацию коммутатора и протестировать ее. С консоли требуется определить версию встроенного программного обеспечения, создать две VLAN-сети, задать им имена и назначить им соответствующие порты.

Тестирование конфигурации VLAN-сети

Хорошей практикой является тестирование конфигурации VLAN-сети с помощью команд **show vlan** (как показано в примере 9.2), **show vlan brief** или **show vlan id id_number**

Пример 9.2. Команда **show vlan**

```
Switch#show vlan
Virtual LAN ID: 300 (IEEE 802.10 Encapsulation)
VLAN Trunk Interface: FDDI 1/1.10
Protocols Configured: Address: Received: Transmitted:
IP 31.108.1.1 642 645
Virtual LAN ID: 400 (ISL Encapsulation)
VLAN Trunk Interface: FastEthernet 2/1.20
Protocols Configured: Address: Received: Transmitted:
IP 171.69.2.2 123456 654321
Bridge Group 50 5190 8234
Virtual LAN ID: 500 (ISL Encapsulation)
VLAN Trunk Interface: FastEthernet 2/1.30
Protocols Configured: Address: Received: Transmitted:
IPX 1000 987654 456789
Virtual LAN ID: 600 (ISL Encapsulation)
VLAN Trunk Interface: FastEthernet 2/1.30
Protocols Configured: Address: Received: Transmitted:
IP 198.92.3.3 8114 4508
IPX 1001 2 3
Bridge Group 50 8234 5190
```

При работе с VLAN-сетями следует руководствоваться следующими положениями:

- созданная VLAN-сеть остается неиспользуемой до тех пор, пока она не будет логически связана с портами коммутатора;
- по умолчанию все порты Ethernet находятся в сети VLAN1.
- между номерами портов не следует вводить пробелы. В этом случае коммутатор реагирует сообщением об ошибке, поскольку пробел отделяет другой аргумент, который не является структурной частью команды.

Сохранение конфигурации VLAN

Полезно иметь копию конфигурации VLAN-сети в виде текстового файла в качестве резервной копии и для целей аудита. Для сохранения файла VLAN-конфигурации можно использовать дискету, с тем чтобы потом передать ее на другие рабочие станции. Если в файле конфигурации окажутся скопированными посторонние символы, то их следует удалить.

Нижес описаны действия, которые следует выполнить для копирования конфигурации VLAN-сети.

- Этап 1. С консоли коммутатора перейти в привилегированный режим конфигурирования коммутатора.
- Этап 2. В окне программы HyperTerminal выбрать опцию Transfer (Передача).
- Этап 3. Выбрать опцию Capture Text.
- Этап 4. Выбрать место сохранения файла конфигурации (такое, например, как “Рабочий стол”).
- Этап 5. Задать имя файла конфигурации VLAN-сети.
- Этап 6. Выбрать опцию Start.
- Этап 7. На коммутаторе выполнить команду **show run**.
- Этап 8. После того, как будут выполнены команды файла конфигурации, (для окончания их выполнения следует нажать несколько раз клавишу пробела), вернуться к опции Transfer окна программы HyperTerminal, выбрать опцию Capture Text, а затем опцию Stop для сохранения и закрытия файла.
- Этап 9. Удалить посторонние символы.



Лабораторная работа: тестирование конфигурации VLAN-сети

В этой лабораторной работе требуется создать базовую конфигурацию коммутатора и две виртуальных локальных сети VLAN. После этого VLAN-сетям следует присвоить имена и назначить им несколько портов.

Протестировать функционирование сетей можно путем перемещения рабочей станции из одной сети в другую.

Удаление конфигурации VLAN-сети

Для удаления сети VLAN на коммутаторе, допускающем конфигурирование из командной строки, следует выполнить команду **clear vlan номер**, как показано в примере 9.3. В этом примере сеть VLAN 2 удаляется из домена с помощью команды **clear vlan 2**. Важно отметить, что эта команда должна быть выполнена на коммутаторе VTP-сервера. На коммутаторе клиента VTP удалить VLAN-сеть невозможно. Если коммутатор с конфигурирован в прозрачном режиме, то VLAN-сеть удалить можно, однако при этом VLAN-сеть будет удалена только на самом коммутаторе Catalyst, но не во всем домене управления. Все операции по добавлению и удалению VLAN-сетей на прозрачном коммутаторе имеют лишь локальное значение. Домены VTP описаны в главе 10.

ПРИМЕЧАНИЕ

При удалении сети VLAN все назначенные ей порты перестают быть активными. Эти порты остаются логически связанными с данной сетью VLAN до тех пор, пока они не будут назначены новой VLAN-сети.

Пример 9.3 Конфигурирование коммутатора

```

Console>(enable) clear vlan 2
This command will deactivate all ports on vlan2
in the entire management domain
Do you want to continue (y/n) [n]?y
Vlan 2 deleted

```

Удаление VLAN-сети с интерфейса командно-программируемого коммутатора Cisco аналогично удалению команды из конфигурации маршрутизатора. В предыдущем примере была создана сеть vlan 2 на порте FastEthernet 0/3 с помощью команды:

```
Switch(config-if)#switchport access vlan 2
```

Для удаления с интерфейса VLAN-сети используется форма этой команды с ключевым словом **no** для интерфейса Fa 0/3:

```
Switch(config-if)#no switchport access vlan 2
```

**Лабораторная работа: удаление конфигурации VLAN-сети**

В этой лабораторной работе требуется создать базовую конфигурацию коммутатора и две виртуальных локальных сети VLAN. После этого VLAN-сетям следует присвоить имена и назначить им несколько портов. После этого их следует удалить. Следует попытаться удалить сеть VLAN1 и убедиться, что это невозможно. Пояснить причины этого.

Устранение ошибок в конфигурации VLAN-сети

В сетях, основанных на коммутации, одной из типичных ошибок является неправильное конфигурирование сетей VLAN. В табл. 9.2 описаны типичные проблемы, связанные с конфигурированием VLAN-сетей, которые могут возникнуть на маршрутизаторе или коммутаторе.

Таблица 9.2. Возможные проблемы в сети VLAN

Проблема	Возможные причины и действия, которые следует предпринять
Сеть функционирует медленно и ненадежно	Сетевой адаптер устройства неисправен. Следует проверить исправность аппаратных устройств. Установка дуплексного (<i>Full-duplex</i>) или полудуплексного режима (<i>half-duplex</i>) Ethernet выполнена с ошибками. Есть проблемы с кабелями. Следует проверить подсоединенные LED. Следует также проверить правильность подсоединения кабеля и не превышает ли длина кабеля допустимого максимального значения.
Подсоединенный терминал или модем не может осуществлять связь с маршрутизатором или коммутатором.	Неправильно сконфигурирован терминальный или консольный порт. Следует проверить правильность задания скорости перелачи (бод/с) и соответствие форматов символов. Также следует проверить, не требуется ли на маршрутизаторе стандартный маршрут для связи с коммутатором в другой IP-подсети.
Устройства локальной VLAN не могут осуществлять связь с удаленными устройствами VLAN сети вне маршрутизатора.	Имеется проблема несовместимости VLAN-сетей. Следует проверить соответствие VLAN-сетей на обеих сторонах магистрали. Есть проблема с ISL. Следует проверить магистраль, использовать сеть VLAN1 и убедиться, что не было действительного обновления информации VTP-сервера.

При наличии проблемы с низкой пропускной способностью сети следует выяснить тип ошибки. Возможно, что неисправен сетевой адаптер. Сочетание ошибки *в контрольной последовательности фрейма (frame check sequence — FCS)* с наличием фреймов-карликов, как правило, указывает на несоответствие дуплексного режима; обычно причиной является неправильное автосогласование или несоответствие установок на концах канала. Рассмотрим следующие вопросы.

- Где возникла проблема — на ближнем или на удаленном конце канала? Следует помнить о том, что в работе канала участвует минимальное количество портов.
- Какой путь избирает пакет? Избирает ли он в качестве маршрута к другим коммутаторам магистраль (или немагистральный канал)?

Если количество коллизий, указываемое в выводе по команде **show interface** быстро возрастает, то проблема может состоять в перегруженности канала. Существует ошибочное мнение, что в сетях Ethernet с коммутацией отсутствуют коллизии. На самом деле коммутаторы минимизируют количество коллизий, но если они работают в полудуплексном режиме, то коллизии все же могут происходить, поскольку два устройства, работающие в полудуплексном режиме могут попытаться начать передачу одновременно.

Примером может служить сервер новостей, имеющий много клиентов, пытающихся передавать данные в одно и то же время. Потоки данных проходят через маршрутизатор и коммутатор к непосредственно подсоединенному серверу. В то же самое время сервер пытается сам передавать данные этим клиентам. В то время как сервер отвечает одному клиенту, другой клиент посылает запрос и в результате становится потенциально возможной коллизия. Единственным способом полностью исключить возможность коллизии является использование дуплексного режима. На рис. 9.16 показан процесс поиска и устранения ошибок в сети VLAN.

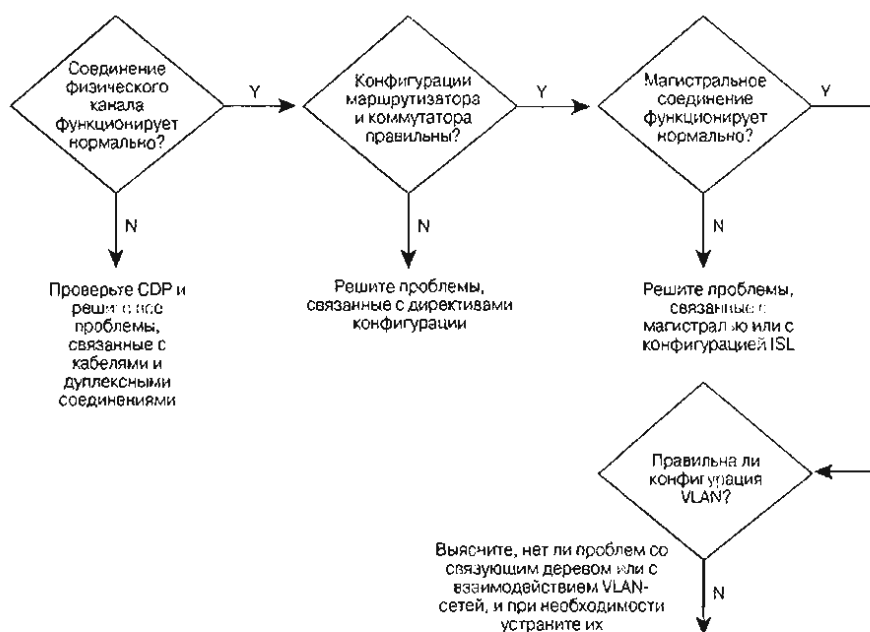


Рис. 9.16. Поиск и устранение ошибок в сети VLAN

В качестве примера рассмотрим ситуацию, когда одному устройству не удастся установить связь с другим устройством. Ниже приводятся возможные способы решения этой проблемы.

- Сначала с помощью команды **show interface** следует проверить правильность задания IP-адресов, маски подсети и задание принадлежности к сети VLAN. Для предотвращения конфликтов следует проверить, что интерфейсы сконфигурированы с IP-адресами и масками подсетей в различных подсетях.
- Если узел находится в той же подсети где и интерфейс коммутатора, то следует убедиться, что интерфейс коммутатора и порт коммутатора, к которому подсоединен этот узел, назначены в одну и ту же виртуальную сеть. Для этого следует использовать команды **show interface** и **show port**.
- Если узел находится в другой подсети, то следует проверить, что стандартный шлюз (маршрут по умолчанию) на коммутаторе сконфигурирован с адресом маршрутизатора в той же самой подсети, где находится и интерфейс коммутатора. Для этого используется команда **show ip route**.
- Далее следует проверить состояние протокола связующего дерева на данном порте с помощью команды **show spantree** (для коммутатора Catalyst 1900) или **show spanning-tree vlan** (для коммутатора Catalyst 2950). Если порт находится в состоянии прослушивания или изучения топологии, то следует подождать его перехода в режим пересылки и попытаться вновь подсоединиться к узлу.
- Проверить правильность установок скорости и типа дуплексного режима на узле и соответствующем коммутаторе. Для этого следует использовать команду **show port**.
- Если подсоединенное устройство является конечной станцией, то следует выполнить следующие действия:
 - Включить на порте режим PortFast протокола связующего дерева. Для этого используется команда **set spantree portfast enable**. Следует помнить, что эти команды не поддерживаются на коммутаторах серии 2900. Применение PortFast немедленно переводит коммутатор в режим пересылки, пропуская режимы прослушивания и изучения топологии. (Не следует использовать эту функцию для соединения с устройствами, которые не являются конечными станциями)
 - Отключить на порте магистральный режим с помощью команды **set trunk**.
 - Отключить на порте каналы. Для этого используется команда **set port channel**. В этой команде следует указать действительный диапазон портов. Нельзя задавать только один порт.
- Следует проверить, что коммутатор изучает MAC-адрес узла. Для этого используется команда **show cam dynamic**.

Резюме

В данной главе было показано, что реализация VLAN-сетей предоставляет пользователю следующие преимущества:

- облегчается перемещение, добавление устройств и изменение их соединений друг с другом;

- достигается большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на 3-м уровне;
- уменьшается потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена;
- сокращается непроизводительное использование процессора CPU за счет сокращения пересылки широковещательных сообщений;
- для поиска и устранения ошибок в сетях VLAN были предложены приведенные ниже методы;
- конкретный подход к поиску и устранению ошибок в сетях VLAN;
- рассмотрены наиболее общие проблемы при конфигурировании VLAN-сетей и предложены методы поиска и устранения ошибок в них;
- предотвращение широковещательных штормов и предотвращение петель;
- описано применение команд поиска и устранения ошибок;

В дополнение к материалу, изложенному в настоящей главе, рекомендуется ознакомиться с лабораторными работами (c-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

Виртуальная локальная сеть (virtual local-area network — VLAN). Группа устройств одной или более локальных сетей LAN, которые конфигурируются (с использованием управляющего программного обеспечения) таким образом, чтобы они могли осуществлять связь между собой как если бы они находились в одном сегменте локальной сети, в то время как они фактически находятся в различных сегментах.

Дуплексная передача (full-duplex). Одновременная передача данных принимающим и передающим устройствами.

Контрольная последовательность фрейма (frame check sequence — FCS). Дополнительные символы, добавляемые к фрейму для контроля ошибок при передаче.

Магистральный протокол виртуальных локальных сетей (VLAN Trunking Protocol — VTP). Протокол VTP позволяет уменьшить объем административных работ в сети с коммутацией. При конфигурировании новой VLAN-сети на сервере VTP сеть VLAN распределяется по всем коммутаторам домена. Это избавляет от необходимости конфигурировать одну и ту же сеть VLAN во всех локальных сетях. Протокол VTP является фирменным протоколом Cisco, который имеется на большинстве коммутаторов Catalyst Cisco.

Полудуплексная передача (half-duplex). Передача данных между принимающей и передающей станциями только в одном направлении.

Протокол обнаружения устройств Cisco (Cisco Discovery Protocol — CDP). Этот протокол содержит одну фирменную команду, позволяющую сетевому администратору получить доступ к набору конфигураций на других, непосредственно подсоединенных маршрутизаторах.

Широковещание (broadcast). Рассылка пакетов данных всем узлам сети. Широковещательные пакеты идентифицируются широковещательным адресом.

Контрольные вопросы

1. Для чего используются адреса VLAN?
 - A. Для обеспечения масштабируемости сети
 - B. Для обеспечения безопасности сети
 - C. Для управления потоками данных
 - D. Все вышеперечисленное
2. Что из перечисленного ниже характерно для сетей VLAN?
 - A. Широковещательный домен
 - B. Коллизионный домен
 - C. Одновременно широковещательный и коллизионный домен
 - D. Имя домена
3. Какова цель использования маршрутизаторов в топологиях сетей VLAN?
 - A. Фильтрация широковещания
 - B. Безопасность сети
 - C. Управление потоками данных
 - D. Все вышеперечисленное
4. Что означает фраза: “Микросегментация вместе с масштабируемостью”?
 - A. Возможность увеличивать размер сети без создания коллизионных доменов
 - B. Возможность подключения огромного количества станций к одному коммутатору
 - C. Возможность широковещания одновременно на несколько узлов
 - D. Все вышеперечисленное
5. Являясь базовым элементом VLAN-сетей, коммутаторы обладают интеллектуальными возможностями для выполнения следующих функций:
 - A. Они группируют пользователей, порты и логические адреса в сети VLAN.
 - B. Они выполняют фильтрацию и принимают решения о пересылке фреймов.
 - C. Они осуществляют связь между коммутаторами и маршрутизаторами.
 - D. Все вышеперечисленное.
6. Каждый сегмент _____, подсоединенный к порту _____ может быть причислен только к одной сети VLAN.
 - A. Коммутатора; концентратора
 - B. концентратора; маршрутизатора
 - C. концентратора; коммутатора
 - D. сети LAN; концентратора
7. Что из перечисленного ниже не является преимуществом статических VLAN-сетей?
 - A. Они гарантируют безопасность.
 - B. Их легко конфигурировать.

- C. За ними легко осуществлять наблюдение (мониторинг).
 - D. Они автоматически конфигурируют порты при добавлении новых станций.
8. Что из перечисленного ниже не является критерием, на котором могут базироваться сети VLAN?
- A. Идентификатор ID порта.
 - B. Протокол.
 - C. MAC-адрес.
 - D. Все вышеперечисленные элементы являются критериями на которых могут базироваться сети VLAN.
9. Что из перечисленного ниже является положительным результатом добавления сети VLAN? (Выбрать все правильные ответы).
- A. Коммутаторы не требуют конфигурирования.
 - B. Возможно управление широковещанием.
 - C. Возможна защита конфиденциальных данных.
 - D. Могут быть удалены физические границы, препятствующие группировке пользователей.
10. Какие из приведенных ниже утверждений, относящиеся к виртуальным локальным сетям, не являются справедливыми?
- A. Наиболее общими подходами к логической группировке пользователей в отдельные VLAN-сети являются фильтрация и идентификация фреймов.
 - B. Преимущества сетей VLAN включают в себя более надежную защиту сети и создание безопасных групп пользователей.
 - C. Мосты являются одним из базовых компонентов коммуникации в сетях VLAN.
 - D. VLAN-сети помогают осуществлять перераспределение нагрузки.
11. Какая функция коммутатора 3-го уровня позволяет легко управлять устройствами, расположенными в различных IP-подсетях?
- A. Создание прозрачных мостовых соединений
 - B. Сегментация
 - C. Сокращение числа коллизийных доменов
 - D. Создание сетей VLAN
12. Какое из перечисленных ниже устройств требуется для передачи пакета из одной сети VLAN в другую?
- A. Мост
 - B. Маршрутизатор
 - C. Коммутатор
 - D. Концентратор
13. На каком уровне эталонной модели OSI происходит добавление к фрейму тега?
- A. На 1-м уровне
 - B. На 2-м уровне
 - C. На 3-м уровне
 - D. На 4-м уровне

14. _____ позволяет коммутаторам совместно использовать таблицы адресов, а _____ назначает определенные пользователем идентификаторы ID сетей VLAN каждому фрейму.
- A. Присоединение тегов; пересылка фреймов
 - B. Идентификация фреймов; удаление фреймов
 - C. Фильтрация фреймов; присоединение тегов
 - D. Присоединение тегов; фильтрация фреймов
15. В чем состоит важность создания VLAN-сетей?
- A. Становятся более простыми удаление, добавление устройств и другие перемены в сети.
 - B. Уменьшается объем передаваемых служебных данных.
 - C. Маршрутизатор быстрее осуществляет коммутацию.
 - D. А и B.



В этой главе...

- Описаны магистральные соединения
- Рассмотрены основы протокола VTP и его конфигурирование
- Рассмотрена маршрутизация между VLAN-сетями
- Описано конфигурирование маршрутизации между VLAN-сетями

Магистральный протокол VLAN

В данной главе будет рассмотрено происхождение магистралей и их функционирование. Также будет описано, как магистральный протокол VLAN-сетей (VLAN Trunking Protocol — VTP) может решить некоторые проблемы, связанные с управлением и реализацией виртуальных локальных сетей (virtual LAN — VLAN) в среде крупной локальной сети LAN. В заключение будут приведены начальные сведения о маршрутизации между VLAN-сетями.

Рекомендуется выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Магистральные соединения

История *магистральных соединений (trunking)* уходит своими корнями в радио- и телефонные технологии. В радиотехнологиях под магистралью понимается отдельная линия связи, по которой передается информация нескольких каналов радиосигналов.

В телефонии понятие магистрали связано с маршрутом телефонной связи или каналом между двумя точками (одним из которых обычно является центральная АТС). Пример магистрали приведен на рис. 10.1.

Магистрали общего пользования могут быть созданы для создания избыточности при связи между центральными АТС (central offices — CO) (рис. 10.2)

То же понятие магистрали, которое использовалось в телефонии и радиоиндустрии, было принято в аппаратном обеспечении телекоммуникаций. Примером этого может служить сегмент сети связи, в котором сходится несколько каналов, как показано на рис. 10.3. Магистраль состоит из нескольких магистральных каналов.

В настоящее время этот же принцип создания магистралей применяется в технологиях коммутации, в которых под магистралью понимается физическое и логическое соединение между двумя коммутаторами, по которому передаются данные между сетями.

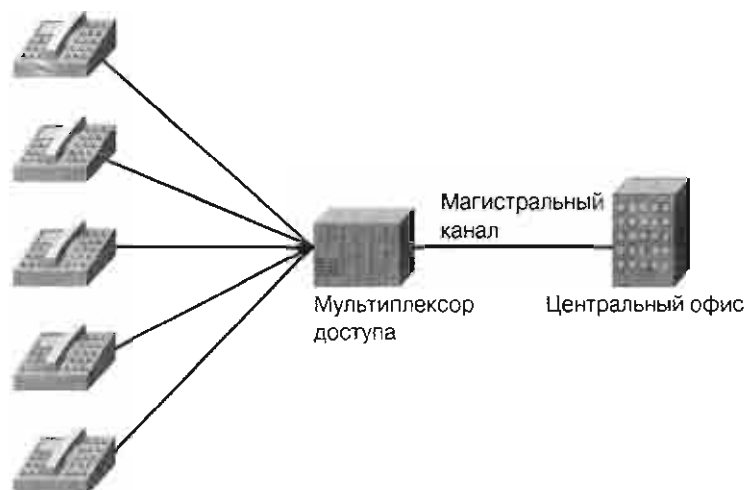


Рис. 10.1. Магистральный канал

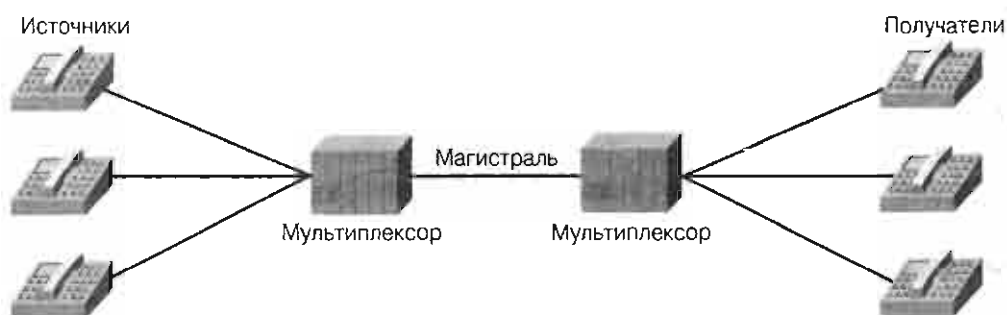


Рис. 10.2. Общий магистральный канал

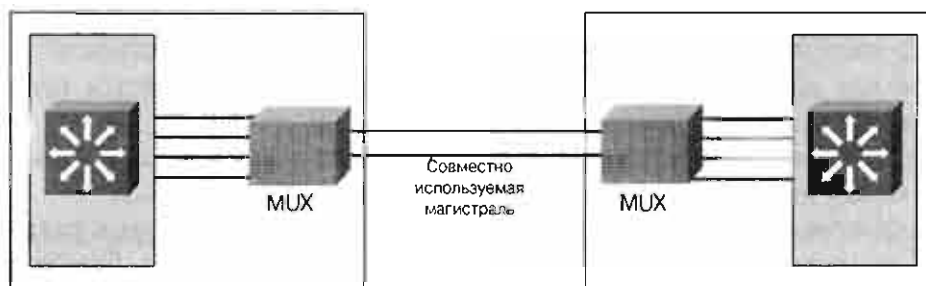


Рис. 10.3. Магистральные каналы, использующие мультиплексирование с разделением фреймов

Понятие магистралей

Под *магистралью (trunk)* понимается отдельный канал передачи между двумя точками, которыми обычно являются центры коммутации. Магистраль представляет собой физическое соединение, по которому проходят логические каналы.

В контексте среды коммутации VLAN-сетей магистраль является каналом типа "точка-точка", который поддерживает несколько VLAN-сетей. Целью использования магистралей является экономия портов при создании канала связи между двумя устройствами, реализующими VLAN-сети, обычно этими устройствами являются два коммутатора. На рис. 10.4 показаны две VLAN-сети, которые выходят на коммутаторы Sa и Sb.

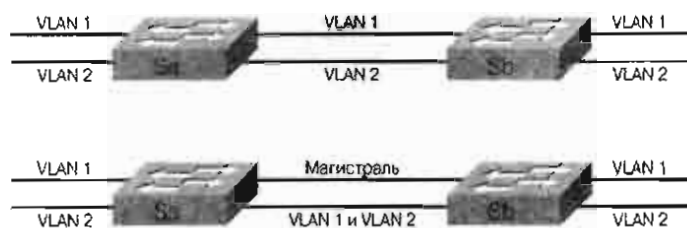


Рис. 10.4. Зачем нужна магистраль?

При использовании первого подхода, проиллюстрированного на рис. 10.4, создаются два физических канала между устройствами, по каждому из которых передаются данные для отдельной VLAN-сети. Такое решение трудно масштабировать. При добавлении третьей VLAN-сети придется пожертвовать двумя портами. Такой подход неэффективен также в плане распределения нагрузки, поскольку использование отдельного выделенного канала для некоторых VLAN может оказаться неоправданным. Магистраль объединяет несколько виртуальных (логических) каналов в один физический канал.

Функционирование магистралей

По мере увеличения числа VLAN-сетей, данные которых передаются по магистральной, использование существующих обычных таблиц коммутации на обоих концах магистралей, основанных на MAC-адресах, находящихся в передаваемых фреймах, становится медленным и сложным. Чем больше размер таблицы, которую требуется хранить коммутатору, тем медленнее становится процесс принятия решения об отправке фреймов на соответствующие порты. Для эффективного управления передачей фреймов от различных VLAN-сетей по одному физическому каналу или линии между двумя сетевыми устройствами требуется новый способ связи или язык коммуникации между этими двумя устройствами. Такой способ связи или протокол, используется для того, чтобы эти устройства могли «договориться» о передаче и последующем распределении фреймов на соответствующие порты на обоих концах магистралей. Для этой цели были созданы различные магистральные протоколы.

Эти магистральные протоколы позволяют осуществлять передачу фреймов от различных VLAN-сетей по одному физическому каналу; они также управляют распределением фреймов на соответствующие логически связанные VLAN-порты. В настоящее время применяются два магистральных механизма: фильтрация фреймов и добавление к ним тегов. В настоящей главе рассматривается механизм добавления тегов поскольку этот метод является стандартным магистральным механизмом, рекомендуемым IEEE. На рис. 10.5 приведен пример магистральных каналов.

В магистральных протоколах используется механизм добавления тегов, который назначает фреймам некоторый идентификатор, что облегчает управление этими фреймами и, соответственно, ускоряет их доставку получателям. Теги добавляются к фреймам на одном конце магистралей и удаляются на другом. Такие фреймы не являются широковековыми (т.е. предназначены только одному устройству на другом конце магистрального канала).

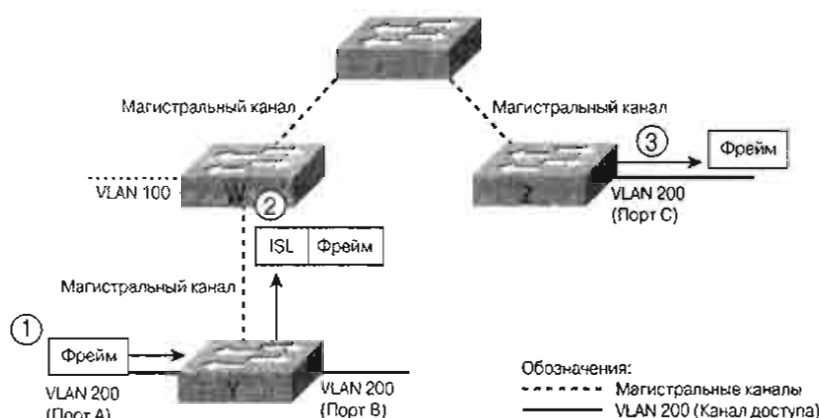


Рис. 10.5. Магистральные каналы

Уникальный физический канал между двумя коммутаторами может передавать данные, предназначенные для любой VLAN-сети. Существуют различные схемы добавления тегов. Наиболее часто используемые в Ethernet-сегментах схемы описаны ниже.

- *Протокол межкоммутаторного канала (Inter-Switch Link — ISL).* Фирменный первоначальный протокол межкоммутаторного канала Cisco;
- *802.1Q.* Стандартный метод IEEE добавления к фреймам Ethernet информации о принадлежности к некоторой VLAN-сети.

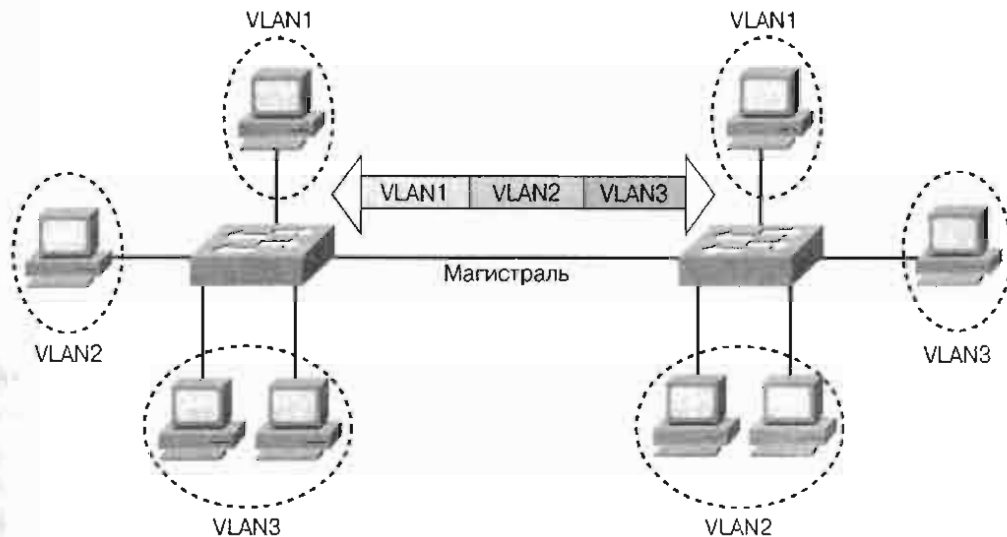
Сети VLAN и магистральные каналы

Для реализации магистральных соединений требуется соблюдать некоторые правила или протоколы. Механизмы магистральных соединений облегчают расширение VLAN-сетей, использующих коммутацию. Сеть VLAN представляет собой группу устройств одной или более локальных сетей LAN, которые сконфигурированы (с использованием управляющего программного обеспечения) таким образом, чтобы они могли осуществлять между собой связь как если бы они были подключены к общей шине, тогда как в действительности они расположены в различных LAN-сегментах. Использование магистралей предоставляет эффективный метод распределения ID-информации VLAN сетей другим коммутаторам и связи между коммутаторами, как показано на рис. 10.6.



Рис. 10.6. Сети VLAN и магистральные каналы

Присвоение тегов является стандартным механизмом магистральных соединений: по сравнению с фильтрацией фреймов присвоение тегов предоставляет большие возможности масштабирования при реализации VLAN-сетей, которые могут быть реализованы в сети кампуса. Спецификация IEEE 802.1Q определяет присвоение тегов как способ реализации VLAN-сетей. Пример присвоения тегов приведен на рис. 10.7.

*Рис. 10.7. Присвоение тегов*

Метод присвоения тегов фреймам виртуальных сетей VLAN был специально разработан для коммутируемых соединений. Операция добавления тега заключается в размещении в заголовке каждого фрейма уникального идентификатора для передачи его по сетевой магистрали. Каждый коммутатор просматривает и анализирует этот идентификатор перед тем как рассылать его широковещательно или передать другим коммутаторам, маршрутизаторам или конечным станциям. Когда фрейм покидает сетевую магистраль, коммутатор удаляет идентификатор перед отправкой этого фрейма конечной станции-получателю. Идентификация фреймов осуществляется на 2-м уровне и не требует трудоемкой обработки или передачи служебной информации.

Магистральный канал не принадлежит ни одной конкретной VLAN-сети. Назначение магистрального канала состоит в том, чтобы обеспечить канал связи между коммутаторами и маршрутизаторами для VLAN-сетей.

Коммутаторы на рис. 10.6 осуществляют связь друг с другом, используя протокол ISL, поддерживающий информацию о VLAN-сетях при передаче данных между коммутаторами. При использовании протокола ISL фрейм Ethernet инкапсулируется с заголовком, который содержит ID сети VLAN.

Интерфейс командной строки коммутатора

В зависимости от модели коммутатора могут встретиться два типа ввода команд. Интерфейс командной строки (Command-Line Interface — CLI) для коммутаторов Cisco может основываться на наборе команд IOS Cisco или на специальном наборе команд. В первом случае используется набор команд, аналогичный командам IOS Cisco. Во втором случае используется специальный набор команд конфигурирования коммутатора. Наборы команд для этих двух типов CLI могут различаться. Оба типа команд используются в приведенных ниже примерах конфигурации. Коммутаторы серии 2900 используют команды IOS Cisco. Коммутаторы серий 4500 и 6500 используют команды из специального набора. Прежние модели коммутаторов, такие как коммутаторы серии 1900 используют команды IOS, а также имеют основанный на меню интерфейс. Все модели коммутаторов имеют управляющий графический Web-интерфейс, к которому можно получить доступ из браузера. Ниже приводится

командная строка привилегированного режима коммутатора, использующего команды IOS Cisco и пример команды:

```
Switch#show trunk
```

Ниже приводится командная строка привилегированного режима коммутатора, использующего специальный набор команд и пример команды:

```
Switch>(enable)set vtp v2 enable
```

Реализация магистральных соединений

Для создания или конфигурирования магистрального VLAN-соединения на коммутаторе, использующем команды IOS Cisco, следует сначала сконфигурировать этот порт как магистральный, а затем указать тип инкапсуляции в этой магистральной. Тип инкапсуляции должен быть одним и тем же на обоих концах магистральной. Для решения этой задачи необходимо выполнить команды, показанные в примере 10.1.

Пример 10.1. Команды конфигурирования VLAN-магистральной

```
Switch(config-if)#switchport mode trunk ?
allowed Set allowed VLAN characteristics when interface is in trunk-
ing
mode
encapsulation Set trunking encapsulation when interface is in trunk-
ing mode
native Set Set trunking native characteristics when interface is in
trunking
mode
pruning Set pruning VLAN characteristics when interface is in trunk-
ing mode
Switch(config-if)#switchport trunk encapsulation ?
dot1q Interface uses only 802.1q trunking encapsulation when trunk-
ing
isl Interface uses only ISL trunking encapsulation when trunking
Switch(config-if)#switchport trunk encapsulation isl
```



Лабораторная работа: магистральное соединение протокола ISL

В этой лабораторной работе требуется создать на коммутаторе базовую конфигурацию, затем создать несколько VLAN-сетей, дать им имена и назначить им соответствующие порты. После этого требуется создать магистральное соединение между двумя VLAN-сетями и протестировать их работу путем перемещения рабочей станции из одной VLAN-сети в другую.

Перед конфигурированием VLAN-магистральной на порте коммутатора необходимо выяснить, какой тип инкапсуляции поддерживается этим портом. Это можно сделать, выполнив команду **show port capabilities** на коммутаторе, использующем специальный набор команд, как показано в примере 10.2. Следует обратить внимание на то, что порт 2/1 поддерживает только инкапсуляцию IEEE 802.1Q.

Пример 10.2. Команда show port capabilities

```
Console>(enable)show port capabilities 2/1
Model WS-X4232-GB-RJ
Port 2/1
Type No GBIC
Speed 1000
Duplex full
Trunk encap type 802.1Q
Trunk mode on,off,desirable,auto,nonegotiate
Channel 2/1-2
Flow control receive-(off,on,desired),send-(off,on,desired)
Security yes
Membership static,dynamic
Fast start yes
QoS scheduling rx-(none), tx-(2q1t)
CoS rewrite no
ToS rewrite no
Rewrite no
UDLD yes
SPAN source,destination
```

Для создания или конфигурирования магистрального VLAN-соединения на коммутаторе, использующем специальный набор команд, следует выполнить команду **set trunk** для конфигурирования портов на обоих концах канала как магистральных и указать VLAN-сети, данные которых будут передаваться по этому магистральному каналу:

```
Switch> (enable) set trunk mod_num/port_num [on | off | desirable |
auto | nonegotiate] vlan_range [isl | dot1q | dot10 | lane | negotiate]
```

Команда **set trunk** может быть также использована для изменения режима работы магистралей, как показано в примере 10.3.

Пример 10.3 Команда set trunk

```
Console>(enable)
Console>(enable)set trunk 2/1 on dot1q
Port(s) 2/1 trunk mode set to on.
Port(s) 2/1 trunk type set to dot1q
```

Ключевыми словами для магистральных режимов технологий Fast Ethernet и Gigabit Ethernet являются следующие:

- **on**. Этот режим переводит порт в постоянное состояние магистрального соединения. Порт становится магистральным даже в том случае, если соседний порт не соглашается на такое изменение. Состояние **on** не позволяет обсуждать тип инкапсуляции; следовательно тип инкапсуляции должен быть указан в конфигурации.
- **off**. Этот режим переводит порт в постоянное немагистральное состояние; при этом обсуждается преобразование канала в немагистральный. При этом порт становится не магистральным даже в том случае, если соседний порт не согласен на такое изменение.

- **desirable**. В этом режиме порт предпринимает попытку преобразовать канал в магистральный. Порт становится магистральным, если соседний порт находится в режимах **on**, **desirable** или в режиме **auto**.
- **auto**. В этом режиме порт намеревается преобразовать канал в магистральный. Порт становится магистральным, если соседний порт находится в режимах **on** или **desirable**. Этот режим является режимом по умолчанию для портов Fast и Gigabit Ethernet. Следует обратить внимание на то, что если на обоих концах магистрального канала приняты установки по умолчанию, то он не станет магистральным, поскольку ни одна из сторон не сделает первой запроса на его преобразование.
- **nonegotiate**. В этом режиме порт переводится в постоянное состояние магистрального, однако не генерирует фреймы протокола динамического магистрального соединения (Dynamic Trunking Protocol — DTP). Для установки магистрального канала необходимо вручную сконфигурировать соседний порт как магистральный.

Проверить правильность установки магистрального соединения и его параметры можно с помощью команды:

```
show trunk [mod_num/port_num]
```

в привилегированном режиме конфигурирования коммутатора.

Протокол магистральных соединений виртуальных локальных сетей VLAN

В настоящем разделе описывается протокол магистральных соединений виртуальных сетей VLAN (VLAN Trunking Protocol — VTP), его функционирование и реализация коммутируемой среды виртуальных локальных сетей VLAN.

История протокола VTP

Протокол VTP был создан для решения возможных проблем в среде коммутации виртуальных локальных сетей VLAN.

Например, рассмотрим домен, в котором имеются несколько связанных друг с другом коммутаторов, которые поддерживают несколько VLAN-сетей. Для создания и поддержки соединений внутри VLAN-сетей каждая из них должна быть сконфигурирована вручную на каждом коммутаторе. По мере роста организации и увеличения количества коммутаторов в сети, каждый новый коммутатор должен быть сконфигурирован вручную с вводом информации о VLAN-сетях. Всего лишь одно неправильное назначение в сети VLAN может вызвать две потенциальных проблемы.

- Перекрестное соединение VLAN-сетей вследствие несогласованности в конфигурации VLAN-сетей;
- Согласование и ликвидация противоречивости конфигураций в смешанной среде передачи, например, в среде, включающей в себя сегменты Ethernet и Fiber Distributed Data Interface (FDDI).

В протоколе VTP согласованность конфигураций VLAN-сетей поддерживается в общем административном домене. Кроме того, протокол VTP уменьшает сложность управления и мониторинга VLAN-сетей.

Общие положения протокола VTP

Назначение протокола VTP состоит в поддержке согласованности конфигураций в общем административном сетевом домене. Протокол VTP является протоколом обмена сообщениями, использующим магистральные фреймы 2-го уровня для управления добавлением, удалением и переименованием VLAN-сетей в одном домене.

Кроме того, протокол VTP позволяет осуществлять централизованные изменения в сети, о которых сообщается всем другим коммутаторам сети.

Сообщения протокола VTP инкапсулируются в фирменные фреймы протоколов ISL или IEEE 802.1Q и передаются далее по магистральным каналам другим устройствам. К фреймам IEEE 802.1Q в качестве тега добавляются 4-байтовое поле. В обоих форматах передается идентификатор ID VLAN-сети.

В то время как порты коммутаторов обычно назначаются только одной VLAN-сети, магистральные порты, по умолчанию, передают фреймы всем VLAN-сетям.

Преимущества использования протокола VTP

Протокол VTP позволяет свести к минимуму возможную рассогласованность конфигураций, которая возникает при изменении топологии сети. Эта несогласованность может привести к снижению защищенности сети, поскольку перекрестное соединение VLAN-сетей при использовании дублирующих имен может привести к внутреннему разединению при преобразовании от одного типа LAN к другому (например, от Ethernet к ATM или FDDI).

Использование протокола VTP предоставляет следующие преимущества.

- Поддержка согласованности конфигураций VLAN-сетей во всей объединенной сети.
- Поддержка схемы преобразования, которая позволяет VLAN-сети осуществлять магистральное соединение по смешанной среде, например, преобразование VLAN-сети в высокоскоростную магистральную VLAN-сеть LANE ATM или FDDI.
- Точное отслеживание и мониторинг VLAN-сетей.
- Динамическое оповещение всех устройств сети о добавлении новой VLAN-сети.
- Конфигурирование режима “Plug-and-play” при добавлении новой VLAN-сети.

Перед созданием на коммутаторе VLAN-сети необходимо сначала создать домен управления протокола VTP, в котором можно протестировать созданную VLAN-сеть. Все коммутаторы в одном и том же домене управления, которые совместно используют информацию о VLAN-сетях. Коммутатор может присутствовать только в одном домене управления протокола VTP. Находящиеся в разных доменах коммутаторы не могут совместно использовать информацию протокола VTP.

В протоколе VTP каждый коммутатор семейства Catalyst передает со своих магистральных портов следующую информацию:

- домен управления;

- номер версии конфигурации;
- известные VLAN-сети и их конкретные параметры.

Домен протокола VTP

Домен протокола VTP состоит из одного или более соединенных между собой устройств, совместно использующих доменное имя протокола VTP. Коммутатор может принадлежать только одному домену протокола VTP.

При передаче сообщений протокола VTP другим коммутаторам сети происходит инкапсуляция этих сообщений во фреймы магистрального протокола, такого как ISL или IEEE 802.1Q. На рис. 10.8 обобщенно показан процесс инкапсуляции данных протокола VTP во фрейм протокола ISL.



Рис. 10.8. Инкапсуляция сообщений протокола VTP во фрейм протокола ISL

Заголовок протокола VTP изменяется в зависимости от типа сообщения, однако, в нем, как правило, присутствуют следующие четыре поля:

- версия протокола VTP — Версия 1 или 2;
- тип сообщения VTP — Один из четырех типов;
- длина имени домена управления — Указывает длину имени домена, которое следует за этим полем;
- имя домена управления — В этом поле содержится имя домена управления, заданное в конфигурации.

Режимы протокола VTP

Протокол VTP может работать в одном из трех режимов:

- режим сервера;
- режим клиента;
- прозрачный режим.

Режим сервера протокола VTP (стандартный)

Если коммутатор сконфигурирован в режиме сервера, то можно создавать, изменять или удалять VLAN-сети и другие параметры конфигурации (такие, как версия протокола VTP или отсечение VTP) для всего VTP-домена. Серверы VTP сохраняют информацию конфигурации VLAN в энергонезависимой оперативной памяти (nonvolatile random-access memory — NVRAM). VTP-серверы рассылают сообщения протокола VTP со всех своих магистральных портов. Они анонсируют конфигурацию своих VLAN-сетей всем коммутаторам своего VTP-домена и согласовывают конфигурацию своих VLAN-сетей с другими коммутаторами на базе анонсирований, полученных от них по магистральным каналам. Такой режим является для магистрального коммутатора режимом по умолчанию.

Режим клиента протокола VTP

Коммутатор, который сконфигурирован как клиент протокола VTP, не может создавать сети VLAN, изменять их или удалять. Кроме того, коммутатор-клиент не может сохранять информацию о VLAN-сетях. Этот режим целесообразно использовать для коммутаторов, которые не имеют достаточной памяти для хранения больших таблиц VLAN-сетей, что требуется для серверов VTP. Клиенты VTP обрабатывают изменения в сетях VLAN, как это делают серверы, и рассылают сообщения протокола VTP со всех своих магистральных портов.

Прозрачный режим протокола VTP

Коммутаторы, сконфигурированные для прозрачного режима, не принимают участия в работе протокола VTP. Коммутатор, работающий в прозрачном режиме, не анонсирует конфигурацию своей VLAN-сети, и не согласовывает конфигурацию своей сети VLAN в соответствии с получаемыми анонсирующими сообщениями. Такие коммутаторы рассылают сообщения, анонсируемые другими устройствами протокола VTP (версия 2), полученные на их магистральных портах, но не анализируют содержащуюся в этих сообщениях информацию. В прозрачном режиме коммутатор не изменяет свою базу данных при получении сообщений об изменении топологии и не рассылает сообщений об изменении топологии своей собственной VLAN-сети. За исключением рассылки анонсирований протокола VTP коммутатор в прозрачном режиме не участвует в работе протокола VTP.

Функционирование протокола VTP

Получение в анонсированиях сообщения о добавлении VLAN-сети служит уведомлением для коммутаторов (как серверов, так и клиентов) о том, что они должны быть готовы к получению на своих магистральных портах сообщений о новых идентификаторах ID VLAN-сетей, об именах эмулированных LAN-сетей или об идентификаторах параметров безопасности (security association identifiers — SAID) спецификации 802.10. На рис. 10.9 коммутатор Switch С передает запись своей базы данных протокола VTP с добавленными или удаленными позициями коммутаторам Switch А и Switch В. Конфигурационная база данных имеет номер версии, который равен номеру уведомления +1.

Большой номер версии указывает на то, что рассылаемая информация о VLAN-сетях является более новой, чем хранящаяся в данный момент. Когда коммутатор получает сообщение об обновлении топологии с более высоким номером версии конфигурации, он переписывает хранящуюся у него информацию и заменяет ее новой, содержащейся в обновлении VTP. Коммутатор не обрабатывает сообщение об обновлении, поскольку оно относится к другому домену.

По умолчанию управление доменами производится без использования мер безопасности; это означает, что коммутаторы обмениваются информацией без запроса паролей. Добавление пароля автоматически переводит домен управления в безопасный режим. Такой же пароль должен быть скомфигурирован на всех коммутаторах домена для того, чтобы была возможна работа в безопасном режиме.

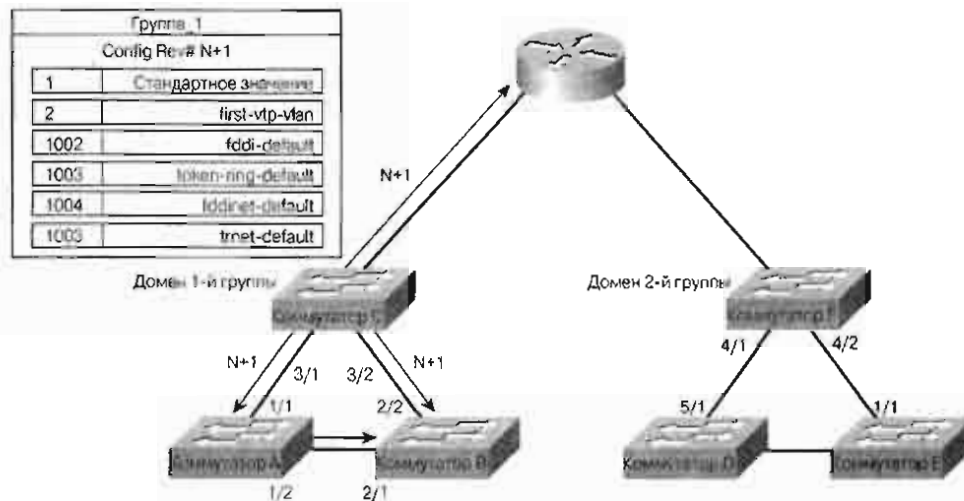


Рис. 10.9. Функционирование протокола VTP

Реализация протокола VTP

При использовании протокола VTP каждый коммутатор анонсирует на своих магистральных портах свой домен управления, номер версии конфигурации, известные ему VLAN-сети и параметры каждой известной ему сети VLAN. Эти фреймы с анонсированиями рассылаются по адресу множественной рассылки и поэтому получают всеми соседними устройствами; однако для рассылки этих фреймов не используются обычные процедуры мостовых соединений. Все устройства в одном и том же домене управления узнают обо всех новых VLAN-сетях, которые в настоящий момент конфигурируются на передающем устройстве. Новая VLAN сеть должна создаваться и конфигурироваться только на одном устройстве домена управления. Все остальные устройства этого домена автоматически получают информацию об этом.

Анонсирование VLAN-сетей с заводскими установками основано на типах передающей среды. Порты пользователя не должны конфигурироваться как магистрали протокола VTP. Каждое анонсирование начинается как версия конфигурации с номером 0. По мере того, как в конфигурацию вносятся изменения, номер версии увеличивается на единицу ($n + 1$). Номер версии в домене управления продолжает возрастать до тех пор, пока он не станет равным 2 147 483 648, после чего счетчик номера версии обнуляется.

В протоколе VTP существуют два типа анонсирований:

- запросы от клиентов, которым требуется информация при перезагрузке;
- ответы серверов.

Имеется три типа сообщений протокола VTP:

- запрос анонсирования (Advertisement request)—Клиент запрашивает информацию о VLAN-сетях;
- анонсирование общей информации (Summary advertisement)—Сервер отвечает, сообщая общую информацию.
- анонсирование подсетей (Subset advertisement)—Сервер отвечает, сообщая информацию о подсетях.

Эти три типа сообщений протокола VTP показаны на рис. 10.10.



Рис. 10.10. Запросы анонсирований

По умолчанию коммутаторы Catalyst, являющиеся серверами и клиентами протокола VTP, анонсируют общую информацию каждые пять минут. Они информируют соседние коммутаторы о том, какой номер версии VTP-конфигурации они считают текущим в настоящий момент. Предполагая, что имя домена является правильным, принимающий сервер или клиент сравнивает полученный номер версии со своим собственным. Если номер версии в анонсировании больше, чем текущий номер версии на получающем коммутаторе, то последний делает запрос на анонсирование новой информации о VLAN-сетях. На рис. 10.11 приведен пример формата общего анонсирования.

Версия	Тип	Количество анонсирований подсетей, которые следует учитывать	Длина имени домена
Имя домена управления (Дополняется нулями до 32 байтов)			
Номер изменения конфигурации			
Идентификационные данные инициатора обновления маршрутов			
Временная отметка инициатора обновления маршрутов (12 байтов)			
Дайджест MD5 (16 байтов)			

Рис. 10.11. Пример формата общего анонсирования

Анонсирования подсетей содержат подробную информацию о VLAN-сетях, такую как тип версии VTP, имя домена и связанные поля, а также номер версии конфигурации. Анонсирования такого типа могут быть вызваны такими событиями, как создание или удаление VLAN-сети, изменение имени VLAN-сети или изменение размера максимального модуля передачи (maximum transmission unit — MTU) в какой-либо из VLAN-сетей. Пример формата анонсирования подсети приведен на рис. 10.12.

Версия	Тип	Номер в последовательности	Длина имени домена
Имя домена управления (Дополняется нулями до 32 байтов)			
Номер изменения конфигурации			
1-е информационное поле VLAN 1			
⋮			
N-е информационное поле VLAN 1			

Информационное поле VLAN содержит информацию о каждой VLAN-сети и форматируется следующим образом:

Длина информационного поля	Состояние	Тип VLAN	Длина имени VLAN
VLAN-идентификатор ISL		Размер MTU	
Индекс 802.10			
Имя VLAN-сети (Дополняется нулями до кратного 4 байтам)			

Рис. 10.12. Формат анонсирования подсети

Анонсирования могут включать в себя все или некоторые из приведенных ниже полей.

- **Имя домена управления (Management domain name)** — Анонсирования, имеющие разные имена, игнорируются.
- **Номер версии конфигурации (Configuration revision number)** — Большой номер версии соответствует более поздней версии.
- **Дайджест сообщения (Message Digest 5 — MD5)** — MD5 представляет собой ключ к шифру который рассылается протоколом VTP в случае назначения пароля. Если ключ шифра не соответствует введенному, то данное обновление игнорируется.
- **Идентификация устройства, обновляющего информацию (Updater identity)** — Идентификация коммутатора, рассылающего анонсирование общей информации.

Конфигурирование протокола VTP

Ниже описаны основные вопросы, которые требуется рассмотреть перед конфигурированием протокола VTP и VLAN-сетей.

- Этап 1.** Определить, какая версия протокола VTP будет использоваться в сети.
- Этап 2.** Принять решение о том, будет ли конфигурируемый коммутатор членом уже существующего домена управления или будет создаваться новый домен. Если домен управления уже существует, то его имя и пароль должно быть задано в конфигурации.
- Этап 3.** Выбрать для коммутатора режим протокола VTP.

Конфигурирование версии протокола VTP

В домене управления протокола VTP могут работать две версии протокола VTP: версия 1 и версия 2. Эти две версии не могут интерактивно взаимодействовать. Если на одном из коммутаторов домена будет установлена версия 2 протокола VTP, то и все остальные коммутаторы этого домена управления должны быть сконфигурированы в этой версии. По умолчанию конфигурируется версия 1 протокола. Установка 2-й версии может потребоваться в том случае, если есть необходимость в особых функциях версии 2, которые отсутствуют в 1-й версии. Из этих функций чаще всего требуется поддержка VLAN-сетей Token Ring.

Для того, чтобы сконфигурировать версию протокола VTP на коммутаторе, использующем IOS Cisco, требуется сначала войти в режим базы данных VLAN-сети. Для изменения версии протокола VTP на коммутаторе, использующем специальный набор команд, следует выполнить приведенные ниже команды.

```
Switch#vlan database
Switch(vlan)#vtp v2-mode
```

Для изменения версии протокола VTP на коммутаторе, использующем специальный набор команд, следует выполнить приведенную ниже команду.

```
Switch(enable) set vtp v2 enable
```

В версии 2 протокола VTP имеются следующие функции, которые не поддерживаются в версии 1.

- **Поддержка Token Ring (Token Ring support)** — версия 2 протокола VTP поддерживает коммутацию и VLAN-сети в LAN-сетях Token Ring.
- **Поддержка функции “Не распознан тип/длина/значение” (Unrecognized type/length/value (TLV) support)** — сервер или клиент протокола VTP распространяет сообщения об изменениях топологии по своим магистральным каналам, даже для тех значений TLV, которые он не может распознать. Нераспознанные TLV сохраняются в памяти NVRAM.
- **Зависящий от версии прозрачный режим (Version-dependent transparent mode)** — в версии 1 протокола VTP находящийся в прозрачном режиме коммутатор VTP просматривает поля имени домена и версии VTP-сообщений и пересылает сообщение только в том случае, если версия и имя домена соответствуют имеющимся у него. Поскольку программным обеспечением супервизора поддерживается только один домен, в версии 2 протокола VTP VTP-сообщения в прозрачном режиме пересылаются без проверки версии протокола VTP.
- **Проверка согласованности (Consistency checks)** — в версии 2 протокола VTP проверка согласованности (в частности, имен VLAN-сетей и значений) выполняется только тогда, когда вводится новая информация через интерфейс командной строки CLI или по простому протоколу управления сетью (Simple Network Management Protocol — SNMP). Проверка согласованности не производится в тех случаях, когда новая информация получена через сообщения протокола VTP или когда она считана из памяти NVRAM. Если дайджест полученного сообщения VTP правилен, то информация этого сообщения принимается без проверки согласованности. Коммутатор, на котором работает версия 2 протокола VTP, может работать в том же самом домене, в котором работают коммутаторы версии 1, если версия 2 остается отключенной на коммутаторе с функциями 2-й версии протокола VTP.

Если все коммутаторы домена могут работать с VTP версии 2, то эту версию нужно включить только на одном коммутаторе (с помощью команды **set vtp v2 enable**). При этом номер версии будет распространен на все остальные коммутаторы этого домена с функциями VTP 2-й версии.

Конфигурирование домена протокола VTP

Если устанавливаемый коммутатор является первым коммутатором в сети, то следует создать домен управления. Если же домен уже существует, то перед добавлением нового коммутатора следует проверить его имя. Если в домене управления введены меры безопасности, то в нем следует задать пароль. Для создания домена управления необходимо выполнить следующую команду:

```
Switch(vlan)#vtp domain Cisco
```

Имя домена может иметь длину от 1 до 32 символов и чувствительно к регистру. Пароль должен иметь длину от 8 до 64 символов.

При добавлении клиента протокола VTP к существующему VTP-домену обязательно требуется проверить, что его номер версии конфигурации меньше, чем аналогичные номера у других коммутаторов данного VTP-домена. Для этого используется команда **show vtp status**. Коммутаторы VTP-домена используют конфигурацию VLAN с наибольшим номером версии VTP-конфигурации. Если номер версии конфигурации на добавляемом коммутаторе окажется большим, чем номер версии в домене, то будет стерта VLAN-информация сервера VTP и домена VTP.

Для создания домена управления или добавления коммутатора к домену управления на коммутаторе со специальным набором команд, используется следующая команда:

```
Switch(enable) set vtp domain domain_name
```

Конфигурирование режима протокола VTP

На коммутаторе может быть установлен один из трех доступных режимов протокола VTP. Ниже приведены некоторые общие рекомендации по выбору режима протокола VTP на коммутаторе.

Если устанавливаемый коммутатор является первым в домене управления и будут добавляться другие коммутаторы, то на нем следует установить режим сервера. Другие добавляемые коммутаторы будут получать VLAN-информацию от этого коммутатора. В домене должен быть хотя бы один сервер.

Если коммутатор добавляется в домен управления, в котором уже имеются коммутаторы, то на этом коммутаторе следует установить режим клиента для предотвращения распространения им некорректной информации в уже существующей сети. Если предполагается в дальнейшем использовать этот коммутатор в качестве сервера, то изменить его режим на режим сервера следует после того, как он получит корректную информацию о VLAN-сетях от других устройств сети. Если для этого коммутатора не предполагается обмена информацией о VLAN-сетях с другими коммутаторами этой сети, то на нем следует установить прозрачный режим. В прозрачном режиме можно создавать, удалять и переименовывать VLAN-сети, не сообщая информацию об этих изменениях другим коммутаторам. Если конфигурирование устройств в сети выполняется несколькими пользователями, то существует риск на-

ложения друг на друга VLAN-сетей с разными функциями в сети, но с одними и теми же идентификационными данными.

Для установки требуемого режима на коммутаторе с функциями IOS Cisco используется следующая команда:

```
Switch(vlan)#vtp {client | server | transparent}
```

Для установки требуемого режима на коммутаторе со специальным набором команд используется команда:

```
Switch>(enable) set vtp mode server | client | transparent
```

Тестирование конфигурации протокола VTP

В примере 10.4 показан вывод по команде **show vtp status**. Эта команда тестирует установки конфигурации протокола VTP на коммутаторе с функциями IOS Cisco.

Пример 10.4. Команда show vtp status

```
Switch#show vtp status
VTP Version                : 2
Configuration Revision      : 2
Maximum VLANs supported locally : 68
Number of existing VLANs    : 6
VTP Operating Mode          : Client
VTP Domain Name             : Cisco
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Enabled
VTP Traps Generation        : Disabled
MD5 Digest                  : 0x35 0x84 0x7B 0x04 0x3D
                           : 0x55 0x3B 0xDA
Configuration last modified by 0.0.0.0 at 12-23-02 20:24:33
```

В примере 10.5 приведен результат выполнения команды **show vtp statistics** на коммутаторе со специальным набором команд. Эта команда отображает общее количество полученных и отправленных анонсирующих сообщений протокола VTP, а также обнаруженные ошибки в конфигурации. Эту команду следует использовать для тестирования протокола VTP.

Пример 10.5. Команда show vtp statistics

```
Switch>(enable) show vtp statistics
VTP statistics:
summary advts received      0
subset advts received       0
request advts received      0
summary advts transmitted  0
subset advts transmitted    0
request advts transmitted   0
No of config revision errors 0
No of config digest errors  0
```

**Лабораторная работа: магистральные соединения 802.1Q**

В этой лабораторной работе требуется создать базовую конфигурацию коммутатора, а затем создать несколько VLAN-сетей, задать им имена и назначить порты. После этого можно создать между двумя коммутаторами магистральный канал и выполнить тестирование VLAN-сетей путем перемещения рабочей станции из одной VLAN-сети в другую.

**Лабораторная работа: конфигурирование клиента и сервера протокола VTP**

В этой лабораторной работе требуется создать несколько VLAN-сетей, задать им имена и назначить порты. После этого требуется создать магистральный канал между коммутаторами и сконфигурировать один коммутатор как VTP-сервер, а другой как клиент протокола VTP. После этого можно выполнить тестирование VLAN-сетей путем перемещения рабочей станции из одной VLAN-сети в другую.

Отсечение каналов в протоколе VTP

По умолчанию коммутатор распространяет по сети широковещательные сообщения и неизвестные пакеты. Такое поведение приводит к передаче по сети данных, которые не являются необходимыми.

Отсечение протокола VTP повышает эффективность использования полосы пропускания путем сокращения передачи данных, которые не являются необходимыми, таких, как широковещательные данные, данные многоадресной рассылки, неизвестные пакеты и одноадресные пакеты, рассылаемые методом лавинной рассылки. Отсечение протокола VTP увеличивает доступную полосу пропускания путем ограничения передачи данных на магистральные каналы, по которым должны передаваться данные соответствующим сетевым устройствам. По умолчанию отсечения протокола VTP отключено. Если на удаленном коммутаторе сети VLAN 3 нет доступного устройства, то отсечение протокола VTP предотвращает рассылку этим коммутатором данных сети VLAN 3 с магистрального порта и нерациональное использование полосы пропускания.

Включение VTP-отсечения на сервере VTP позволяет отсечь целый домен управления. Отсечение VTP начинает работать через несколько секунд после его включения. По умолчанию отсечение может быть выполнено для VLAN-сетей с номерами 2-1000. Для VLAN-сетей для которых отсечение невозможно, оно не осуществляется. В частности, отсечение потоков данных для сети VLAN 1 вообще невозможно. Для других VLAN-сетей можно осуществлять отсечение данных на конкретном устройстве по желанию. Для того, чтобы сделать допустимым отсечение VLAN-сетей на коммутаторе с функциями IOS Cisco, необходимо выполнить следующую команду:

```
Switch(vlan)#vtp pruning
```

Для того, чтобы сделать невозможным отсечение VLAN-сетей на коммутаторе с функциями IOS Cisco, необходимо выполнить следующие команды:

```
Switch(config)#interface fastethernet 0/3  
Switch(config-if)#switchport trunk pruning vlan remove vlan-id
```

Для того, чтобы сделать возможным отсечение VLAN-сетей на коммутаторе со специальным набором команд, необходимо выполнить следующую команду:

```
Console> (enable) set vtp pruneeligible vlan_range
```

Для того, чтобы сделать невозможным отсечение VLAN-сетей на коммутаторе со специальным набором команд, необходимо выполнить команды:

```
Console> (enable) clear vtp pruneeligible vlan_range
```

Межсетевая VLAN-маршрутизация

Если узлу в одном широковещательном домене требуется выполнить обмен данными с узлом другого широковещательного домена, то требуется использование маршрутизатора. Аналогичная ситуация возникает и в сетях VLAN.

Пример такой ситуации показан на рис. 10.13.

Порт 1 коммутатора является частью сети VLAN 1, а порт 2 — частью сети VLAN 200. Если бы все порты коммутатора принадлежали сети VLAN 1, то все узлы, подсоединенные к этим портам, могли бы осуществлять связь между собой. Однако в данном случае порты принадлежат различным VLAN-сетям: сети VLAN 1 и сети VLAN 200. Если узлы принадлежат различным VLAN-сетям и им требуется осуществить обмен данными, то требуется использование маршрутизатора, как показано на рис. 10.14.

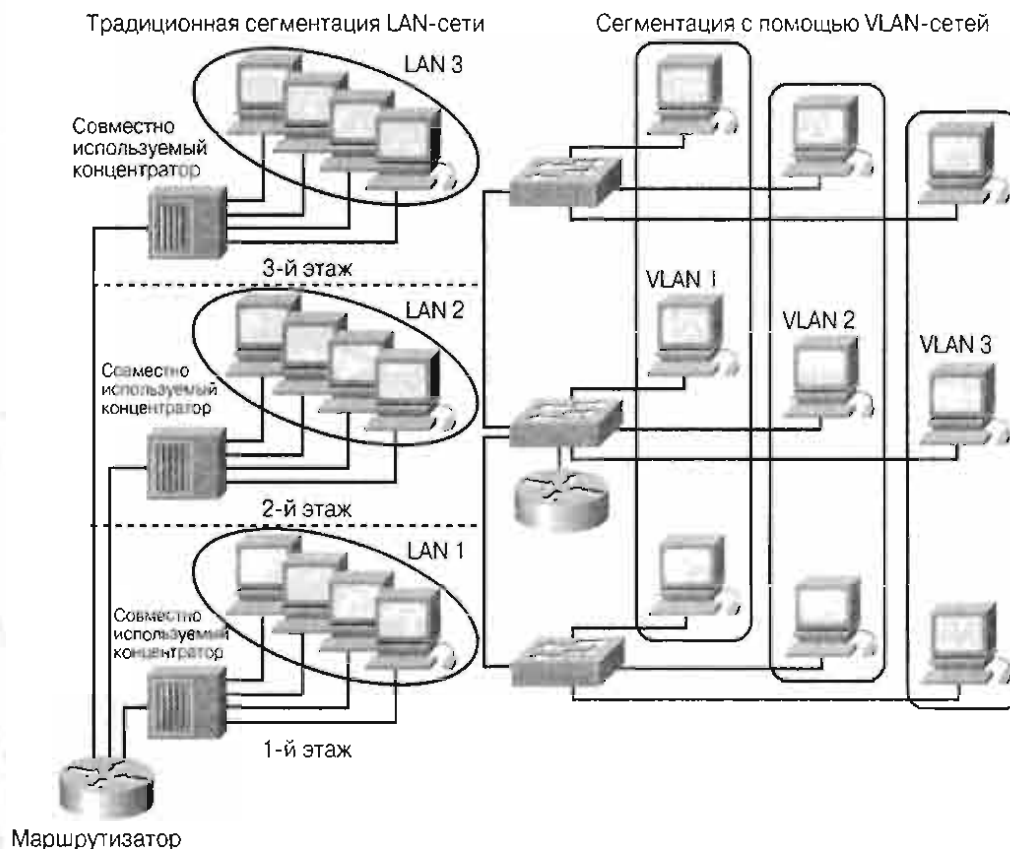


Рис. 10.13. Маршрутизаторы и виртуальные локальные сети VLAN

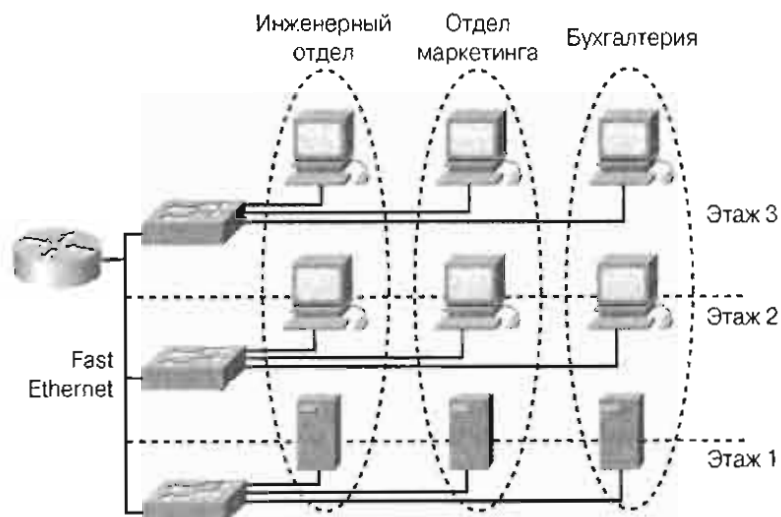


Рис. 10.14. Устранение физических границ

Важным достоинством маршрутизации является ее проверенная временем способность облегчать поддержку работы сетей, особенно крупных. Наиболее очевидным примером этого является глобальная сеть Internet, однако это верно и для всех остальных типов сетей, таких, в частности, как магистрали крупной сети кампуса. Поскольку маршрутизаторы предотвращают распространение широковещательных сообщений и используют более интеллектуальные алгоритмы пересылки, чем мосты и коммутаторы, их использование позволяет более эффективно использовать полосу пропускания. Это одновременно повышает гибкость сети и оптимизирует выбор маршрутов. Например, при использовании маршрутизации в большинстве сетей легко реализовать распределение нагрузки по нескольким маршрутам. С другой стороны, распределение нагрузки на 2-м уровне может оказаться достаточно трудным для проектирования, реализации и поддержки.

Если VLAN-сеть охватывает несколько устройств, то эти устройства соединяются магистральным каналом. По этой магистрали передаются данные нескольких VLAN-сетей. Например, магистраль может соединять два коммутатора, коммутатор с межсетевым VLAN-маршрутизатором или коммутатор с сервером, имеющим специальную карту сетевого интерфейса (network interface card — NIC) и поддерживающим магистральные каналы.

Следует учитывать, что для связи узлов, находящихся в разных VLAN-сетях, необходим маршрутизатор.

Взаимодействие между VLAN-сетями и решение возникающих проблем

При соединении между собой нескольких VLAN-сетей возникают некоторые технические проблемы. Чаще всего в среде нескольких VLAN-сетей приходится решать две проблемы:

- получение устройствами конечного пользователя доступа к нелокальным узлам;
- осуществление связи между узлами различных VLAN-сетей.

Когда устройству требуется осуществить обмен данными с удаленным узлом, оно просматривает свою таблицу маршрутизации в поисках известного маршрута. Если удаленный узел находится в известной подсети, то система проверяет, можно ли связаться с ним через данный интерфейс. Если все известные маршруты не позволяют осуществить связь, то у системы остается только один способ — использовать стандартный маршрут. Этот маршрут относится к специальному типу шлюзовых маршрутов и обычно в системе имеется только один такой маршрут. На маршрутизаторе стандартный маршрут отмечается символом (*) в выводе по команде **show ip route**. Для узлов локальной сети (local-area network — LAN) этот шлюз указывает на любой узел, имеющий непосредственное соединение с внешней средой и он является стандартным шлюзом, указанным в установках протокола TCP/IP для данной рабочей станции. Если стандартный маршрут конфигурируется для маршрутизатора, который выполняет функции шлюза в открытую сеть Internet, то он указывает на устройство-шлюз в сети Internet-провайдера (Internet service provider — ISP). Стандартные маршруты устанавливаются командой **ip route**, как показано в примере 10.6.

Пример 10.6 Команда ip route

```
Router(Config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

В примере 10.6 устройство с адресом 192.168.1.1 является стандартным шлюзом. Связь между различными VLAN-сетями может осуществляться через логическое или физическое соединение. Логическое соединение осуществляется по отдельному или магистральному каналу от коммутатора к маршрутизатору. Этот магистральный канал может поддерживать передачу данных нескольких VLAN-сетей. Такая топология называется “приклеиванием маршрутизатора” (“router on a stick”), поскольку при этом имеется лишь одно соединение с маршрутизатором, однако несколько логических соединений маршрутизатора с коммутатором. Пример такой ситуации приведен на рис. 10.15.



Рис. 10.15. Застревание маршрута

Изолированные широковещательные домены

В сетях, использующих коммутацию, связь между различными VLAN-сетями осуществляется с помощью процессоров маршрутов (Route Processor).

Эти процессоры обеспечивают доступ VLAN-сетей к совместно используемым ресурсам и соединения с другими частями сети, которые либо логически сегментированы с помощью более традиционного деления на подсети, либо требуют доступа к уда-

ленным узлам по каналам распределенных сетей. Процессоры маршрутов во многом аналогичны маршрутизаторам, однако они могут быть встроены в коммутатор. Они могут не иметь физических интерфейсов, однако конфигурируются с помощью тех же команд IOS Cisco, которые используются для обычных маршрутизаторов.

Перед конфигурированием маршрутизации между VLAN-сетями необходимо определить VLAN-сети на коммутаторах сети. Вопросы, связанные с проектированием и определением VLAN-сетей, должны быть решены на этапе проектирования всей сети. При этом должны быть решены следующие вопросы:

- совместное использование ресурсов VLAN-сетями;
- распределение нагрузки;
- избыточность каналов;
- логическая адресация;
- сегментирование сети с помощью VLAN-сетей.

На рис. 10.16 показаны изолированные широковещательные домены.

ПРИМЕЧАНИЕ

Вообще говоря, подход "route on-a-stick" для межсетевой VLAN-маршрутизации является наиболее целесообразным в тех случаях, когда другие возможные варианты отсутствуют. Это не означает, что проектирование по принципу "router-on-a-stick" неэффективно; этим просто констатируется тот факт, что другие подходы, как правило, обеспечивают большую эффективность и функциональность. Другим фактором является то, что метод "router-on-a-stick" функционирует так, как если бы маршрутизатор находился на границе сети (по крайней мере в сетях 2-го уровня) и поэтому он менее тесно интегрирован с остальной частью сети кампуса.

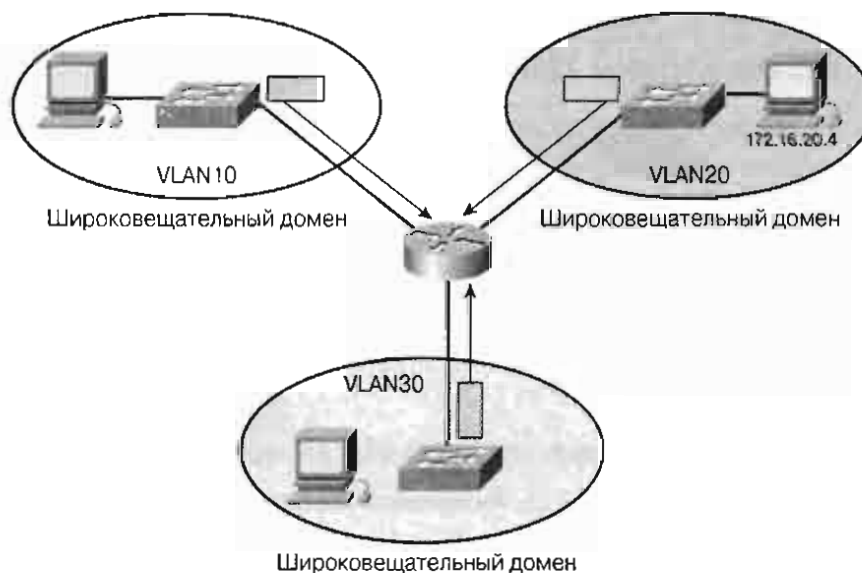


Рис. 10.16. Изолированные широковещательные домены

Нахождение маршрута между VLAN-сетями

Процессор маршрутов (*Route Processor*) содержит большинство компонентов системной памяти и главный процессор системы.

Стандартным шлюзом (*default gateway*) называется интерфейс маршрутизатора, который обычно идентифицируется своим IP-адресом. Стандартным маршрутизатором или маршрутизатором по умолчанию (*default router*) называется маршрутизатор, у которого есть хотя бы один интерфейс, выступающий в качестве стандартного шлюза. Для протокола DHCP стандартным считается маршрутизатор, предоставляющий пул IP-адресов. На рис. 10.17 показан стандартный шлюз.

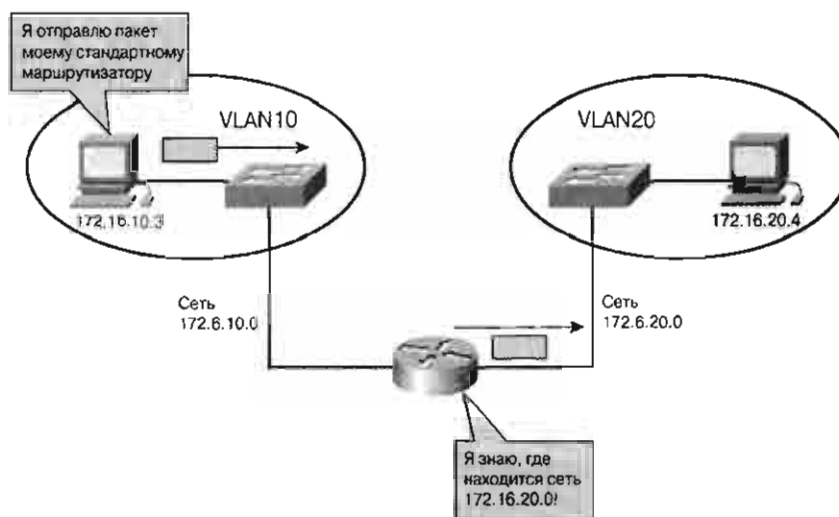


Рис. 10.17. Стандартный шлюз

При подсоединении отдельных подсетей через процессор маршрутов возникает вопрос о том, как осуществлять связь устройствам конечного пользователя с другими устройствами через несколько LAN-сегментов. Некоторые сетевые устройства используют таблицы маршрутизации для идентификации мест доставки пакетов, находящихся вне данного локального сегмента локальной сети. Несмотря на то, что конечные устройства не отвечают за маршрутизацию данных, они могут оказаться способными отправлять данные по адресам подсетей, отличных от их собственных. Поэтому, хотя конечные устройства не обязаны управлять своими собственными таблицами маршрутизации, большинство этих устройств конфигурируются с IP-адресами назначенного процессора маршрутов. Этот назначенный процессор маршрутов представляет собой стандартный маршрутизатор, которому посылаются все пакеты, получатели которых не принадлежат данному локальному сегменту.

Позднее процессор маршрутов пересылает эти пакеты в соответствующие пункты назначения. IP-адрес стандартного маршрутизатора для сетевого устройства зависит от того, в какой IP-подсети находится данное сетевое устройство.

В прежних проектах VLAN-сетей для этого использовались внешние маршрутизаторы, подсоединенные к коммутаторам с функциями VLAN-сетей. При таком подходе традиционные маршрутизаторы подсоединялись к коммутируемым сетям через один или более каналов. При проектировании по методу "router-on-a-stick" используется отдельный магистральный канал, который соединяет маршрутизатор с остальной ча-

стью сети кампуса. Данные, передаваемые между VLAN-сетями, должны пересечь магистраль 2-го уровня для поступления на маршрутизатор, который передаст их в различные VLAN-сети. После этого данные передаются в обратном направлении, т.е. требуемой конечной станции с использованием обычной пересылки на 2-м уровне. Такое перемещение потоков данных “с маршрутизатора и обратно” (“out-to-the-router-and-back”) характерно для проектирования по методу “router-on-a-stick”.

Физические и логические интерфейсы

В обычных ситуациях сети, имеющей, например, четыре VLAN-сети, требовались четыре физических соединения между коммутатором и внешним маршрутизатором. По мере того, как все шире использовались такие технологии как ISL, сетевые проектировщики стали использовать магистральные каналы для соединения маршрутизаторов с коммутаторами. Хотя для этой цели могут быть использованы любые магистральные технологии, такие как ISL, 802.1Q, 802.10 или эмуляция LAN-сетей (LAN Emulation — LANE), наиболее часто используются основанные на Ethernet технологии (ISL и 802.1Q). На коммутаторах Catalyst серии 2900 по умолчанию используется технология 802.1Q, в то время как на коммутаторах 29xx по умолчанию используется технология ISL.

Фирменный протокол Cisco ISL создает магистральные соединения VLAN-сетей по каналам Fast Ethernet. По мере того, как в сети увеличивается количество VLAN-сетей, физический подход, состоящий в выделении одного интерфейса маршрутизатора каждой VLAN-сети быстро становится неприемлемым. В сетях с большим количеством VLAN приходится использовать магистральные VLAN-соединения и назначать несколько VLAN одному физическому интерфейсу маршрутизатора.

Первичным преимуществом использования магистральных каналов является сокращение количества требуемых портов на коммутаторах и маршрутизаторах. Это не только сокращает расходы, но также уменьшает сложность конфигурирования сети. При таком подходе к маршрутизатору может быть подсоединено значительно большее количество VLAN-сетей чем при проектировании отдельных каналов для каждой VLAN-сети.

Создание подынтерфейсов на физическом интерфейсе

Подынтерфейсом (subinterface) называется логический интерфейс на физическом интерфейсе, такой, например, как интерфейс Fast Ethernet на маршрутизаторе. На одном физическом интерфейсе могут быть созданы несколько подынтерфейсов.

Каждый подынтерфейс поддерживает одну VLAN-сеть и имеет свой IP-адрес. Для того, чтобы несколько устройств одной и той же VLAN могли осуществлять связь друг с другом, их IP-адреса должны принадлежать одной и той же сети или подсети. Например, если подынтерфейс 2 имеет IP-адрес 192.168.1.1, то 192.168.1.2, 192.168.1.3 и 192.1.1.4 являются IP-адресами устройств, подсоединенных к подынтерфейсу 2. Для передачи данных между VLAN-сетями с подынтерфейсами необходимо создать подынтерфейсы для каждой VLAN.

Конфигурирование маршрутизации между VLAN-сетями

В настоящем разделе описываются команды, необходимые для конфигурирования маршрутизации в среде VLAN-сетей между маршрутизатором и коммутатором. Перед выполнением этих команд необходимо проверить каждый маршрутизатор

и коммутатор с целью выяснения типа VLAN-инкапсуляции, который ими поддерживается. Например, коммутаторы Catalyst 2950 поддерживали магистральные соединения 802.1Q с момента появления версии IOS Cisco 12.0(5.2)WC(1), но они не поддерживают магистральные соединения ISL. Маршрутизаторы Cisco поддерживают магистральные соединения ISL и 802.1Q начиная с версии Cisco IOS 12.0(T). Для того, чтобы маршрутизация между VLAN-сетями работала соответствующим образом, необходимо чтобы все участвующие в ней маршрутизаторы и коммутаторы поддерживали один и тот же тип инкапсуляции. На маршрутизаторе один физический подынтерфейс может быть подразделен на несколько виртуальных подынтерфейсов. Подынтерфейсы предоставляют гибкое решение задачи маршрутизации нескольких потоков данных через один физический интерфейс. Для определения подынтерфейсов на физическом интерфейсе необходимо решить следующие задачи.

1. Идентифицировать интерфейс.
2. Задать инкапсуляцию VLAN-сетей.
3. Назначить интерфейсу IP-адрес.

Для идентификации интерфейса используется команда **interface** в режиме глобального конфигурирования:

```
Router(config)#interface FastEthernet port-number subinterface-number
```

Параметр *port-number* задает физический интерфейс, а параметр *subinterface-number* — виртуальный интерфейс. Маршрутизатор должен быть способен обмениваться информацией с коммутатором, используя стандартизованный магистральный протокол. Это означает, что оба соединенных между собой устройства должны понимать друг друга. В приведенном примере используется протокол 802.1Q.

Для задания типа VLAN-инкапсуляции используется команда **encapsulation** в режиме конфигурирования интерфейса:

```
Router(config-if)#encapsulation dot1q vlan-number
```

Параметр *vlan-number* задает VLAN-сеть, для которой передает данные данный интерфейс VLAN. Идентификатор ID VLAN-сети добавляется к фрейму только в том случае, если этот фрейм предназначен для удаленной сети (т.е. не принадлежащей данной локальной сети). Каждый VLAN-пакет переносит в заголовке пакета идентификатор ID VLAN-сети. Для назначения интерфейсу IP-адреса следует ввести в режиме конфигурирования интерфейса команду:

```
Router(config-if)#ip address ip-address subnet-mask
```

Параметры *ip-address* и *subnet-mask* представляют собой 32-битовый адрес сети и маску конкретного интерфейса.



Лабораторная работа: конфигурирование межсетевой VLAN-маршрутизации

В этой лабораторной работе требуется сконфигурировать внешний маршрутизатор для передачи данных между несколькими VLAN-сетями с помощью коммутаторов.

Резюме

В среде виртуальных локальных сетей VLAN магистральные соединения реализуются для расширения сферы связи по VLAN-сетям за пределы одной сети. Обычно магистральные соединения реализуются между коммутаторами путем перевода по крайней мере одного порта на каждом из коммутаторов, участвующих в работе магистрального канала, в магистральный режим. Двумя наиболее часто используемыми магистральными протоколами, позволяющими управлять передачей данных от различных VLAN-сетей являются:

- протокол ISL;
- протокол 802.1Q.

Магистральный протокол VLAN-сетей VLAN Trunking Protocol — VTP) был разработан для решения некоторых потенциальных проблем в среде VLAN-сетей путем поддержки в сети согласования. Протокол VTP обладает следующими преимуществами:

- согласование конфигураций VLAN-сетей во всей сети;
- схема преобразования, позволяющая осуществлять магистральные соединения VLAN-сетей по смешанной среде передачи;
- тщательное наблюдение и мониторинг VLAN-сетей;
- динамическая регистрация и оповещение всех устройств сети о добавлении новых VLAN-сетей;
- конфигурирование “plug-and-play” при добавлении новых VLAN-сетей.

В случае, когда конечной станции одной VLAN-сети требуется осуществить связь с конечной станцией в другой VLAN-сети, требуется межсетевая VLAN-маршрутизация.

В дополнение к материалу, изложенному в настоящей главе, рекомендуется ознакомиться с лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

802.1Q. Магистральный протокол, по которому можно передавать данные более чем одной подсети по одному кабелю. Комитет IEEE 802.1Q определил этот метод мультиплексирования VLAN-сетей в качестве основы для поддержки VLAN-сетей на оборудовании разных производителей.

Виртуальная локальная сеть (virtual LAN — VLAN). Группа устройств, принадлежащих одной или нескольким локальным сетям LAN, которые конфигурируются (с использованием программного обеспечения) таким образом, чтобы они могли осуществлять связь между собой, как если бы они были подключены к общей шине, в то время как фактически они находятся в разных LAN-сегментах.

Магистраль (trunk). Отдельный канал передачи между двумя точками сети, которыми обычно являются коммутационные центры.

Магистральное соединение (trunking). Физическое и логическое соединение между двумя коммутаторами, по которому передаются данные. Магистраль состоит из нескольких магистральных соединений.

Магистральный протокол виртуальных локальных сетей (VLAN Trunking Protocol — VTP). Протокол VTP представляет собой протокол передачи сообщений, использующий магистральные фреймы 2-го уровня для управления добавлением, удалением и переименованием VLAN-сетей во всей сети.

Маршрутизатор, используемый по умолчанию (default router). Так называется маршрутизатор, имеющий как минимум один интерфейс, используемый в качестве стандартного.

Подынтерфейс (subinterface). Один из нескольких виртуальных интерфейсов на одном физическом интерфейсе.

Протокол межкоммутаторного канала (Inter-Switch Link — ISL). Фирменный магистральный протокол Cisco, используемый для соединения между собой нескольких коммутаторов и поддерживающий информацию о VLAN-сетях при передаче данных между коммутаторами по магистральным каналам.

Процессор маршрутов (route processor). Это процессор содержит большинство системных компонент памяти и главный процессор системы.

Стандартный шлюз (default gateway). Интерфейс маршрутизатора, который обычно идентифицируется своим IP-адресом.

Контрольные вопросы

1. В чем состоит основное преимущество использования магистрального канала?
 - A. Магистральный канал обеспечивает большую полосу пропускания для каждого канала
 - B. Магистральный канал обеспечивает эффективное использование портов маршрутизаторов и коммутаторов
 - C. Магистральный канал позволяет создать отдельную VLAN-сеть на каждом физическом порте
 - D. Магистральный канал уменьшает объем передачи служебных данных на маршрутизаторе
2. Какой протокол передает данные нескольких VLAN-сетей по одному магистральному каналу?
 - A. Протокол 802.2
 - B. Протокол 802.3
 - C. Протокол 802.1Q
 - D. Протокол 802.11B
3. Какой фирменный протокол Cisco предназначен для передачи данных от нескольких VLAN-сетей?
 - A. 802.11A
 - B. 802.1Q
 - C. VNET
 - D. ISL

4. Справедливо ли утверждение: для создания или конфигурирования магистрального VLAN-канала на коммутаторе с функциями IOS Cisco необходимо сначала сконфигурировать порт как магистральный, а затем задать тип инкапсуляции в канале
 - A. Справедливо
 - B. Неверно
5. Сообщения протокола VTP инкапсулируются в формат фирменного протокола межкоммутаторного канала Cisco (Inter-Switch Link — ISL) или в какой-либо из приведенных ниже форматов?
 - A. Формат фреймов протокола IEEE 802.1Q
 - B. Формат фреймов протокола IEEE 802.1R
 - C. Формат фреймов протокола 802.11D
 - D. Формат фреймов протокола 802.1P
6. При использовании протокола VTP все коммутаторы семейства Catalyst анонсируют на своих магистральных портах:
 - A. Домен управления
 - B. Версию конфигурации
 - C. Известные им VLAN-сети и их конкретные параметры
 - D. Все вышеперечисленное
7. Коммутаторы протокола VTP могут функционировать в режиме?
 - A. Сервера
 - B. Клиента
 - C. В прозрачном режиме
 - D. Все вышеперечисленное
8. Справедливо ли утверждение: в одном домене управления могут функционировать две версии протокола VTP — версия 1 и версия 2. Эти две версии являются совместимыми и могут работать в одном и том же домене.
 - A. Справедливо
 - B. Неверно
9. Для создания домена управления используется команда:

```
Switch(vlan)#domain Cisco
Switch(vtp)#domain Cisco
Switch(vlan)#vtp domain Cisco
Switch(vtp)#vtp domain Cisco
```
10. По умолчанию коммутатор распространяет по сети широковещательные сообщения и неизвестные _____
 - A. фреймы
 - B. пакеты
 - C. теги
 - D. информацию о VLAN-сетях

11. Активизация отсечения на сервере VTP дает возможность предотвратить рассылку данных для _____.
 - A. Коммутатора в режиме сервера
 - B. Коммутатора в прозрачном режиме
 - C. Коммутатора в режиме управления
 - D. Коммутатора в режиме пользователя
12. В сети, построенной на основе коммутаторов, для связи между VLAN-сетями используются _____.
 - A. Процессоры маршрутов
 - B. Модуляторы
 - C. Протокол VTP
 - D. Подсети протокола VTP



В этой главе...

- Объясняется необходимость в масштабировании IP-адресов
- Описана терминология адресации NAT
- Описаны функции NAT
- Рассмотрены различия между статической NAT, динамической NAT и PAT
- Описано конфигурирование и тестирование NAT и PAT
- Рассмотрены поиск и устранение ошибок в конфигурациях NAT и PAT
- Рассмотрены различия между протоколами BOOTP и DHCP
- Описано конфигурирование и тестирование протокола DHCP
- Описаны терминология и функции протокола DHCP
- Рассмотрены поиск и устранение ошибок в конфигурации протокола DHCP
- Рассмотрены открытые и частные IP-адреса и различия между ними

Масштабирование IP-адресов

IP-адрес требуется любому устройству, имеющему соединение с Internet. Количество устройств, которым требуются IP-адреса, быстро увеличивается, однако количество этих адресов ограничено. В настоящей главе обсуждаются проблема истощения пространства IP-адресов и разработанные решения, которые позволяют смягчить эту проблему. В качестве предлагаемых решений рассматриваются трансляция сетевых адресов (*network address translation* — NAT), трансляция адресов портов (*port address translation* — PAT), использование протокола динамического конфигурирования хоста (узла) (*Dynamic Host Configuration Protocol* — DHCP) и частных IP-адресов. В ней будут описаны конфигурирование, тестирование и устранение ошибок протоколов NAT и DHCP на маршрутизаторах.

Рекомендуется выполнить лабораторные работы (*e-Lab Activities*), ознакомиться с видеоклипами (*Videos*) и фотографиями (*PhotoZooms*), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Обзор протокола Internet

Протокол IP используется в качестве способа осуществления связи между сетевыми устройствами. IP-приложения активно разрабатываются, их количество стремительно растет и все большее количество устройств имеет возможность выхода в Internet. На ранних стадиях развития сети Internet к ней подключались лишь такие устройства, как персональные компьютеры, рабочие станции, серверы и маршрутизаторы. IP-адреса этим устройствам назначались статически сетевым администратором.

В настоящее время к Internet подключаются персональные цифровые организаторы (*Personal Digital Assistant* — PDA), портативные компьютеры, настольные компьютеры, мейнфреймы, устройства для хранения данных, маршрутизаторы, коммутаторы, игровые видеоприставки и камеры безопасности (слежения). Говорится даже о подключении к Internet домашних бытовых устройств. Становится очевидным, что без развития методов масштабирования Internet-революция скоро достигнет пределов своего развития.

В последние годы были разработаны несколько таких методов, включая использование масок подсетей переменной длины (*variable-length subnet mask* — VLSM), бесклассовой междоменной маршрутизации (*classless interdomain routing* — CIDR) и 6-й версии протокола IP (*Internet Protocol version 6* — IPv6). В настоящей главе представлены три других решения проблемы масштабирования IP-адресов: использование ча-

стных адресов (RFC 1918), трансляции адресов (NAT и PAT), а также использование пулов адресов (address pooling, DHCP).

В настоящей главе представлены решения проблемы масштабируемости в IP-сетях. В настоящее время перед Internet стоят две проблемы масштабируемости.

- Пространство зарегистрированных IP-адресов истощается, а размер сети Internet продолжает возрастать.
- По мере роста Internet растет и количество IP-маршрутов в таблицах маршрутизации магистральных маршрутизаторов Internet. Это создает проблему масштабируемости для алгоритмов маршрутизации.

Протоколом IP предлагаются следующие решения этих проблем:

- использование адресации NAT;
- использование протокола DHCP;
- использование частных IP-адресов (RFC 1918).

Адресация NAT представляет собой механизм ограничения количества зарегистрированных IP-адресов в крупных сетях и упрощения задач управления, связанных с IP-адресацией. Адресация NAT основана на стандартах и описана в RFC 1631.

При прохождении пакета через маршрутизатор с функциями NAT, которые обеспечиваются IOS Cisco, IP-адрес источника, присвоенный в частной внутренней сети, преобразуется в официально зарегистрированный IP-адрес для того, чтобы его можно было передать по открытой внешней сети, такой как Internet.

Адреса ответных пакетов также преобразуются в обратном порядке для доставки их конкретному получателю во внутренней сети. Адресация NAT подробно обсуждается в настоящей главе.

Глобальная сеть Internet растет взрывным образом и нет тенденции замедления этого процесса. Администраторам требуется назначать IP-адреса, стандартные шлюзы и вводить на узлах другую информацию для подсоединения этих устройств к сети Internet. Использование протокола DHCP позволяет администраторам назначать устройствам IP-адреса динамически.

Когда стала развиваться глобальная сеть Internet, многие организации выразили желание использовать протокол IP для своих соединений, однако не хотели делать свои узлы открытыми для всех узлов Internet. В RFC 1918 эта проблема решается путем определения открытого адресного пространства IP и частного пространства IP-адресов, используемых только для адресации в частной сети.

Организация по назначению адресов в Internet (Internet Assigned Numbers Authority — IANA) определила три блока (класса) IP-адресов, приведенных в табл. 11.1. В RFC 1918 приведены рекомендации по эффективному их использованию.

Таблица 11.1 Адреса RFC 1918

Класс	Диапазон внутренних адресов (согласно RFC 1918)	Префикс маршрутизации CIDR
A	10.0.0.0–10.255.255.255	10.0.0.0/8
B	172.16.0.0–172.31.255.255	172.16.0.0/12
C	192.168.0.0–192.168.255.255	192.168.0.0/16

Эти три диапазона предоставляют более 17 миллионов частных адресов. Термин “частный” (*private*) в данном контексте означает, что они не могут использоваться в открытой сети Internet, однако организации могут свободно использовать их в своих корпоративных сетях. Соответственно, они считаются разрешенными для маршрутизации (*on-routable*).

Адреса протоколов IPv4 и IPv6 назначаются уполномоченными организациями. Пользователям такие адреса назначаются провайдерами служб Internet (Internet service providers — ISP). Эти провайдеры получают адреса из локального реестра Internet (local Internet registry — LIR), национального реестра Internet (national Internet registry — NIR) или своего регионального реестра Internet (regional Internet registry — RIR). В качестве такого реестра могут выступать Азиатско-Тихоокеанский центр сетевой информации (Asia Pacific Network Information Centre — APNIC), Американский Регистр Internet-адресов (American Registry for Internet Numbers — ARIN), Региональный регистр адресов Латинской Америки и Карибского региона (Latin American and Caribbean IP Address Regional Registry — LACNIC) или Европейская IP-сеть (Rйseaux IP Europйens — RIPE NCC).

Частные IP-адреса могут свободно использоваться всеми пользователями сетей. Это означает, что один и тот же частный адрес может использоваться в двух сетях или в двух миллионах сетей. Адреса, указанные в RFC 1918, не могут использоваться в открытой сети Internet и работающие в ней маршрутизаторы не пересылают данные с такими адресами, поскольку провайдеры ISP обычно конфигурируют свои маршрутизаторы таким образом, что они не позволяют пересылку данных с частными IP-адресами.

Для адресации в частных интранет-сетях, для тестирования сетей или внутреннего использования вместо глобально уникальных адресов используются частные адреса. Глобальные адреса пользователи получают от провайдера или из регистра за определенную плату.

Адреса RFC 1918 могут также использоваться в производственных корпоративных сетях. Использование масок переменной длины VLSM позволяет ввести в уже существующих подсетях новые подсети, однако это возможно только в остающихся единственными доступными в настоящее время сетях класса C.

Хотя такое решение более эффективно, чем затрата всей подсети с 30-адресами для узлов на каждом WAN-канале с двумя узлами, оно все же требует затраты одной подсети, которая могла бы быть использована для будущего роста сети. Менее расточительным решением является использование в WAN-каналах частных сетевых адресов. На рис. 11.1 для адресации в WAN-каналах используются частные адреса из пространства 10.0.0.0/8.

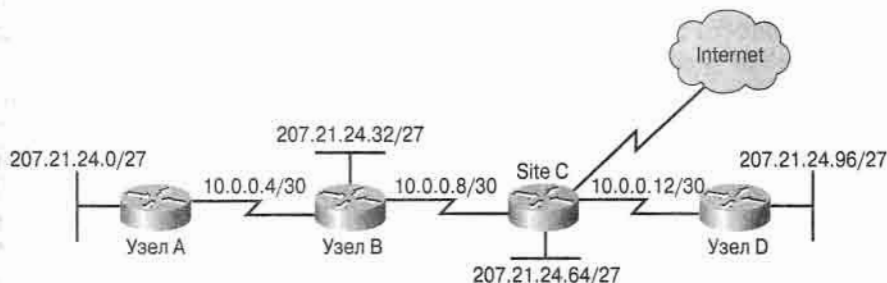


Рис. 11.1. Использование частных адресов в WAN-каналах

Каким образом эти маршрутизаторы могут использовать частные адреса, если пользователи LAN-сетей в узлах А, В, С и D ожидают доступа в Internet? Конечные пользователи этих узлов не должны иметь проблем, поскольку они имеют зарегистрированные глобально уникальные адреса сети 207.21.24.0. Эти маршрутизаторы используют свои последовательные интерфейсы с частными адресами только для пересылки данных и обмена информацией маршрутизации. Находящиеся в восходящем направлении провайдеры и Internet-маршрутизаторы видят в пакете только IP-адреса источника и получателя и их не интересует тот факт, что эти пакеты на определенном этапе прошли через каналы с частными адресами. Фактически многие провайдеры используют сетевые адреса RFC 1918 в своих базовых сетях для того, чтобы предотвратить истощение своего пространства глобально уникальных адресов.

Компромиссом при использовании частных адресов в WAN-каналах является то, что эти последовательные интерфейсы не могут быть оригинальным источником данных для Internet или конечным получателем данных из сети Internet. Обычно маршрутизаторы не затрачивают время на навигацию в Internet, поэтому такое ограничение становится проблемой только при поиске и устранении ошибок с помощью протокола ICMP или при осуществлении удаленного соединения по протоколу Telnet через сеть Internet. В этих случаях адресация маршрутизатора может осуществляться только по его глобально уникальным LAN-интерфейсам.

Адресация NAT предоставляет индивидуальным компаниям и сети Internet огромные преимущества. До появления NAT-адресации узел с частным адресом не мог получить доступ в Internet. При использовании этой адресации отдельные компании могут адресовать часть или все свои узлы с помощью частных адресов, а затем использовать NAT для получения доступа к открытой сети Internet. В то же самое время эти узлы могут подсоединяться к Internet не затрачивая адресов из своего адресного пространства.

Адресации NAT и PAT

Сущность NAT-адресации состоит в замене в IP-заголовке пакета адреса получателя, источника или их обоих другими, назначаемыми администратором адресами. Этот процесс замены адресов осуществляется специализированным программным или аппаратным обеспечением с функциями NAT. Назначение адресации NAT состоит в упрощении и сбережении IP-адресов, поскольку при ее использовании частные объединенные IP-сети, использующие незарегистрированные IP-адреса, могут подсоединяться к Internet транслируя эти частные адреса в глобально уникальные зарегистрированные адреса. Адресация NAT IOS Cisco также повышает уровень конфиденциальности сети, поскольку при этом внутренние IP-адреса оказываются "спрятанными" от внешних сетей.

Устройство с функциями NAT обычно работает на границе тупиковой сети. Под тупиковой сетью понимается сеть, имеющая только одно соединение с соседней сетью. На рис. 11.2 приведен простой пример тупиковой сети. В том случае, когда узлу тупиковой сети требуется передать данные узлу, находящемуся вне его собственной, пересылка осуществляется через граничный шлюзовой маршрутизатор. В этом случае граничный шлюзовой маршрутизатор также должен обладать функциями NAT-адресации.

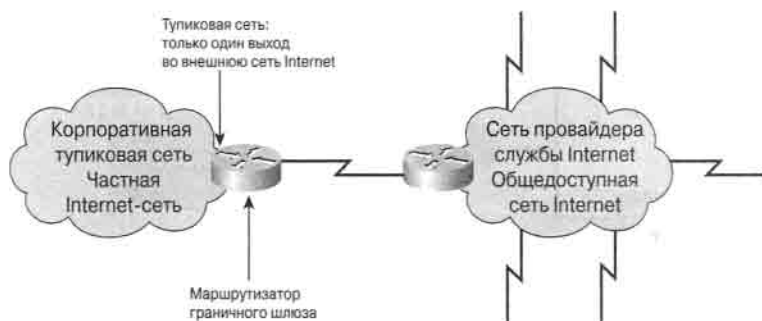


Рис. 11.2. Пример тупиковой сети

Адресация NAT обычно функционирует на маршрутизаторе Cisco, соединяя две сети и транслирует частные (внутренние локальные) адреса внутренней сети в открытые адреса (глобальной сети) перед отправкой пакетов в другую сеть, как показано на рис. 11.3–11.5.

Как показано на рис. 11.3, внутреннему узлу (10.0.0.2) требуется обменяться данными с внешним узлом (128.23.2.2). Для этого он посылает пакеты своему шлюзовому маршрутизатору RTA.

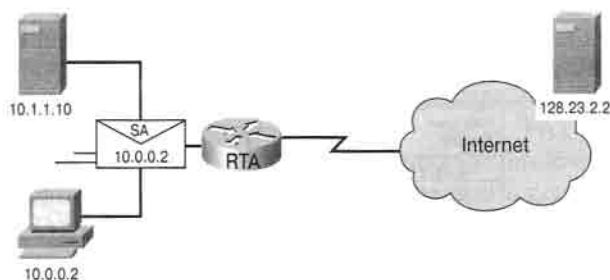


Рис. 11.3. Адресация NAT

Маршрутизатор RTA выясняет, что пакет необходимо переслать во внешнюю сеть Internet. Процесс адресации NAT выбирает глобально уникальный IP-адрес (179.9.8.80) и заменяет локальный адрес в поле источника пакета этим глобальным адресом. Он сохраняет это преобразование локального адреса в глобальный в своей NAT-таблице, как показано на рис. 11.4.

После этого пакет направляется получателю. В среде “клиент-сервер” сервер может ответить пакетом, возвращающимся к маршрутизатору RTA с глобальным адресом 179.9.8.80, как показано на рис. 11.5.

В ситуации, показанной на рис. 11.6, процесс адресации NAT просматривает пакет, направленный из внешней сети во внутреннюю и просматривает свою адресную таблицу для нахождения преобразования данного глобального адреса в локальный. После этого глобальный адрес в поле получателя пакета заменяется на локальный и пакет пересылается по внутренней сети.

В терминах NAT-адресации под внутренней сетью понимается набор сетей, для которых осуществляется трансляция адресов. Понятие внешней сети относится ко всем остальным адресам. Обычно это зарегистрированные адреса, расположенные в Internet.

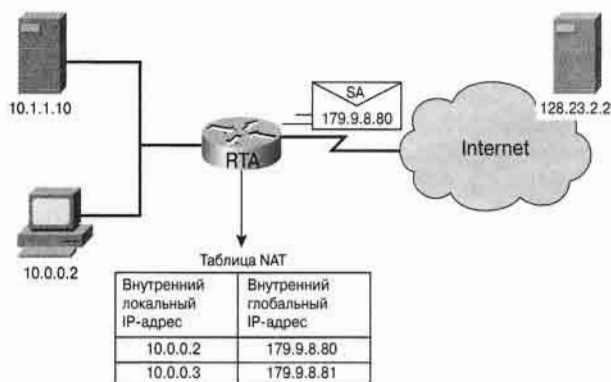


Рис. 11.4. Адресная таблица NAT

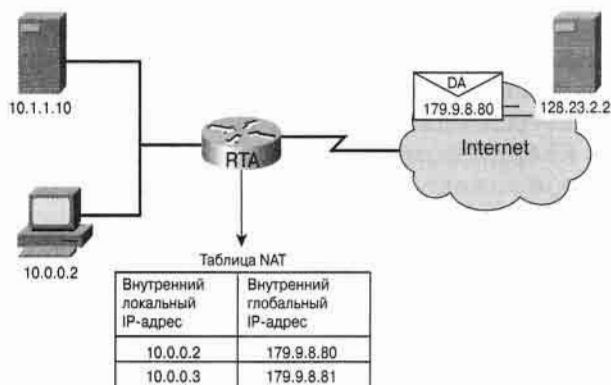


Рис. 11.5. Адресация NAT: получение ответного пакета

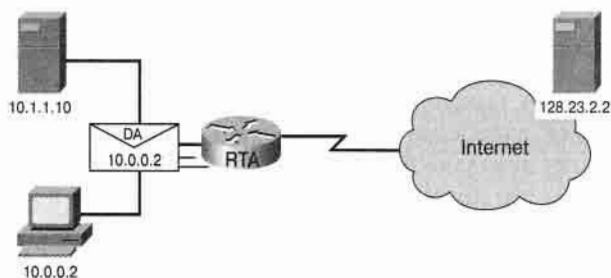


Рис. 11.6. Адресация NAT: окончание пересылки пакета

В качестве составной части этих функций адресация NAT может быть сконфигурирована для анонсирования только одного адреса для всей сети для внешнего мира. Такой способ эффективно скрывает внутреннюю структуру сети от внешнего мира и повышает уровень безопасности. Эта функция адресации NAT называется статической PAT; она проиллюстрирована на рис. 11.7 и 11.8. Понятие PAT также употребляется в конфигурировании IOS Cisco. Использование адресации NAT позволяет выполнить трансляцию ряда внутренних адресов, в то время как PAT может транслировать лишь один или несколько внешних адресов. Как показано на рис. 11.7, уз-

ды 10.0.0.2 и 10.0.0.3 посылают пакеты во внешнюю среду, используя один IP-адрес 179.9.8.80. Маршрутизатор регистрирует пакеты каждого узла путем добавления к внешнему IP-адресу уникального номера порта источника.

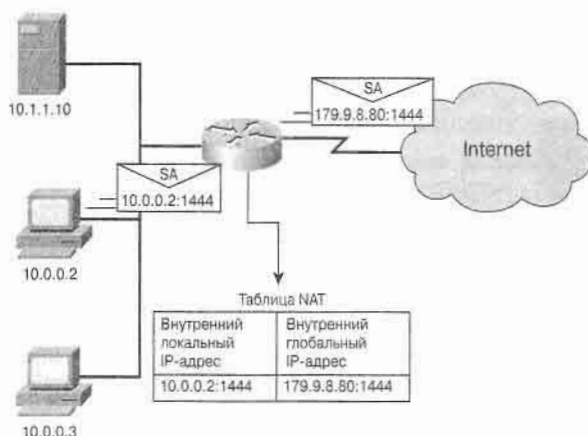


Рис. 11.7. Функционирование PAT-адресации

Для того, чтобы отличать транслированные адреса друг от друга адресация PAT использует во внутреннем глобальном IP-адресе уникальный номер порта источника. Поскольку номер порта записывается 16 битами, общее количество внутренних адресов, которые могут быть транслированы в один внешний адрес при использовании PAT теоретически может достигать 65 536 для каждого IP-адреса. PAT пытается сохранить первоначальный порт источника. Если порт источника уже выделен, то адресация PAT пытается найти первый доступный номер порта, начиная с соответствующей группы порта 0-511, 512-1023 или 1024-65535. Если в соответствующей группе порта нет доступных портов и конфигурируется более одного IP-адреса, то PAT переходит к следующему IP-адресу и пытается вновь выделить первоначальный порт источника. Это процесс продолжается до тех пор, пока PAT не исчерпает доступные порты и внешние IP-адреса.

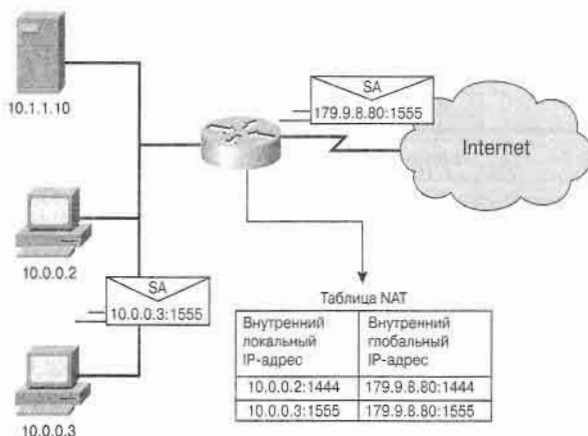


Рис. 11.8. Функционирование адресации PAT: окончание

Функции NAT и PAT

Адресация NAT может функционировать статически или динамически и использоваться в различных целях. Статическая NAT-адресация предназначена для взаимно однозначного преобразования локальных и глобальных адресов, как показано на рис. 11.9. Это особенно полезно для внутренних IP-узлов, которые должны быть доступны из Internet, таких как сервер DNS или сервер электронной почты (e-mail server).



Рис. 11.9. Статическая NAT-адресация

Динамическая NAT-адресация предназначена для преобразования незарегистрированных IP-адресов в зарегистрированный IP-адрес из группы зарегистрированных IP-адресов, как показано на рис. 11.10.



Рис. 11.10. Динамическая NAT-адресация

Корпорация Cisco определила для NAT-адресации следующие термины.

- Внутренние локальные адреса (*Inside local address*) — IP-адреса, назначенные узлу во внутренней сети; обычно это частные адреса, соответствующие RFC 1918.
- Внутренние глобальные адреса (*Inside global address*) — Зарегистрированные IP-адреса, назначаемые провайдером службы или выделяемые из регионального регистра Internet (Regional Internet Registries — RIR). Они предоставляют один или более внутренних локальных IP-адресов для связи с внешней сетевой средой.
- Внешние локальные адреса (*Outside local address*) — IP-адреса внешних узлов, в том виде как они известны узлам внутренней сети.

- Внешние глобальные адреса (*Outside global address*) — IP-адрес, назначаемый владельцем узла, этому узлу для использования во внешней сети.

Адресация NAT предоставляет следующие преимущества.

- **Отсутствует передача служебной информации, связанная с переадресацией, вызванной, например, сменой провайдера службы Internet.** Пропадает необходимость переадресации всех устройств, которым требуется доступ за пределами сети. Это сокращает финансовые затраты и экономит время.
- **Экономятся адреса за счет мультиплексирования на уровне “порт-приложение”.** При использовании NAT внутренние узлы могут совместно использовать один зарегистрированный IP-адрес для внешних связей. При этом типе связи требуется относительно немного внешних адресов для поддержки многих внутренних узлов, что экономит IP-адреса.
- **Повышается уровень безопасности в сети.** Поскольку частные сети не анонсируют свои адреса или внутреннюю топологию, они сохраняют высокий уровень безопасности, в сочетании с NAT для получения контролируемого внешнего доступа.

Конфигурирование NAT и PAT

В настоящем разделе рассматриваются следующие вопросы конфигурирования:

- статическая трансляция;
- динамическая трансляция;
- перезагрузка NAT (PAT).

Статическая трансляция

Под статической трансляцией понимается ручное конфигурирование адресов в просмотрной таблице. Конкретный внутренний локальный адрес преобразуется в заранее определенный внутренний глобальный адрес. Внутренний локальный и внутренний глобальный адреса статически преобразуются друг в друга. Это означает, что для каждого внутреннего локального адреса при использовании статической NAT требуется внутренний глобальный адрес. Для того, чтобы сконфигурировать статическую трансляцию внутреннего адреса, требуется выполнить действия, описанные в табл. 11.2.

Таблица 11.2. Конфигурирование статической адресации NAT

Этап	Действие	Примечания
1.	Задать статическую трансляцию внутреннего локального адреса во внутренний глобальный адрес. <code>Router(config)#ip nat inside source static local-ip global-ip</code>	Для удаления статической трансляции следует ввести в режиме глобального конфигурирования команду <code>no ip nat inside source static</code>
2.	Задать внутренний интерфейс <code>Router(config)#interface type Number</code> Пометить интерфейс как принадлежащий к внутренней сети <code>Router(config-if)#ip nat inside</code>	При вводе команды <code>interface</code> подсказка CLI изменяется с <code>(config)#</code> на <code>(config-if)#</code> .

Этап	Действие	Примечания
3.	<p>Задать выходной интерфейс.</p> <pre>Router(config-if)#interface type number</pre> <p>Пометить интерфейс как подсоединенный извне</p> <pre>Router(config-if)#ip nat outside</pre>	

Статическая трансляция записывается непосредственно в конфигурацию и эти преобразования можно увидеть в таблице трансляции. В примере 11.1 показаны соответствующие команды для маршрутизаторов IOS Cisco.

Пример 11.1. Конфигурирование статической адресации NAT

```
Router(config)#ip nat inside source static 10.1.1.2 192.168.1.2
Router(config)#interface s0
Router(config-if)#ip nat outside
Router(config-if)#interface e0
Router(config-if)#ip nat inside
```

На рис. 11.11 показано использование статической NAT. Маршрутизатор заменяет в пакете адрес источника 10.1.1.2 адресом 192.168.1.2. В примере 11.2 приведено конфигурирование шлюза.



Рис. 11.11. Пример статической адресации NAT

Пример 11.2. Конфигурирование шлюза

```
hostname GW
!
ip nat inside source static 10.1.1. 2 192.168.1.2
!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
interface Serial0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
ip nat inside source static 10.1.1.2 192.168.1.2
```


Динамическая трансляция адресов

При использовании динамической трансляции адресов преобразования адресов не существуют в NAT-таблице до тех пор, пока маршрутизатор не получит данные, для которых такая трансляция требуется (тип таких данных задается администратором). Динамические преобразования адресов являются временными и в конечном итоге устаревают и удаляются. Для того, чтобы сконфигурировать трансляцию внутренних адресов, следует выполнить действия, описанные в табл. 11.3.

Таблица 11.3. Конфигурирование динамической NAT

Этап	Действие	Примечание
1.	Задать набор глобальных адресов, которые будут использоваться по мере необходимости. Router(config)#ip nat pool имя нач-ип конеч-ип (netmask маска prefix-length длина-преф)	Для удаления набора глобальных адресов следует ввести в режиме глобального конфигурирования команду no ip nat pool
2.	Создать список доступа для идентификации хостов при трансляции Router(config)#access-list номер- списка permit источник [шаблон-источн]	Для удаления списка доступа следует ввести в режиме глобального конфигурирования команду no access-list номер-списка
3.	Сконфигурировать динамический NAT на основе адресов источника Router(config)#ip nat inside source list номер-списка-дост pool имя	Для удаления динамического NAT следует ввести в режиме глобального конфигурирования команду no ip nat inside source
4.	Указать внутренний интерфейс Router(config)#interface тип номер Router(config-if)#ip nat inside	После ввода команды interface , приглашение командной строки изменяется с (config)# на (config-if)#
5.	Указать внешний интерфейс Router(config)#interface тип номер Router(config-if)#ip nat outside	

При динамической трансляции задается пул глобальных адресов, в которые могут быть преобразованы внутренние адреса, как показано в примере 11.3.

Пример 11.3. Конфигурирование динамической NAT

```
Router(config)#ip nat pool nat-pool 179.9.8.80 179.9.8.95 netmask
255.255.255.0 255.255.255.240
```

Список доступа должен определять только те адреса, которые следует транслировать. Следует помнить о том, что неявная команда **deny all** присутствует в каждом списке доступа. Недостаточно строгий список доступа может привести к непредсказуемым результатам. Cisco настоятельно рекомендует не конфигурировать списки доступа, на которые ссылаются команды NAT с **permit any**. Использо-

ние **permit any** может привести к тому, что NAT будет потреблять слишком много ресурсов маршрутизатора, что может вызвать проблемы в сети.

Приведенные ниже команды конфигурируют соответствующие интерфейсы для выполнения внутренних и внешних функций.

```
Router(config)#interface s0
Router(config-if)#ip nat outside
Router(config-if)#interface e0
Router(config-if)#ip nat inside
```

В примере на рис. 11.12 происходит трансляция всех адресов, проходящих через список доступа 1 (имеющие адрес источника от 10.0.0.0/16) в адрес из пула с именем *nat-pool*. Этот пул содержит адреса из диапазона от 179.9.8.80 до 179.9.8.95.



Рис. 11.12. Пример работы адресации PAT

Конфигурирование для GW показано в примере 11.4.

Пример 11.4. Конфигурирование для GW

```
<вывод пропущен>
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface fastethernet0/0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
interface Serial0/0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
```

ПРИМЕЧАНИЕ

NAT не будет транслировать адрес узла 10.1.1.2, поскольку его трансляция не разрешена списком доступа.

Перезагрузка NAT

Одной из наиболее мощных функций NAT является способность использовать PAT. Это иногда называется NAT-адресацией “много-в-один” или перегрузкой адреса. При использовании перегрузки (*overloading*) сотни узлов с частными адресами могут получать доступ к Internet, используя лишь один глобальный адрес. NAT-

маршрутизатор отслеживает различные сеансы связи устанавливая соответствие TCP и номеров портов UDP в таблице трансляции.

Для того, сконфигурировать перегрузку внутренних глобальных адресов, следует выполнить действия, описанные в табл. 11.4.

Таблица 11.4 Конфигурирование перегрузки в NAT

Этап	Действие	Примечание
1.	<p>Определить стандартный список доступа, разрешающий те адреса, которые должны транслироваться</p> <pre>Router(config)#access-list номер-списка permit источник [шаблон-источн]</pre>	Для удаления списка доступа следует ввести в режиме глобального конфигурирования команду no access-list номер-списка
2.A.	<p>Сконфигурировать динамический NAT на основе адресов источника, указать список доступа, определенный на предыдущем этапе.</p> <pre>Router(config)#ip nat inside source list номер-списка-дост interface интерфейс overload</pre>	Для удаления динамического NAT следует ввести в режиме глобального конфигурирования команду no ip nat inside source . Ключевое слово overload задает PAT.
2.B.	<p>Задать набор глобальных адресов, которые будут использоваться для перегрузки.</p> <pre>Router(config)#ip nat pool имя ip-адр (netmask маска prefix-length длина-преф)</pre> <p>Запустить трансляцию с перегрузкой.</p> <pre>Router(config)#ip nat inside source list номер-списка-дост pool имя overload</pre>	
3.	<p>Указать внутренний интерфейс</p> <pre>Router(config)#interface тип номер</pre> <pre>Router(config-if)#ip nat inside</pre>	После ввода команды interface , приглашение командной строки изменяется с (config) # на (config-if) #
4.	<p>Указать внешний интерфейс</p> <pre>Router(config)#interface тип номер</pre> <pre>Router(config-if)#ip nat outside</pre>	

Следует определить стандартный IP-список доступа, разрешив внутренние локальные, для которых должна выполняться трансляция, как показано в примере 11.5..

Пример 11.5. Стандартный список доступа для IP-адресов

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255
```

Задать перегрузку трансляции, указав IP-адрес, который должен быть перегружен, как адрес, назначенный внешнему интерфейсу (Пример 11.6).

Пример 11.6. Перегрузка на интерфейсе

```
Router(config)#ip nat inside source list 1 interface serial0/0 overload
```

Задать перегрузку трансляции, указав IP-адрес, который должен быть перезагружен, как адрес, назначенный имени пула (Пример 11.7).

Пример 11.7. Перегрузка с использованием пула

```
Router(config)#ip nat pool nat-pool2 179.9.8.20 netmask  
255.255.255.240  
Router(config)#ip nat inside source list 1 pool nat-pool2 overload  
Router(config)#interface s0  
Router(config-if)#ip nat outside  
Router(config-if)#interface ethernet 0  
Router(config-if)#ip nat inside
```

**Лабораторная работа: конфигурирование NAT**

В этой работе требуется сконфигурировать маршрутизатор, используя NAT для преобразования внутренних частных IP-адресов во внешние общедоступные адреса.

**Лабораторная работа: конфигурирование PAT**

В этой работе требуется сконфигурировать маршрутизатор, используя PAT для преобразования внутренних частных IP-адресов во внешние общедоступные адреса.

**Лабораторная работа: конфигурирование статических NAT-адресов**

В этой работе требуется сконфигурировать маршрутизатор, используя PAT для преобразования внутренних частных IP-адресов во внешние общедоступные адреса. Требуется также задать статические IP-преобразования для обеспечения внешнего доступа к внутренним персональным компьютерам.

Тестирование конфигурации NAT и PAT

После того, как NAT сконфигурирована, следует выполнить ее тестирование с помощью команд **clear** и **show**.

По умолчанию время существования преобразования в NAT-таблице равно периоду неиспользования. Если трансляция порта не сконфигурирована, то период существования преобразования равен 24 часам, кроме случая когда было выполнено реконфигурирование с помощью команды **ip nat translation**. Для очистки позиций таблицы до истечения интервала таймера используется одна из команд, приведенных в табл. 11.5.

Таблица 11.5. Команды очистки позиций NAT-таблицы

Команда	Описание
<code>clear ip nat translation *</code>	Удаляет все элементы таблицы NAT, соответствующие динамической трансляции адресов
<code>clear ip nat translation inside глоб-ip лок-ip [outside лок-ip глоб-ip]</code>	Удаляет указанный элемент таблицы NAT, соответствующий внутреннему адресу или как внутреннему, так и наружному адресу
<code>clear ip nat translation protocol inside глоб-ip глоб-порт лок-ip лок-порт [outside лок-ip лок-порт глоб-ip глоб-порт]</code>	Удаляет расширенный элемент таблицы NAT

Для отображения информации о трансляции следует выполнить в привилегированном EXEC-режиме одну из команд, приведенных в табл. 11.6.

Таблица 11.6. Команды отображения информации о трансляции

Команда	Описание
<code>show ip nat translation</code>	Отображает активные сеансы трансляции адресов
<code>show ip nat statistics</code>	Отображает статистику трансляций

Другим вариантом является использование команды **show run** для просмотра NAT, списка доступа, интерфейса или команд **pool** с соответствующими параметрами.



Лабораторная работа: тестирование конфигурации NAT и PAT

В этой работе требуется выполнить тестирование функционирования NAT и PAT, правильно используя команды **clear** и **show**.

Поиск и устранение ошибок в конфигурировании NAT и PAT

Когда в среде NAT возникают проблемы связи по протоколу IP, причину проблемы найти бывает нелегко. Часто в таких случаях обвиняют саму адресацию NAT, в то время как причина может оказаться значительно глубже.

В случае наличия проблем в IP-соединениях, целесообразнее исключить NAT из числа возможных проблем. Для проверки правильности функционирования NAT следует выполнить приведенные ниже действия.

- Этап 1.** В зависимости от конкретной конфигурации необходимо ясно определить, для решения каких задач предполагается использование NAT.
- Этап 2.** Проверить правильность соответствующих преобразований адресов в таблице трансляции.
- Этап 3.** Проверить, что трансляция функционирует с помощью команд **show** и **debug**.
- Этап 4.** Подробно проследить что происходит с пакетами и убедиться в том, что маршрутизаторы обладают правильной информацией маршрутизации для последующей пересылки пакета.

Для тестирования функций NAT используется команда **debug ip nat**, которая отображает информацию обо всех пакетах, транслируемых маршрутизатором. По команде **debug ip nat detailed** выводится описание каждого пакета, для которого предполагается трансляция. При этом также выводится информация об определенных ошибках или исключительных условиях, таких, например, как невозможность выделить глобальный адрес.

В примере 11.8 приведен вывод по команде **debug ip nat** для сети, показанной на рис. 11.13. В этом примере первые две строки описывают отладочный вывод, производимый запросом системы доменных имен (Domain Name System — DNS) и соответствующим ответом. В остальных строках приводится отладочный вывод от соединения Telnet между узлом находящимся внутри сети и узлом вне ее.

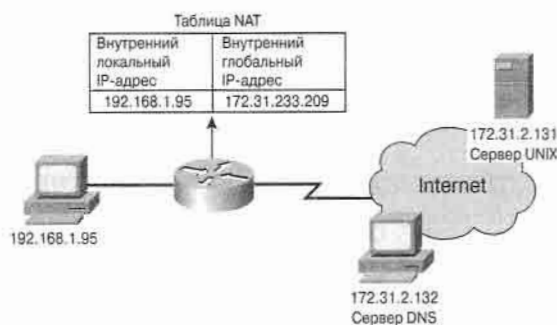


Рис. 11.13. Использование отладочных команд адресации NAT

Пример 11.8. Вывод по команде **debug ip nat**

```
Router#debug ip nat
NAT: s=192.168.1.95->172.31.233.209, d=172.31.2.132 [6825]
NAT: s=172.31.2.132, d=172.31.233.209->192.168.1.95 [21852]
NAT: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6826]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23311]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6827]
NAT*: s=192.168.1.95->172.31.233.209, d=172.31.1.161 [6828]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23313]
NAT*: s=172.31.1.161, d=172.31.233.209->192.168.1.95 [23325]
```

Ниже приведены пояснения для отдельных элементов вывода по команде **debug**:

- **NAT** — Символ звездочки (*) за аббревиатурой NAT указывает на то, что трансляция происходит по маршруту быстрой коммутации. Первый пакет при обмене информацией всегда проходит по медленному маршруту (т.е. коммутируется самим процессом). Остальные пакеты пройдут по маршруту быстрой коммутации при условии, что существует соответствующая позиция в кэше.
- **s** = *a.b.c.d* — *a.b.c.d* = адрес источника.
- **a.b.c.d->w.x.y.z** — *w.x.y.z* = адрес, в который был преобразован адрес источника.
- **d** = *a.b.c.d* — *a.b.c.d* = адрес получателя.

- [23325] — Значение в скобках представляет собой идентификационный IP-номер. Эта информация может оказаться полезной при отладке, поскольку она позволяет выполнить корреляцию с другими данными о прохождении пакета, например, от анализаторов протокола.



Лабораторная работа: поиск и устранение ошибок в конфигурации NAT и PAT

В этой работе требуется найти ошибки в конфигурациях NAT и PAT с помощью команд **show** и **debug**.

Преимущества и недостатки NAT

Использование NAT-адресации предоставляет следующие преимущества.

- NAT сохраняет зарегистрированную схему адресации путем приватизации сетей интранет.
- NAT повышает гибкость системы соединений с открытой сетью. Для обеспечения надежной системы соединений с открытой сетью могут быть созданы множественные пулы, резервные пулы и пулы распределения/балансирования нагрузки. Деприватизация сети требует полного изменения адресации в уже существующей сети; при этом расходы пропорциональны количеству узлов и требуется переход к новой схеме адресации. NAT позволяет сохранить существующую схему и при этом поддерживает новую назначенную схему адресации вне данной (уже существующей) частной сети.

Вместе с тем NAT не лишена недостатков. Недостатком трансляции адресов является понижение функциональности, особенно для протоколов и приложений включающих в себя рассылку информации об IP-адресах в полезной нагрузке IP-сообщений. Это требует дополнительной поддержки с помощью блока NAT. К недостаткам NAT можно отнести следующее.

- NAT увеличивает задержку. Задержка коммутации на маршруте конечно, увеличивается, поскольку требуется трансляция каждого IP-адреса в заголовках пакета. Производительность также может понизиться, поскольку NAT в настоящее время реализуется путем использования коммутации процесса. Центральный процессор CPU должен рассматривать каждый пакет и решать, требуется ли ему трансляция, а затем изменять IP-заголовок, и, возможно, TCP-заголовок. Маловероятно, что этот процесс можно легко кэшировать.
- Другим серьезным недостатком при реализации и использовании NAT является потеря полной сквозной трассировки. Значительно труднее становится трассировать пакеты, которые претерпевают многочисленные изменения адресов при прохождении по нескольких NAT-переходах. Однако такое развитие событий повышает безопасность каналов, поскольку хакерам, пытающимся определить источник пакета, становится трудно, если не невозможно, проследить путь пакета или определить первоначальный адрес источника или получателя.
- NAT также приостанавливает функционирование некоторых приложений, использующих IP-адресацию, поскольку при этом становятся недоступными сквозные IP-адреса. Приложения, использующие физические адреса вместо

квалифицированных доменных имен, не смогут достичь пунктов назначения, адреса которых транслируются в NAT-маршрутизаторе. Иногда эту проблему удается обойти путем реализации статических NAT-преобразований.

- NAT поддерживает передачу данных протоколов TCP/UDP, у которых в данных приложения не передаются IP-адреса источника или получателя, таких как HTTP, TFTP и Telnet.

Хотя в приведенных ниже типах данных в потоках данных приложений передаются IP-адреса, ниже приведены приложения, которые поддерживаются адресацией NAT IOS Cisco.

- ICMP.
- Протокол передачи файлов (File Transfer Protocol — FTP) (включая команды **PORT** и **PASV**).
- NetBIOS по протоколу TCP/IP (службы дейтаграмм, имен и сеансов).
- RealAudio of Progressive Networks.
- CuSeeMe of White Pines.
- Streamworks of Xing Technologies.
- DNS-запросы “A” и “PTR”.
- NetMeeting (2.1, 2.11 & 3.01).
- H.323v2 (Сообщения типов H.225/245 кроме RAS - 12.1(5)T).
- VDOLive [11.3(4)/11.3(4)T и более поздние].
- Vxtreme [11.3(4)/11.3(4)T и более поздние].
- Многоадресатная IP-рассылка [12.0(1)T] (трансляция только адреса источника).

NAT Cisco IOS *не* поддерживает следующие типы данных.

- Обновления таблиц маршрутизации.
- Передачи в зонах DNS
- BOOTP.
- talk, ntalk.
- простой протокол управления сетью (Simple Network Management Protocol — SNMP).
- NetShow.

Обзор протокола DHCP

Маршрутизаторы, серверы и другие ключевые узлы обычно требуют задания конкретных IP-адресов. Однако для пользователей настольных систем, как правило, достаточно любого адреса из некоторого диапазона. Такой диапазон обычно находится в диапазоне адресов IP-подсети. Такой пользователь находится в некоторой конкретной подсети и может иметь любой адрес из диапазона, а все остальные установки принимаются по умолчанию. Эти установки включают в себя маску подсети, шлюз по умолчанию и адрес сервера DNS для сети или подсети.

Конфигурирование узла, подсоединенного к TCP/IP Internet требует задания нескольких значений:

- IP-адрес;
- маска подсети;
- шлюз по умолчанию;
- адрес сервера DNS.

Этот список является минимальным; в него могут включаться другие переменные в зависимости от сетевой среды. Эти переменные приходится конфигурировать вручную на каждом IP-узле. Обычно они хранятся в файле конфигурации и доступ к ним осуществляется компьютером при загрузке.

Кроме того, некоторые пользователи не имеют жестких дисков, а операционная система и программное обеспечение хранятся в оперативной памяти. Производитель чипа ROM, естественно, не может знать параметры конкретной IP-конфигурации при изготовлении чипа, поэтому их невозможно изменить. Конфигурацию приходится устанавливать после загрузки компьютера. В таких средах задавать эти IP-значения динамически при загрузке компьютера невозможно. Протокол DHCP предназначен для решения этой задачи. Поскольку пользователи настольных компьютеров составляют основную часть узлов сети, протокол DHCP оказался хорошим помощником сетевого администратора.

Установка в сети протокола DHCP

Протокол DHCP, который работает в режиме клиент-сервер, позволяет узлам (клиентам DHCP) сети IP получать свои конфигурации с сервера (сервера DHCP). Это сокращает объем работ по администрированию IP-сети. Наиболее важной опцией конфигурации, которую клиент получает от сервера, является IP-адрес. Протокол DHCP описан в RFC 2131.

Клиент DHCP является частью большинства современных операционных систем, таких как Windows 9x/NT/ 2000/XP, Solaris, Linux и MAC OS. Клиентская часть запрашивает значения конфигурации из сети. В сети должен иметься сервер DHCP, который управляет выделением IP-параметров и отвечает на запросы клиентов. Сервер DHCP может быть ответственным за ответы на запросы от многих подсетей. Протокол DHCP не предназначен для конфигурирования маршрутизаторов, коммутаторов и серверов, поскольку для этих узлов необходимо иметь статический IP-адрес.

Протокол DHCP конфигурирует сервер для раздачи клиентам их IP-параметров и другой информации. Клиенты арендуют эти параметры у сервера на задаваемый администратором период. Когда время такой аренды истекает, клиент должен запросить другой адрес, хотя обычно ему назначается тот же самый.

Обычно администраторы предпочитают для обеспечения служб DHCP использовать сервер Microsoft NT/2000/XP или компьютер UNIX, поскольку такие решения масштабируемы и относительно легко управляются. Но и набор функций IOS Cisco (Easy IP) обеспечивает полнофункциональный сервер DHCP, который может предоставляться маршрутизатором. По умолчанию он предоставляет конфигурации на 24 часа. Эта функция полезна в малых и домашних офисах, которые могут воспользоваться преимуществами DHCP и NAT без использования сервера-компьютера.

Администраторы устанавливают серверы DHCP для назначения адресов из заранее определенных пулов. Серверы DHCP могут также предоставлять другие параметры, такие как адреса серверов DNS, серверов WINS и имена доменов. Кроме того, большинство серверов DHCP позволяют администратору конкретно указать, какие MAC-адреса клиентов должны обслуживаться и автоматически назначать им каждый раз одни и те же IP-адреса.

Клиент DHCP посылает широковещательный запрос в виде пакета запроса DHCP. В простейшем случае сервер DHCP находится в этом же сегменте и принимает этот запрос.

На рис. 11.14-11.16 проиллюстрирован процесс обмена сообщениями запросов и ответов. Сервер обнаруживает, что поле GIADDR не заполнено и делает вывод о том, что клиент находится в этом же сегменте. Он также регистрирует аппаратный адрес клиента, как показано на рис. 11.14.

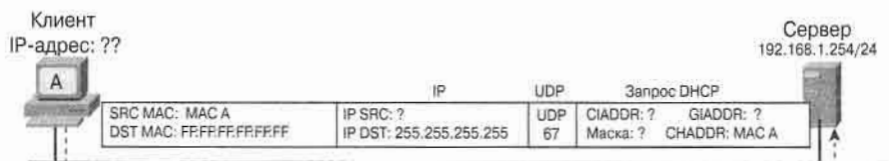


Рис. 11.14. Начало процесса DHCP

Сервер DHCP выбирает IP-адрес из пула доступных для данного сегмента, а также другой сегмент и глобальные параметры. После этого сервер DHCP помещает эту информацию в соответствующие поля пакета DHCP. Сервер использует аппаратный адрес A (в CHADDR) для создания соответствующего фрейма, который будет отправлен клиенту, как показано на рис. 11.15.

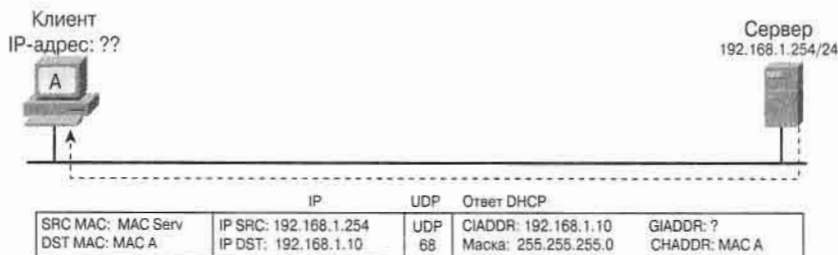


Рис. 11.15. Ответ сервера DHCP

Операционная система клиента DHCP использует эти значения в DHCP-ответе для конфигурирования стека протокола IP для данного клиента, как показано на рис. 11.16.



Рис. 11.16. Работа протокола DHCP закончена

Протокол DHCP использует UDP в качестве своего транспортного протокола. Клиент посылает сообщения на сервер, на порт 67, а сервер отправляет свои с порта 68.

Различия между протоколами BOOTP и DHCP

Internet-сообщество первоначально разработало протокол начальной загрузки (*Bootstrap Protocol — BOOTP*) для конфигурирования в сети бездисковых пользователей. Протокол BOOTP был первоначально определен в RFC 951 в 1985 году. Будучи предшественником DHCP, BOOTP обладает рядом общих с ним характеристик. Оба протокола работают в режиме “клиент-сервер” и используют порты 67 и 68 протокола UDP, известные как порты BOOTP, поскольку этот протокол появился раньше DHCP.

BOOTP обеспечивает четыре уже упомянутых IP-параметра.

Однако BOOTP не является динамическим. Когда клиент запрашивает IP-адрес, сервер BOOTP ищет в заранее заданной таблице позицию, соответствующую MAC-адресу клиента. Если такая позиция существует, то клиенту направляется соответствующий IP-адрес. Это означает, что связь между MAC-адресом и IP-адресом должна быть уже заранее сконфигурирована на сервере BOOTP.

DHCP определяет механизмы, посредством которых клиентам могут быть назначены IP-адреса на некоторый конечный период времени, что позволяет позднее переназначить IP-адрес другому клиенту или назначить этому же клиенту другой адрес, если он перемещается в другую подсеть. Клиенты могут продлить срок аренды уже имеющегося у них адресов.

DHCP предоставляет клиентам механизм сбора другой IP-информации (например, таких параметров, как WINS или доменные имена), которые требуются ему для работы в сети TCP/IP.

В табл. 11.7 приведены различия между протоколами DHCP и BOOTP.

Таблица 11.7. Протоколы DHCP и BOOTP

BOOTP	DHCP
Статическое отображение	Динамическое отображение
Постоянные назначения	Временные назначения
Поддерживает до 4 параметров конфигурации	Поддерживает более 30 параметров конфигурации
Используется для пересылки образа программы начальной загрузки на узел сети	Не может использоваться для пересылки образа программы начальной загрузки на узел сети

Функции протокола DHCP

Имеются три механизма назначения клиенту IP-адреса.

- **Автоматическое выделение (Automatic allocation)**—DHCP.
- **Ручное выделение (Manual allocation)**— адрес назначается клиенту администратором, а DHCP передает этот адрес клиенту.
- **Динамическое выделение (Dynamic allocation)** — DHCP назначает клиенту IP-адрес на ограниченное время (аренда).

Центральной темой данного раздела является механизм динамического выделения адресов. Некоторые из доступных параметров конфигурации приведены в IETF RFC 1533. Ниже приведены часть из них.

- IP-адрес.
- Маска подсети.
- Маршрутизатор (стандартный шлюз).
- Доменное имя.
- Сервер доменных имен.
- Сервер имен (такой как WINS).

Рассмотрим ситуацию на рис. 11.17. Сервер DHCP создает пул IP-адресов и ассоциированных параметров. Пулы предназначены для отдельных логических IP-подсетей, что позволяет нескольким серверам DHCP отвечать одной подсети; в сущности, IP-клиенты могут быть и мобильными. Если ответить могут несколько серверов, то клиент может получить сразу несколько предложений, однако клиент может выбрать только один сервер. В примере 11.9 показана информация, которую сервер DHCP посылает своему клиенту.



Рис. 11.17. Клиент и сервер протокола DHCP

Пример 11.9. Файл конфигурации протокола DHCP

```
IP Address: 192.204.18.7
Subnet Mask: 255.255.255.0
Default Routers: 192.204.18.1, 192.204.18.3
DNS Servers: 192.204.18.8, 192.204.18.9
Lease Time: 5 days
```

Клиенты DHCP реализованы в ряде операционных систем различных производителей, включая Windows 3.1, Windows 9x, Windows NT, Windows 2000, Windows XP, Solaris, Linux, MAC OS, Novell NetWare, FTP Software, NetManage и Cisco.

Функционирование протокола DHCP

Процесс конфигурирования клиента DHCP показан на рис. 11.18.

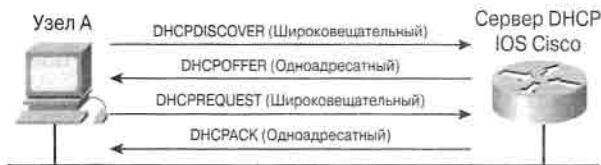


Рис. 11.18. Процесс обнаружения сервера протокола DHCP

Этот процесс включает в себя пять этапов, описанных ниже.

1. **Клиент посылает широковещательное сообщение DHCPDISCOVER всем узлам** — клиент сконфигурирован для использования протокола DHCP. Клиент посылает запрос какому-либо серверу на предоставление параметров IP-конфигурации (обычно во время загрузки). Возможен вариант, когда клиент сам предлагает IP-адрес, который он желает использовать (например, при запросе продления срока аренды). После этого клиент пытается найти сервер DHCP рассылая широковещательное сообщение (255.255.255.255), называемое сообщением DHCPDISCOVER в своем локальном сегменте.
2. **Сервер посылает одноадресатное сообщение DHCPOFFER клиенту** — после получения широковещательного сообщения сервер определяет, может ли он обслужить этот запрос на основе своей собственной базы данных. Если он не может обслужить запрос, то может переслать запрос другому DHCP-серверу (серверам), в зависимости от конфигурации. Если же он может обслужить запрос самостоятельно, то он предлагает клиенту конфигурационную IP-информацию в виде одноадресатного сообщения DHCPOFFER. Сообщение DHCPOFFER представляет собой предлагаемую конфигурацию, которая может включать в себя IP-адрес, адрес сервера DNS и срок аренды.
3. **Клиент рассылает широковещательное сообщение DHCPREQUEST всем узлам** — если клиент находит полученное предложение подходящим, то он рассылает новое широковещательное сообщение DHCPREQUEST, запрашивая именно эти конкретные IP-параметры. Возникает вопрос: почему клиент рассылает этот новый запрос широковещательно, а не одноадресатным сообщением конкретному серверу (от которого получено предложение)? Широковещание используется потому, что его первый запрос DHCPDISCOVER мог быть получен более чем одним сервером DHCP. Если предложения были сделаны более чем одним сервером, то данное широковещательное сообщение DHCPREQUEST уведомляет всех остальных, что предложение было принято. Обычно клиент принимает первое сделанное предложение.
4. **Сервер посылает одноадресатное сообщение DHCPACK клиенту** — сервер, получающий сообщение DHCPREQUEST, делает конфигурацию активной путем отправки одноадресатного сообщения-подтверждения DHCPACK. Следует отметить, что возможен, хотя и крайне маловероятен случай, когда сервер не отправляет сообщения DHCPACK, поскольку за это время предоставил эту информацию другому клиенту. Получение сообщения DHCPACK позволяет клиенту немедленно начать использование назначенного ему адреса.

Если клиент обнаруживает, что этот адрес уже используется в данном локальном сегменте, то он отправляет сообщение DHCPDECLINE и процесс начи-

нается снова если клиент получает сообщение DHCPNAK от сервера после отправки сообщения DHCPREQUEST, то он начинает повторно весь процесс.

5. **Клиент освобождает IP-адрес** — если клиенту больше не нужен его IP-адрес, то он отправляет серверу сообщение DHCPRELEASE. В зависимости от политики организации возможны варианты, для конечного пользователя или администратора есть возможность статически назначить узлу IP-адрес, принадлежащий пулу адресов сервера DHCP. На всякий случай сервер DHCP IOS Cisco перед тем как предложить адрес клиенту всегда проверяет, не находится ли он в использовании. Перед отправкой клиенту сообщения DHCPOFFER сервер посылает эхо-запросы (выполняет команду ping) пулу адресов. По умолчанию количество эхо-запросов проверки потенциального IP-адреса равно двум, хотя оно может быть изменено в конфигурации.

Если сервер находится в другом сегменте, то для передачи запроса в этот другой сегмент может быть использован агент передачи протокола BOOTP.

Конфигурирование протокола DHCP

Как и NAT, сервер DHCP требует, чтобы администратор определил пул доступных адресов. Команда **ip dhcp pool** определяет, какие адреса будут выделены узлам. Эта команда имеет следующий синтаксис:

```
Router(config)#ip dhcp pool name1
Router(dhcp-config)#network ip-address mask
```

Первая команда, **ip dhcp pool name1**, создает пул с именем *name1* и переводит маршрутизатор в специализированный режим конфигурации DHCP. В этом режиме данная команда определяет диапазон адресов, которые будут отдаваться в аренду. Если какие-либо сетевые адреса требуется исключить, то необходимо вернуться в глобальный режим и выполнить команду **ip dhcp excluded-address**. Для выхода из режима конфигурирования DHCP следует ввести команду **exit**.

Команда **ip dhcp excluded-address** конфигурирует на маршрутизаторе исключение адреса или диапазона адресов при их назначении клиентам. Эта команда может использоваться для резервирования адресов, которые назначены статически ключевым узлам, например, маршрутизаторам. Команда имеет следующий синтаксис:

```
Router(config)#ip dhcp excluded-address ip-address [ end-ip-address]
```

Как правило сервер DHCP конфигурируется для назначения более чем одного IP-адреса. В режиме конфигурирования DHCP можно установить и другие параметры IP-конфигурации. Клиенты IP не смогут серьезно работать без шлюза по умолчанию. Такой шлюз задается командой **defaultrouter**. Можно также сконфигурировать адрес сервера DNS (командой **dns-server**) или сервер WINS (командой **netbios-name-server**). Практически DHCP-сервер IOS может предоставить своим клиентам любую информацию TCP/IP.

Список ключевых команд для сервера DHCP, которые могут быть выполнены в режиме конфигурирования пула DHCP, приведен в табл. 11.8.

Таблица 11.8. Команды конфигурирования пула DHCP

Команда	Описание
<code>Router(config)#ip dhcp pool имя</code>	Назначает имя набору адресов DHCP-сервера и переводит устройство в режим конфигурирования пула DHCP (об этом свидетельствует изменение приглашения на <code>config-dhcp#</code>)
<code>Router(config-dhcp)#network номер-сети [маска /префикс-длина]</code>	Определяет номер и маску подсети для набора адресов DHCP-сервера. Параметр <i>префикс-длина</i> определяет количество битов в адресе, соответствующих префиксу подсети. Указание префикса — это еще один способ определения маски подсети для клиента. Длина префикса в битах указывается через косую черту после адреса подсети
<code>Router(config-dhcp)#domain-name имя</code>	Определяет доменное имя клиента
<code>Router(config-dhcp)#dns-server адр [адр2 адр3...адр8]</code>	Определяет IP-адрес DNS-сервера, которым должны пользоваться клиенты DHCP. Как минимум должен быть указан один IP-адрес. В одной строке можно указать до 8 IP-адресов серверов DNS
<code>Router(config-dhcp)#netbios-name-server адр [адр2 адр3...адр8]</code>	Определяет адрес WINS-сервера протокола NetBIOS, которым должны пользоваться клиенты Microsoft DHCP. Как минимум должен быть указан один адрес. В одной строке можно указать до 8 адресов серверов
<code>Router(config-dhcp)#default-router адр [адр2 адр3...адр8]</code>	Определяет IP-адрес стандартного маршрутизатора для клиента DHCP. Как минимум должен быть указан один IP-адрес. В одной строке можно указать до 8 IP-адресов маршрутизаторов
<code>Router(config-dhcp)#lease {дни [часы] [минуты]}</code>	Определяет длительность аренды. По умолчанию один день

Хотя это принимается по умолчанию во всех версиях IOS Cisco, поддерживающих DHCP, процесс сервера DHCP может быть повторно инициализирован с использованием команды глобального конфигурирования **service dhcp**. Отключает сервер команда **no service dhcp**.

Тестирование работы протокола DHCP

В табл. 11.9 приведены команды, которые при необходимости используются в EXEC-режиме.

Таблица 11.9 Команды отображения информации о сервере DHCP

Команда	Описание
<code>Router>show ip dhcp binding [адр]</code>	Отображает список всех привязок, созданных на указанном DHCP-сервере
<code>Router>show ip dhcp conflict [адр]</code>	Отображает список всех конфликтов адресов, зарегистрированных на указанном DHCP-сервере

Окончание табл. 11.9

Команда	Описание
Router>show ip dhcp database [url]	Отображает свежую статистику активности базы данных DHCP. Эту команду можно использовать только в привилегированном EXEC-режиме.
Router>show ip dhcp server statistics	Отображает накопленную статистическую информацию о деятельности сервера и полученных и отосланных сообщениях

Поиск и устранение ошибок в конфигурации DHCP

Для включения режима отладки сервера DHCP следует использовать команду привилегированного EXEC-режима **debug ip dhcp server**. В табл. 11.10 приведены команды отладки сервера DHCP.

Таблица 11.10. Команды отладки сервера DHCP

Команда	Описание
debug ip dhcp server events	Выводит список событий сервера, таких как назначение адресов или обновление базы данных
debug ip dhcp server packets	Декодирует полученные и отосланные пакеты
debug ip dhcp server linkage	Отображает информацию базы данных о связях (например, такую как отношения "родитель-потомок" в базисном дереве)

Для поиска и устранения ошибок работы сервера DHCP следует использовать команду **debug ip dhcp server events**, как показано в примере 11.10.

Пример 11.10. Команда отладки DHCP

```
Router#debug ip dhcp server events
Router#
00:22:53: DHCPD: checking for expired leases.
00:23:23: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a4.97f4.6d.
00:27:49: DHCPD: returned 172.16.13.11 to address pool remote.
00:29:59: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a4.97f4.6d.
```

Этот вывод показывает, что периодически сервер проверяет, не истекло ли у кого-либо из клиентов время аренды. Можно также увидеть, какие адреса возвращаются и когда они выделяются.

Передача DHCP

Как было показано ранее, клиенты протокола DHCP используют широковещательные IP-пакеты для нахождения в сегменте сервера DHCP. Однако что происходит, если клиент и сервер находятся в разных сегментах и разделены маршрутизатором? Маршрутизаторы не пересылают такие широковещательные сообщения.

DHCP не единственная важная служба, которая использует широковещание. Маршрутизаторы Cisco и другие устройства могут использовать широковещание для поиска серверов протокола простой передачи файлов (Trivial File Transfer Protocol — TFTP). Некоторым клиентам может потребоваться найти сервер Terminal Access Controller Access Control System (Terminal Access Controller Access Control System — TACACS). Обычно в сложной иерархической сети клиенты находятся в той же подсети, где и ключевые серверы. Удаленные клиенты для поиска этих серверов рассылают широковещательные сообщения, но по умолчанию маршрутизаторы не пересылают эти сообщения за пределы своих подсетей.

Поскольку некоторым клиентам такие службы как DHCP жизненно необходимы, приходится выбирать одно из двух решений: размещать серверы во всех подсетях или использовать функцию Cisco IOS `helper address`. На некоторых компьютерах реализация таких служб, как DHCP или DNS создает избыточную служебную нагрузку и головную боль у администраторов, поэтому первый из упомянутых выше способов мало привлекателен. Когда это оказывается возможным, администраторы используют команду `ip helper-address` для передачи широковещательных запросов для этих ключевых служб протокола UDP.

При использовании функции `helper address` можно сконфигурировать маршрутизатор для приема широковещательного запроса на службу UDP, а затем переслать его как одноадресатный пакет на конкретный IP-адрес. По умолчанию команда `ip helper-address` пересылает пакеты следующих 8 служб UDP:

- служба (синхронизации) времени Time;
- TACACS;
- DNS;
- Сервер BOOTP/DHCP;
- Клиент BOOTP/DHCP;
- TFTP;
- Служба имен NetBIOS;
- Служба дейтаграмм NetBIOS.

В конкретном случае протокола DHCP клиент рассылает широковещательные пакеты обнаружения сервера в своем локальном сегменте. На рис. 11.19 показан формат сообщения DHCP. Шлюз получает этот пакет, и, если сконфигурирован вспомогательный адрес (`helper address`), пересылает этот пакет DHCP на указанный адрес.

Перед отправкой пакета маршрутизатор заполняет его поле `GIADDR` IP-адресом маршрутизатора для данного сегмента. Этот адрес будет адресом шлюза для клиента DHCP при получении IP-адреса, как показано на рис. 11.20.

Сервер DHCP получает пакет обнаружения и использует поле `GIADDR` для индексирования в списке пулов адресов; он ищет пул, в котором есть адрес шлюза, равный значению поля `GIADDR`. Этот пул позднее используется для выделения клиенту его IP-адреса. На рис. 11.21 показан широковещательный пакет клиента DHCP, на рис. 11.22 — одноадресатный ответ сервера.

Код ОП	Тип оборудования	Длина	ПЕРЕХОДЫ
Идентификатор транзакции (XID)			
Секунды		Флаги	
IP-адрес клиента (CIADDR)			
IP-адрес пользователя (YADDR)			
IP-адрес сервера (SIADDR)			
IP-адрес шлюза (GIADDR)			
Аппаратный адрес клиента (CHADDR) — 16 байтов			
Имя сервера (SNAME)—64 байта			
Имя файла —128 байтов			
Опции протокола DHCP			

Рис. 11.19. Формат сообщения протокола DHCP

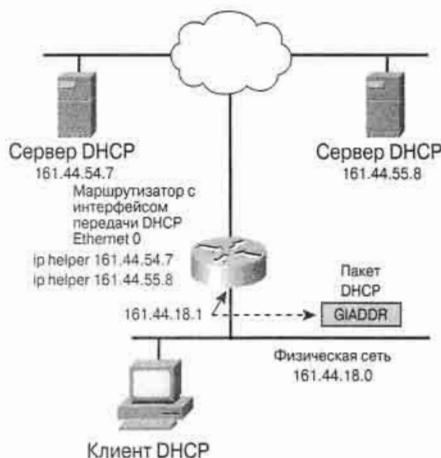


Рис. 11.20. Клиент DHCP получает IP-адрес

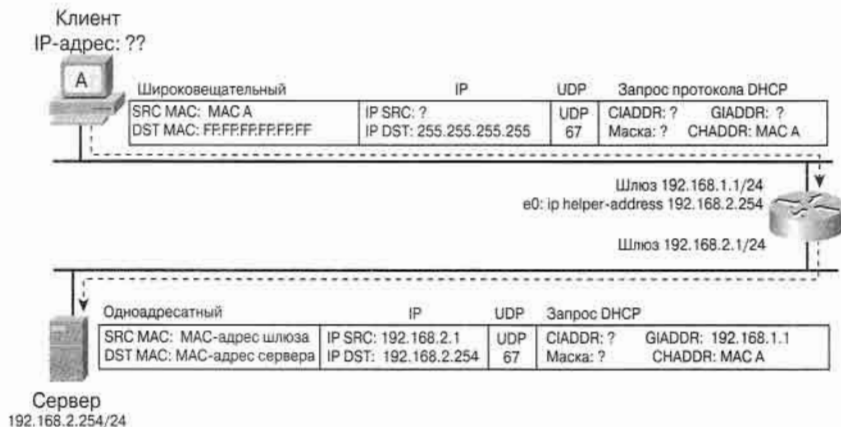


Рис. 11.21. Широковещательное сообщение клиента DHCP

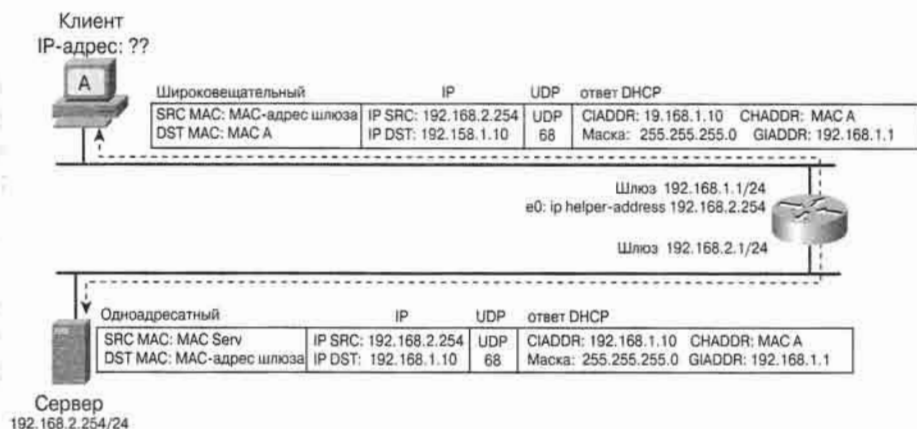


Рис. 11.22. Одноадресатное сообщение сервера DHCP

**Лабораторная работа: конфигурирование DHCP**

В этой работе требуется сконфигурировать на маршрутизаторе сервер DHCP, который будет динамически выделять адреса подсоединенным узлам.

**Лабораторная работа: конфигурирование передачи DHCP**

В этой работе требуется сконфигурировать на маршрутизаторе сервер DHCP, а затем добавить возможность рабочим станциям удаленно получать адреса DHCP и динамически назначать их подсоединенным узлам.

Резюме

В этой главе были рассмотрены следующие вопросы.

- По мере того, как растет Internet, столь же стремительно растет и количество IP-маршрутов в таблицах маршрутизации магистральных каналов Internet. Это создает проблему масштабируемости для алгоритмов маршрутизации. Для решения этой проблемы были предложены три решения.
- RFC 1918 задает почву для выделения IP-адресов для частных объединенных IP-сетей. Здесь же приводятся рекомендации по реализации для компаний, которые хотят реализовать IP, но которым не требуется полного соединения к Internet.
- Адресация NAT позволяет выполнять трансляцию частных адресов в открытые общедоступные адреса, которые можно использовать в Internet. Приведены примеры конфигурирования и тестирования NAT.
- Адресация PAT создавать группу внутренних узлов для связи с внешними узлами и совместно использовать перегруженные адреса в конфигурации NAT.
- Протокол DHCP является механизмом динамического выделения IP-адресов; при этом адреса могут повторно использоваться, когда у узлов в них пропадает необходимость. Приведены примеры конфигурирования и поиска ошибок.

В дополнение к материалу, изложенному в настоящей главе, рекомендуется ознакомиться с лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

Бесклассовая междоменная маршрутизация (Classless Interdomain Routing — CIDR). Позволяет маршрутизаторам группировать маршруты для уменьшения объема информации маршрутизации, передаваемой базовыми маршрутизаторами. При использовании CIDR несколько IP-сетей предстают для внешних (по отношению к данной группе) сетей как одно целое.

Внешний глобальный адрес (Outside Global Address). IP-адрес внешнего узла в том виде, в каком он известен узлам внутренней сети.

Внешний локальный адрес (Outside Local Address). IP-адрес, назначаемый владельцем хоста узлу во внешней сети

Внутренний глобальный адрес (Inside Global Address). В конфигурации NAT — IP-адрес, в который транслируется внутренний локальный адрес.

Внутренний локальный адрес (Inside Local Address). В конфигурации NAT — транслируемый IP-адрес.

Перегрузка адреса (overloading). Использует номера портов протокола TCP для обеспечения связи внутренних узлов со внешними и совместного использования перегруженного адреса в NAT-конфигурации.

Протокол динамического конфигурирования узла (Dynamic Host Configuration Protocol — DHCP). Обеспечивает динамическое выделение IP-адресов, при котором адреса могут использовать повторно, если у данного узла исчезла потребность в данном адресе.

Протокол начальной загрузки (Bootstrap Protocol — BOOTP). Первоначально описан в RFC 951 в 1985 году. Протокол BOOTP является предшественником DHCP; эти протоколы имеют ряд общих операционных характеристик. Оба протокола используют порты 67 и 68 UDP, которые широко известны как “BOOTP-порты”, поскольку BOOTP появился ранее DHCP.

Трансляция сетевых адресов (Network Address Translation — NAT). Трансляция частных адресов в общедоступные адреса для использования в открытой сети Internet. Эффективное средство скрыть реальную адресацию устройств в частной сети.

Контрольные вопросы

1. Кем назначаются частные адреса?
 - A. Сетевым администратором согласно RFC 1918.
 - B. ARIN.
 - C. RIPE.
 - D. Частным адресом может быть любой адрес.
2. Какой из приведенных ниже адресов является действительным частным адресом согласно RFC 1918?
 - A. 10.0.0.0/7
 - B. 10.0.0.0/8
 - C. 192.168.0.0/16
 - D. 172.16.0.0/12
3. Компания BOX поддерживает свой собственный открытый Web-сервер и намеревается реализовать адресацию NAT. Какой тип NAT следует использовать для этого Web-сервера?

- A. Динамическую
 - B. Статическую
 - C. PAT
 - D. Вообще не использовать
4. Какое из приведенных ниже приложений поддерживает Cisco IOS NAT?
- A. ICMP
 - B. Зональные передачи DNS
 - C. BOOTP
 - D. FTP (включая команды PORT и PASV)
5. Какие из приведенных ниже типов данных адресация NAT Cisco IOS не поддерживает?
- A. ICMP
 - B. Зональные переходы DNS
 - C. BOOTP
 - D. FTP (включая команды PORT и PASV)
6. BOOTP поддерживает _____ в то время как DHCP поддерживает _____
- A. Статическое отображение
 - B. Динамическое отображение
 - C. PAT
 - D. NAT
7. Расположите приведенные ниже сообщения протокола DHCP в том порядке, в каком они появляются в процессе.
- A. DHCPACK
 - B. DHCPREQUEST
 - C. DHCPOFFER
 - D. DHCPDISCOVER
8. Как расшифровывается аббревиатура DHCP?
- A. Dynamic Host Configuration Protocol
 - B. Dynamic Hosting Configuration Protocol
 - C. Dynamic Host Computer Protocol
 - D. Dynamic Host Computer Port
9. Справедливо ли утверждение: адресация NAT сохраняет зарегистрированную схему адресации за счет путем приватизации сетей intranet.
- A. Справедливо
 - B. Ошибочно
10. Справедливо ли утверждение: протокол DHCP не предназначен для конфигурирования маршрутизаторов, коммутаторов и серверов, поскольку узлы должны иметь статические IP-адреса.
- A. Справедливо
 - B. Ошибочно



В этой главе...

- Описаны различия между сетями LAN и WAN
- Рассмотрены устройства, используемые в сетях WAN
- Перечислены стандарты WAN
- Описана инкапсуляция в WAN-сетях
- Классифицированы различные каналные опции WAN
- Проанализированы различия между WAN-технологиями коммутации пакетов и коммутации каналов
- Описаны этапы проектирования распределенных сетей WAN

Технологии распределенных сетей WAN

По мере того как размеры предприятия увеличиваются и его подразделения приходится располагать в разных местах, возникает необходимость в соединении между собой локальных сетей этих подразделений и создания распределенной сети (wide-area network — WAN) предприятия. В настоящей главе рассматриваются некоторые способы такого соединения, требуемое аппаратное обеспечение и используемая при обсуждении этих вопросов терминология.

Рекомендуется выполнить лабораторные работы, ознакомиться с видеоклипами и фотографиями, которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Обзор технологий распределенных сетей WAN

Под распределенной сетью WAN понимается коммуникационная сеть, которая функционирует на территории, географически превышающей сферу работы локальной сети (local-area network — LAN). Основное отличие распределенной сети от локальной состоит в том, что для использования распределенной сети коммерческая компания или организация должна заключить договор с внешним провайдером службы распределенных сетей для того, чтобы воспользоваться его услугами. Для получения доступа к полосе пропускания на обширной территории сеть WAN обычно использует каналы связи, предоставляемые операторами служб WAN. Как правило, сеть WAN соединяет между собой филиалы одной или нескольких организаций, предоставляет доступ к внешним службам (таким как базы данных) и обеспечивает доступ удаленным пользователям. По сетям WAN передаются данные различных типов, такие как голосовые, обычные цифровые или видео. Чаще всего эти сети предоставляют телефонные службы и передачу обычных данных.

Устройства, расположенные на территории пользователя (рис. 12.1), называются, соответственно, *устройствами пользователя* (*Customer Premises Equipment — CPE*) и могут принадлежать самому пользователю или арендоваться у провайдера службы. Для связи устройств CPE с ближайшим пунктом расположения устройств провайдера службы, называемым *центральной офисом* (*Central Office — CO*), используются медные или оптоволоконные кабели. Эти кабели часто называют локальным ответвлением или “последней милей”. Передача данных происходит либо между этими

локальными ответвлениями или, выходя за пределы локальной области, по магистральному каналу к первичному центру и далее к региональному или международному центру. На рис. 12.2 показана структура сети провайдера службы WAN.

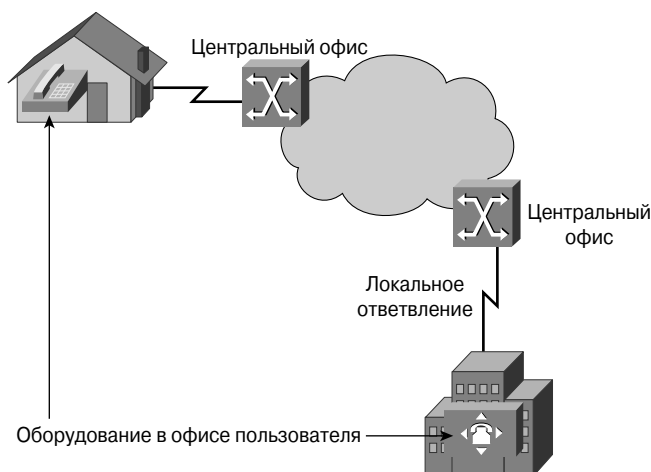


Рис. 12.1. Устройства CPE

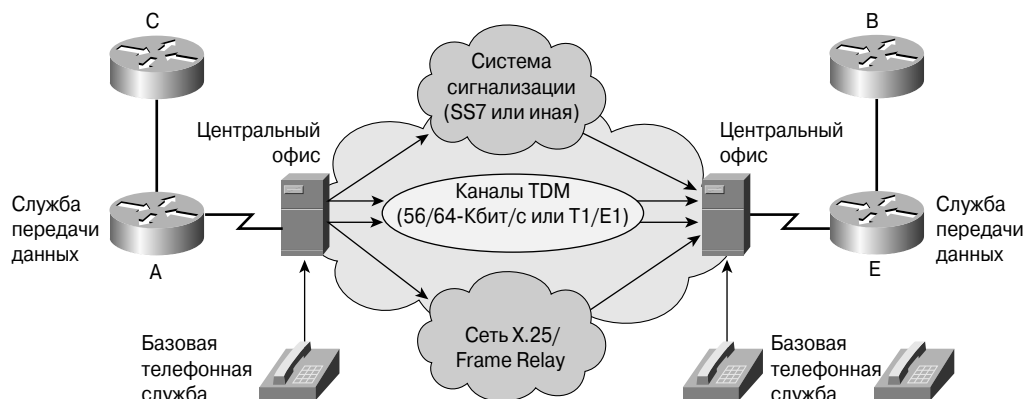


Рис. 12.2. Структура сети провайдера службы WAN

Если локальное ответвление предназначено для передачи данных, то возникает необходимость в устройстве, таком как модем, для их передачи по физической среде. Устройства, передающие данные в локальное ответвление называются *терминальным оборудованием канала передачи данных* (*data circuit-terminating equipment, data communications equipment — DCE*). Устройства пользователя, передающие данные устройствам DCE, называются *терминальным оборудованием* (*data terminal equipment — DTE*). На рис. 12.3 приведены примеры устройств DCE и DTE. Первичное назначение устройств DCE состоит в обеспечении интерфейса между DTE и каналом связи в среде WAN. Интерфейс DTE/DCE протоколов X.25/Frame Relay использует различные протоколы физического уровня (такие как высокоскоростной последовательный интерфейс [High-Speed Serial Interface — HSSI] или V.35), генерирующих кодированные сигналы, с помощью которых устройства обмениваются данными, как показано на рис. 12.4.

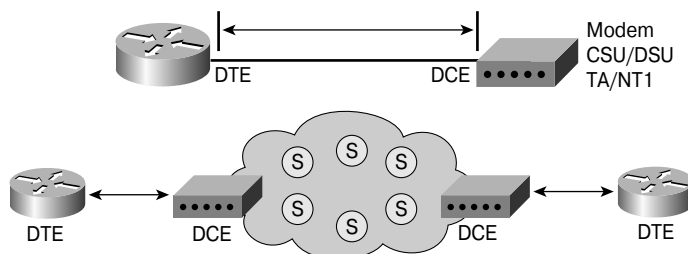


Рис. 12.3. Интерфейс DTE/DCE

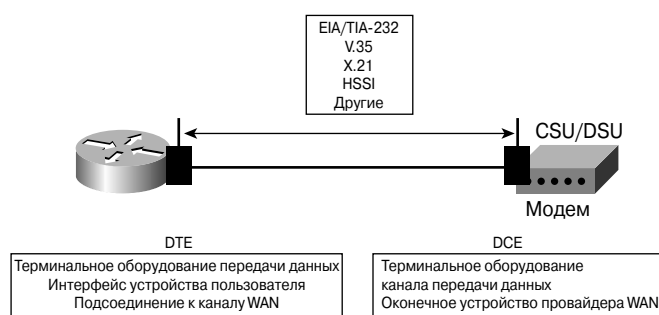


Рис. 12.4. Физический уровень сетей WAN

Каналы WAN, предоставляемые провайдером службы WAN, могут иметь различную скорость, выражаемую в битах в секунду (бит/с), в килобитах в секунду (Кбит/с, 1000 бит/с), мегабитах в секунду (Мбит/с, 1000 Кбит/с) и гигабитах в секунду (Гбит/с, 1000 Мбит/с). Значения, выраженные в битах в секунду, обычно подразумевают дуплексный режим передачи, поэтому по линии E1 реальная скорость передачи составляет до 2 Мбит/с, а по линии T1 — до 1,5 Мбит/с в каждом направлении одновременно. Отметим что 1 Кбит/с равен 1000 бит/с, в то время как один килобайт (kB, kilobyte) равен 1024 байтам. Скорости передачи данных измеряются с использованием десятичного значения К, в то время как для хранения данных используется бинарное (в виде степени числа 2) значение К. Технически Кбит/с следовало бы записывать со строчной буквы для указания на десятичный характер записи, однако практически все записывают его с прописной буквы. В табл. 12.1 приведены основные типы каналов связи распределенных сетей WAN и их полоса пропускания.

Таблица 12.1. Типы каналов сетей WAN и ширина полосы пропускания

Тип линии	Стандарт сигнала	Скорость передачи
56	DS0	56 Кбит/с
64	DS0	64 Кбит/с
T1	DS1	1,544 Мбит/с
E1	ZM	2,048 Мбит/с
J1	Y1	2,048 Мбит/с

Окончание табл. 12.1

Тип линии	Стандарт сигнала	Скорость передачи
E3	M3	34,064 Мбит/с
T3	DS3	44,736 Мбит/с
OC-1	SONET	51,840 Мбит/с
OC-3	SONET	155,520 Мбит/с
OC-9	SONET	466,560 Мбит/с
OC-12	SONET	622,08 Мбит/с
OC-18	SONET	933,12 Мбит/с
OC-24	SONET	1244,16 Мбит/с
OC-36	SONET	1866,24 Мбит/с
OC-48	SONET	2488,32 Мбит/с
OC-96	SONET	4976,640 Мбит/с
OC-192	SONET	9953,280 Мбит/с

Устройства сетей WAN

По существу, сети WAN представляют собой группы сетей LAN, соединенные между собой каналами связи, предоставляемыми провайдерами служб. Поскольку эти каналы связи не могут быть непосредственно подсоединены к сетям LAN, возникает необходимость в различных типах устройств, реализующих этот интерфейс.

Компьютеры локальных сетей, которым требуется передать данные, направляют их на маршрутизатор, который имеет как LAN-интерфейсы, так и WAN-интерфейсы, как показано на рис. 12.5. Для передачи данных на соответствующий WAN-интерфейс маршрутизатор использует адресную информацию. Маршрутизаторы являются активными интеллектуальными устройствами и, следовательно, могут принимать участие в управлении работой сети. Они осуществляют это путем динамического контроля ресурсов и поддержки выполнения сетью своих задач, таких как поддержка связи, обеспечение надежности передачи данных, контроля управления и гибкости при изменении условий работы.

Для передачи по коммуникационным каналам сигналы должны быть соответствующим образом отформатированы. Цифровым каналам требуются такие устройства, как *модуль обслуживания канала (Channel Service Unit — CSU)* и *модуль обработки данных (Data [or digital] Service Unit — DSU)*. На практике они часто объединяются в одном элементе оборудования (модуль CSU/DSU), как показано на рис. 12.6. Иногда модуль CSU/DSU устанавливается на интерфейсной плате маршрутизатора.

Если локальное ответвление является аналоговым, а не цифровым, то требуется модем, (рис. 12.7). Он позволяет передавать цифровые данные по голосовой телефонной линии путем модуляции и демодуляции сигнала. При этом для передачи по линии цифровые сигналы накладываются на аналоговый голосовой сигнал (модулированный), который можно услышать через внутренний динамик модема. Он прослушивается как серия шипящих и свистящих звуков.

На принимающем конце аналоговый сигнал возвращается в цифровую форму. Этот процесс называется демодуляцией.

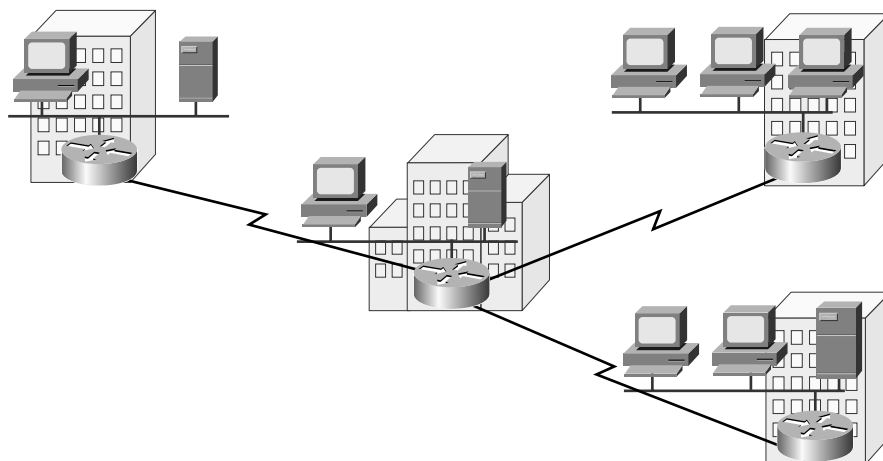


Рис. 12.5. Сети WAN и LAN, соединенные между собой посредством маршрутизаторов

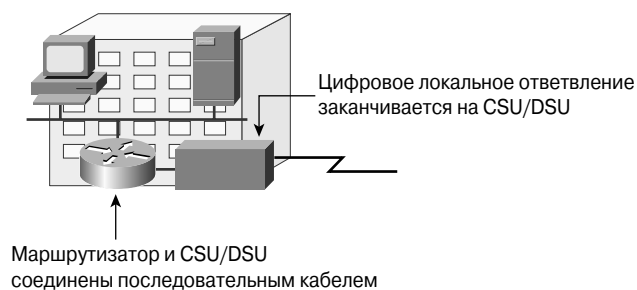


Рис. 12.6. Модуль CSU/DSU сети WAN

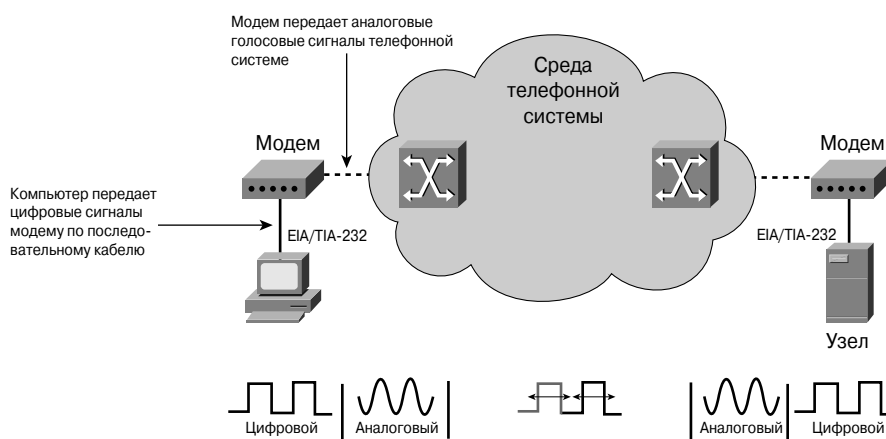


Рис. 12.7. Сети WAN и модемы

При использовании в качестве канала связи цифровой сети интегрированных служб (Integrated Services Digital Network — ISDN) все оборудование, подсоединенное к шине ISDN, должно быть ISDN-совместимым. Как правило, эта совмести-

мость обеспечивается интерфейсом внутри компьютера для соединений непосредственного доступа и в маршрутизаторе для соединений сетей LAN с сетями WAN. В оборудовании ранних поколений не всегда есть интерфейс ISDN; в этом случае может быть использован терминальный адаптер ISDN (terminal adapter — TA).

Коммуникационные серверы, концентрирующие передачу данных удаленных пользователей, используются для обеспечения удаленного доступа к сетям LAN. Они могут иметь различные комбинации аналоговых и цифровых (ISDN) интерфейсов и одновременно передают данные десятков и сотен пользователей.

Стандарты сетей WAN

При описании WAN-сетей, как и для локальных сетей, используется эталонная модель OSI, однако для них основными являются нижние два уровня. Стандарты сетей WAN обычно описывают методы доставки на физическом уровне и требования канального уровня, включая адресацию, управление потоком и инкапсуляцию. Стандарты сетей WAN определяются и контролируются рядом авторитетных организаций.

Протоколы физического уровня описывают электрические, механические операционные и функциональные характеристики соединений со службами, предоставляемыми провайдерами служб связи. Устройства, которые будут подсоединяться к сети WAN, обычно маршрутизаторы, рассматриваются как устройства DTE, а устройства на другом конце соединения, обеспечивающие интерфейс с провайдером службы, рассматриваются как оборудование DCE. В табл. 12.2 приведены некоторые общие стандарты физического уровня, а на рис. 21.8 изображены их разъемы.

Таблица 12.2. Стандарты физического уровня сетей WAN

Стандарт	Описание
EIA*/TIA* 232	Предназначен для передачи сигналов со скоростями до 64 Кбит/с через 25-контактный D-разъем на короткие расстояния. Ранее назывался RS-232. Спецификация ITU-T v.24 практически идентична этому стандарту
EIA/TIA 449 EIA-530	Более скоростная (до 2 Мбит/с) версия EIA/TIA 232, использует 36-контактный D-разъем и позволяет использовать более длинные отрезки кабеля. Используется в нескольких версиях. Также известна как RS-422 и RS-423
EIA/TIA 612/613	Высокоскоростной последовательный интерфейс (High Speed Serial Interface — HSSI), предоставляющий доступ к службам со скоростями до 52 Мбит/с через 50-контактный D-разъем
V.35	Стандарт ITU* для высокоскоростного синхронного обмена данными. В США V.35 является стандартом интерфейса, используемым для большинства маршрутизаторов и устройств DSU, подсоединенных к линиям T1
X.21	Стандарт ITU-T* для синхронных цифровых коммуникаций. Использует 15-контактный D-разъем. Этот тип разъема используется главным образом в Европе и в Японии

*EIA = Electronic Industries Association

*TIA = Telecommunications Industry Association

*ITU = International Telecommunication Union

*ITU-T = International Telecommunication Union Telecommunication Standardization Sector

Протоколы канального уровня определяют, способы инкапсуляции данных для передачи их на удаленные узлы и механизмы передачи созданных фреймов. Для этого используется ряд технологий, таких как ISDN, Frame Relay и режим асинхронной передачи (Asynchronous Transfer Mode — ATM), однако все они используют практически один и тот же базовый механизм создания фреймов — высокоуровневый протокол управления канального уровня (High-Level Data Link Control — HDLC), являющийся стандартом ISO, либо один из его вариантов или подмножеств, как показано на рис. 12.9.

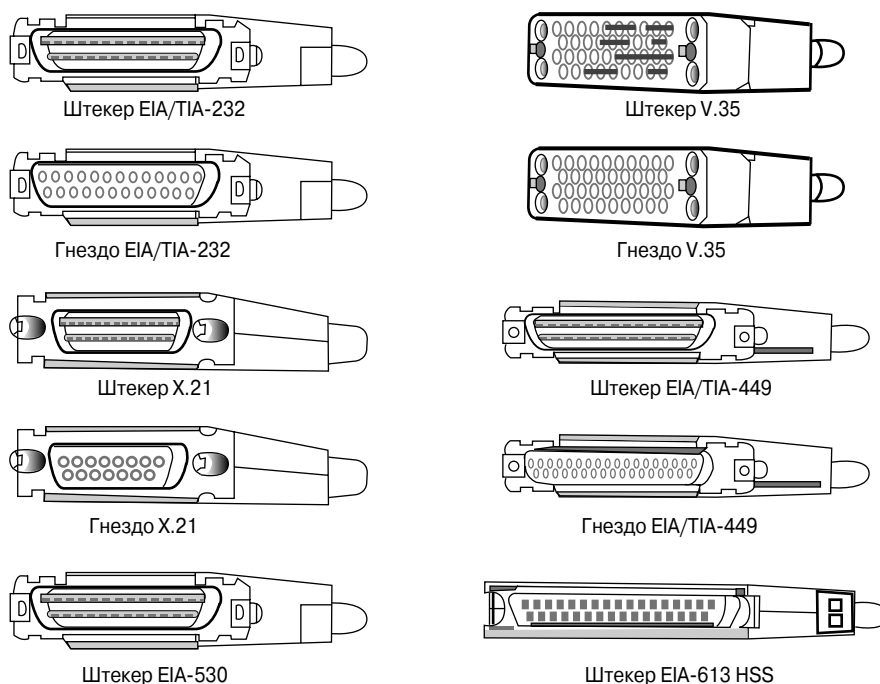


Рис. 12.8. Разъемы WAN-сетей

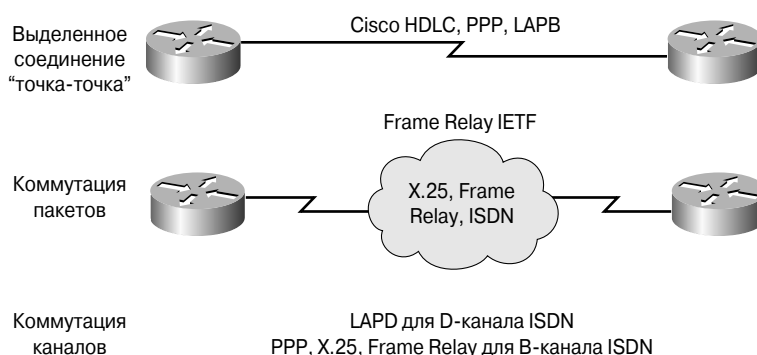


Рис. 12.9. Протоколы канального уровня распределенных сетей

Инкапсуляция в распределенных сетях

Данные сетевого уровня передаются на канальный уровень для последующей передачи по нему обычно через соединения типа “точка-точка”. Фрейм канального уровня образуется путем добавления к данным заголовка и трейлера, используемых в дальнейшем для управления и выполнения необходимых проверок. Все типы WAN-соединений используют какой-либо протокол 2-го уровня для инкапсуляции данных при передаче их по каналу WAN-сети. Для корректного использования протокола на каждом последовательном интерфейсе маршрутизатора должен быть сконфигурирован тип используемой инкапсуляции. Выбор протокола инкапсуляции определяется используемой WAN-технологией и коммуникационным оборудованием. Как правило, механизм создания фреймов базируется на стандарте HDLC.

При разработке механизма создания фреймов HDLC ставилась цель обеспечить надежную доставку данных по ненадежным линиям, поэтому он включает в себя средства сигнализации для управления потоком и контроля ошибок. Каждый фрейм начинается и заканчивается 8-битовым полем флага, двоичное значение которого равно 01111110 или 7E в шестнадцатеричной записи. Поскольку существует вероятность того, что такое значение встретится в самих передаваемых данных, отправляющая HDLC-система вставляет нулевой бит после каждого пяти единиц в поле данных, поэтому на практике значение флага может встретиться только в конце фрейма. Принимающая система удаляет вставленные биты. Если фрейм передается непосредственно за предшествующим, то конечный флаг первого фрейма используется как начальный флаг следующего.

Необходимость в адресном поле в каналах WAN отсутствует, поскольку они практически всегда они являются соединениями “точка-точка”, однако оно все же присутствует и может иметь длину 1 или 2 байта. В управляющем поле указывается тип фрейма, который может быть информационным, контрольным или нумерованным. В нумерованных фреймах передаются сообщения установки канала, в информационных фреймах — данные сетевого уровня, а контрольные фреймы используются для управления потоком информационных фреймов и при необходимости, в случае ошибки, запрашивают повторную передачу данных. Управляющее поле обычно имеет длину один байт, однако в системах с расширенным скользящим окном его длина равна двум байтам. Вместе адресное и контрольное поля называются заголовком фрейма.

За управляющим полем находятся инкапсулированные данные, а затем контрольная последовательность фрейма (frame check sequence — FCS), использующая механизм контроля циклической избыточности и образующая поле длиной 2 или 4 байта. Используются несколько протоколов канального уровня, включая подмножества протокола HDLC и его фирменные версии (рис. 12.10). Обе версии HDLC — для протоколов PPP и Cisco, имеют дополнительное поле в заголовке, которое используется для указания протокола сетевого уровня для инкапсулированных данных.

PPP						
Флаг	Адрес	Управление	Протокол	Данные	FCS	Флаг

HDLC						
Флаг	Адрес	Управление	Proprietary	Данные	FCS	Флаг

Рис. 12.10. Форматы фреймов в сетях WAN

Варианты соединений WAN-сетей

В последующих разделах обсуждаются различные технологии, используемые главным образом для WAN-соединений. Целесообразно сделать сначала общий обзор и классификацию этих технологий.

Соединения с коммутацией каналов

Коммутация каналов (circuit switching) может быть использована при установке соединения для передачи голосовых или обычных данных между двумя географически удаленными пунктами. Перед началом передачи полезных данных необходимо создать соединение путем установки коммутаторов. Это осуществляется телефонной службой путем набора номера в обычных голосовых линиях или в цифровых каналах ISDN.

Для сокращения задержки, связанной с этапом установки соединения, операторы телефонных служб также предлагают постоянные каналы в своих системах. Такие выделенные или арендованные линии обеспечивают большую полосу пропускания, чем коммутируемые соединения. Примерами соединений с коммутацией каналов могут служить:

- общедоступная коммутируемая телефонная сеть (Public Switched Telephone Network — PSTN);
- интерфейс базовой скорости ISDN (Basic Rate Interface — BRI);
- интерфейс первичной скорости ISDN (Primary Rate Interface — PRI).

Соединения с коммутацией пакетов

Многим пользователям WAN-сетей не удастся добиться эффективного использования полосы пропускания, предоставляемой выделенным каналом, постоянным или коммутируемым, вследствие того, что их потоки данных имеют взрывообразный характер. Для более рационального обслуживания таких пользователей провайдеры служб предоставляют технологии, в которых данные передаются в помеченных ячейках, фреймах или пакетах по сетям с коммутацией пакетов. Поскольку внутренние каналы между коммутаторами используются многими пользователями, стоимость связи в сети с *коммутацией пакетов (packet switching)* ниже чем в сети с коммутацией каналов. Всем пользователям требуется один и тот же канал, а пакеты должны быть полностью приняты, прежде чем перейдут в другой, поэтому задержка (delay, latency) и вариация задержки (также называемая дребезжанием [variability of delay, jitter]) в сетях с коммутацией пакетов больше чем в сетях с коммутацией каналов. Несмотря на задержку и дребезжание, присущие совместно используемым сетям, современные технологии обеспечивают удовлетворительную передачу по таким сетям голосовых данных и даже видео.

Для осуществления отдельного сквозного соединения в сети с коммутацией пакетов необходимо создать маршрут через коммутаторы. Если маршруты создаются сразу после включения коммутаторов, то они называются *постоянными виртуальными каналами (Permanent Virtual Circuits — PVC)*; если маршруты создаются по требованию, то они называются *коммутируемыми виртуальными каналами (Switched Virtual Circuit — SVC)*. Сеть, в которой маршрут не устанавливается заранее, а создается каждым коммутатором для каждого отдельного пакета, называется сетью без ориентации на соединение (connectionless).

Для подсоединения к сети, в которой используется коммутация пакетов, пользователю необходимо создать локальное ответвление к ближайшему месту, в котором доступна служба провайдера, называемому точкой присутствия службы (point of presence — POP). Обычно это арендуемая выделенная линия. Она значительно короче той, которая бы потребовалась для непосредственного подсоединения к месту расположения пользователя; часто по ней проходят несколько виртуальных каналов (virtual circuit — VC). Поскольку маловероятно, что сразу всем каналам VC одновременно потребуется максимум полосы пропускания, пропускная способность выделенной линии может быть меньше, чем сумма пропускных способностей отдельных каналов VC. Примерами технологий, использующих соединения с коммутацией пакетов или ячеек являются:

- Frame Relay;
- X.25;
- ATM.

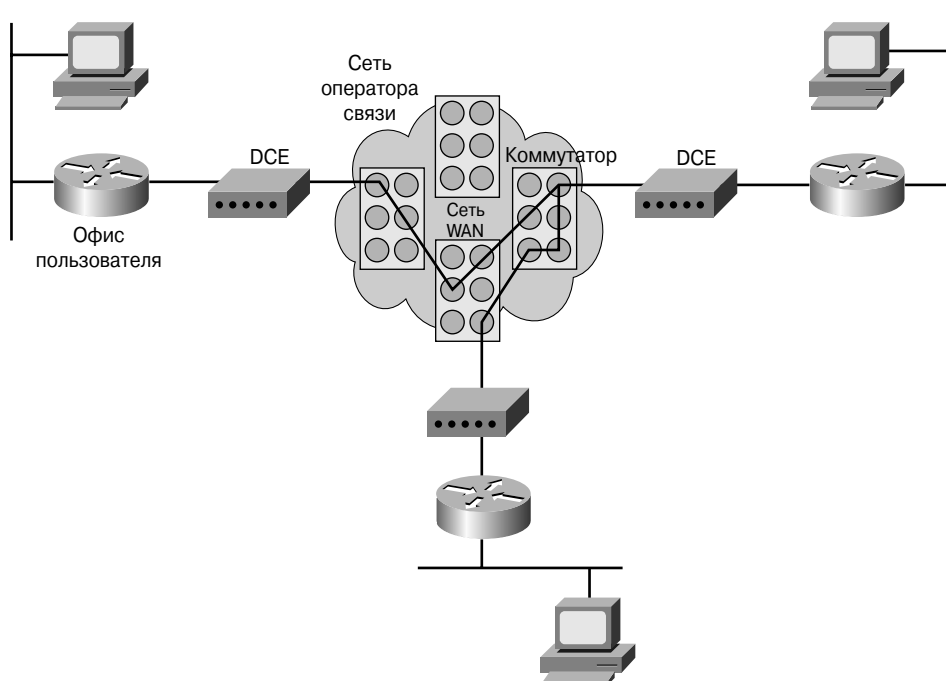
Коммутация пакетов и каналов

Сети с коммутацией пакетов были разработаны для того, чтобы избежать значительных расходов, связанных с эксплуатацией общедоступных сетей, использующих коммутацию каналов, и предоставления более экономичной WAN-технологии.

Когда абонент делает телефонный звонок, набранный номер используется для установки коммутаторов в промежуточных пунктах по всей длине маршрута таким образом, чтобы образовался непрерывный канал от телефонной трубки вызывающей стороны до телефонного аппарата вызываемой стороны. Поскольку для создания канала используется операция коммутации, такая телефонная система называется сетью с коммутацией каналов. Если в такой системе заменить телефонные трубки модемами, подсоединенными к компьютерам, то по такому скоммутированному каналу можно передавать компьютерные данные. На рис. 12.11 приведен пример сети с коммутацией каналов.

На практике канал может включать в себя участки, передающая среда которых отличается от медного провода, например, оптоволоконный кабель или микроволновая связь. На внутренних участках маршрута между отдельными промежуточными точками могут передаваться данные и других пользователей, поэтому для предоставления им всем по очереди возможности использовать соединение используется *мультиплексирование с разделением времени (Time-Division Multiplexing — TDM)*. Использование TDM гарантирует, что каждому пользователю будет предоставлена определенная часть полосы пропускания соединения.

Если канал используется для передачи компьютерных данных, то использование таких фиксированных частей полосы пропускания может оказаться неэффективным. Например, если канал используется для доступа к Internet, то при передаче Web-страницы происходит всплеск активности, после которого наступает период бездействия канала пока пользователь читает страницу, а затем новый всплеск при получении новой. Такие колебания интенсивности между нулевой и максимальной типичны для потоков данных в компьютерных сетях. Поскольку пользователь имеет исключительное право на использование такой фиксированной полосы пропускания, коммутируемые каналы являются дорогостоящим способом передачи данных.

*Рис. 12.11. Коммутация каналов*

Альтернативой такому подходу является выделение полосы пропускания только в том случае, когда это необходимо и совместное использование полосы пропускания многими пользователями. В соединении с коммутацией каналов биты данных, переданные в канал, автоматически передаются на дальний конец канала, поскольку канал уже установлен. При совместном использовании канала несколькими пользователями необходим какой-либо механизм, помечающий биты для того, чтобы система знала, в какой пункт их требуется доставить. Поскольку пометить индивидуальные биты затруднительно, они объединяются в группы, которые в разных ситуациях называются ячейками, фреймами или пакетами. Созданные помеченные порции данных, называемые пакетами, передаются между промежуточными пунктами сети провайдера с последующей доставкой конечному получателю. Сети, реализующие такой подход, называются сетями с коммутацией пакетов. На рис. 12.12 приведен пример сети с коммутацией пакетов.

Поскольку каналы, соединяющие промежуточные пункты или коммутаторы в сети провайдера выделяются отдельному пользователю только в том случае, если у него есть данные для передачи, становится возможным использование каналов многими пользователями, а стоимость канала для каждого пользователя может оказаться значительно ниже, чем в случае выделенного соединения с коммутацией каналов. С другой стороны, вследствие того, что отдельному пакету, возможно, придется ожидать передачи на коммутаторе до тех пор, пока пакет другого пользователя не покинет канал, задержка передачи данных в сетях с коммутацией пакетов оказывается непредсказуемой.

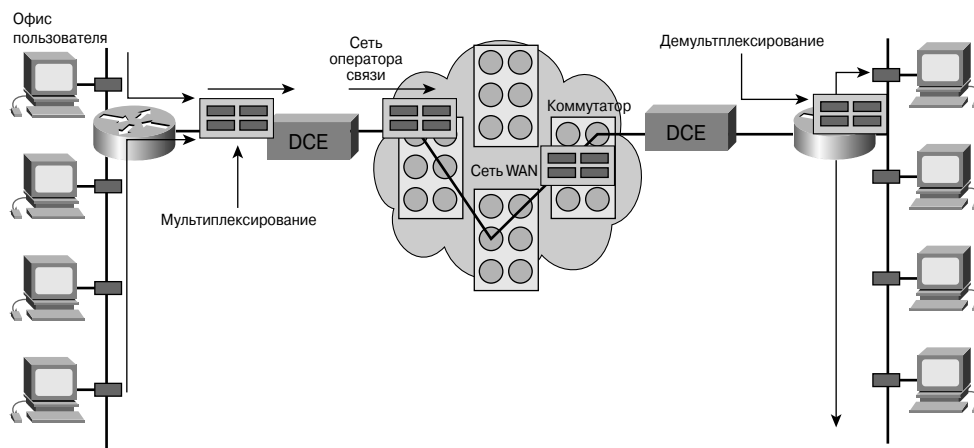


Рис. 12.12. Сеть, использующая коммутацию пакетов

Коммутаторы в сетях с коммутацией пакетов должны быть способны определить по адресной информации каждого пакета следующий канал, в который следует отправить этот пакет. Для определения этого канала могут быть использованы два подхода: без ориентации на соединение (*connectionless*) и ориентированный на установку соединения. В системах без ориентации на соединение таких, например, как Internet, вся адресная информация содержится в каждом пакете. В системах, ориентированных на соединение, маршрут каждого пакета предопределен и каждому пакету требуется только идентификатор. В технологии Frame Relay такой идентификатор называется идентификатором канального уровня (*data-link connection identifier — DLCI*). Коммутатор определяет маршрут в восходящем направлении просматривая таблицу идентификаторов, находящуюся в его оперативной памяти. Совокупность позиций во всех таких таблицах определяет конкретный маршрут или канал в системе; если такой “канал” физически существует только во время прохождения по нему пакета, то он называется виртуальным каналом (*virtual circuit — VC*).

Позиции таблиц, образующие виртуальный канал VC, могут быть заполнены путем рассылки по сети запросов на соединение; в этом случае получаемый канал называется коммутируемым виртуальным каналом (*switched virtual circuit — SVC*). Данные, которые должны пройти по каналу SVC, должны ожидать заполнения соответствующих позиций таблиц, однако после установки канал SVC может функционировать в течение нескольких часов, дней или даже недель. В том случае, когда канал должен быть доступен постоянно, создаются постоянные виртуальные каналы (*permanent virtual circuit — PVC*). Для таких каналов позиции таблиц заполняются во время загрузки коммутаторов, поэтому каналы PVC всегда доступны.

Технологии WAN-сетей

В последующих разделах обсуждаются некоторые из многочисленных существующих WAN-технологий, используемых для создания соединений распределенных сетей, таких как аналоговые соединения удаленного доступа, ISDN, выделенные линии, X.25, Frame Relay, ATM, DSL и кабельные соединения. В этом разделе также обсуждаются преимущества и недостатки этих технологий и некоторые типовые ситуации в которых они используются.

Аналоговые соединения удаленного доступа

В тех случаях, когда по сети передаются небольшие объемы данных и потоки данных имеют пульсирующий характер, использование модемов и аналоговых телефонных линий позволяет осуществлять коммутируемые выделенные соединения с небольшой пропускной способностью (рис. 12.13).

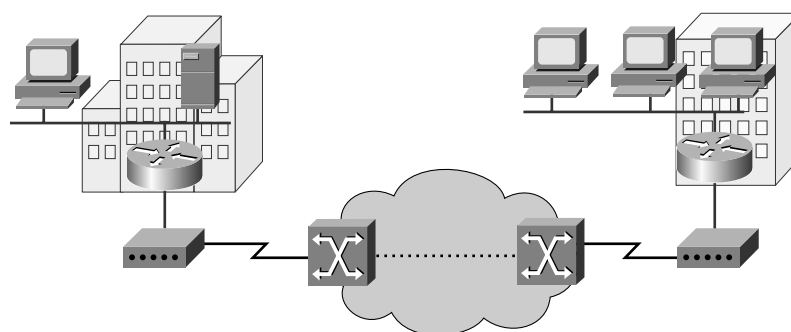


Рис. 12.13. Сети WAN, использующие модемы

В традиционной телефонии телефонный аппарат пользователя соединен с сетью PSTN медным кабелем, называемым локальным ответвлением. Во время телефонного разговора сигнал в локальном ответвлении представляет собой электрическую копию голоса абонента и является непрерывно изменяющимся сигналом.

Локальное ответвление не позволяет непосредственно передавать двоичные компьютерные данные, однако при использовании модема компьютерные данные могут быть переданы по голосовой телефонной сети. Модем модулирует бинарные данные на аналоговых сигналах и, наоборот, демодулирует аналоговые сигналы в бинарные данные.

Скорость такого преобразования ограничена физическими характеристиками локального ответвления и его подсоединения к PSTN и не может превышать верхнего предела, равного примерно 33 Кбит/с. Эта скорость может быть повышена до примерно 56 Кбит/с при условии, что сигнал поступает из цифрового источника.

На небольших предприятиях эта скорость может оказаться удовлетворительной для таких операций, как обмен коммерческой информацией (данные продаж, прайс-листы, стандартные отчеты) и для электронной почты. Для передачи больших файлов или резервирования данных пользователь может воспользоваться преимуществами низкой стоимости такой связи в нерабочее время и в выходные дни. Тарифы такой связи зависят от расстояния между конечными точками, времени суток и продолжительности вызова.

Преимуществами использования модема и аналоговой линии являются простота и небольшая стоимость реализации. Недостатками являются невысокая скорость передачи и относительно большое время, затрачиваемое на установку соединения. Часто в ситуациях, когда используются модемы, довольно длительное время установки соединения не вызывает проблем. Постоянная выделенная линия не вызывает задержки и дребезжания для данных, передаваемых по каналу “точка-точка”, однако голосовые и видеоданные не могут адекватно передаваться при таких низких скоростях.

Технология ISDN

За прошедшее время передача по соединениям или магистралям сети PSTN аналоговых мультиплексированных сигналов с разделением частот уступила место передаче мультиплексированных цифровых сигналов с разделением времени (time-division multiplexed — TDM). Очевидным следующим шагом является перевод локального ответвления на передачу цифровых сигналов, что обеспечивает коммутируемые соединения с большей полосой пропускания.

Служба цифровой сети интегрированных служб (Integrated Services Digital Network — ISDN) превращает локальное ответвление в цифровое соединение TDM. Это соединение имеет каналы носителя с полосой пропускания 64 Кбит/с (В-каналы) для передачи голоса и данных и сигнальный канал (дельта-канал или D-канал) для установки вызова и других целей.

Интерфейс базовой скорости ISDN (Basic Rate Interface — BRI), предназначенный для домашних офисов и малых предприятий, обеспечивает два В-канала и один D-канал с полосой пропускания 16 Кбит/с. Для более крупных предприятий предназначен интерфейс первичной скорости передачи (Primary Rate Interface — PRI) ISDN. Интерфейс PRI предоставляет в Северной Америке 23 В-канала и один D-канал, что обеспечивает суммарную пропускную способность до 1,544 Мбит/с (эта величина включает в себя некоторый объем служебной нагрузки для синхронизации). В Европе, Австралии и других частях света PRI предоставляет 30 В-каналов и один D-канал, которые обеспечивают суммарную пропускную способность до 2,048 Мбит/с (включая некоторый объем служебной нагрузки для синхронизации). D-канал с пропускной способностью 64 Кбит/с показан на рис. 12.14. Отметим, что скорость передачи интерфейса PRI в Северной Америке соответствует скорости передачи по линии T1. Скорость международного интерфейса PRI соответствует скорости передачи по линии E1.

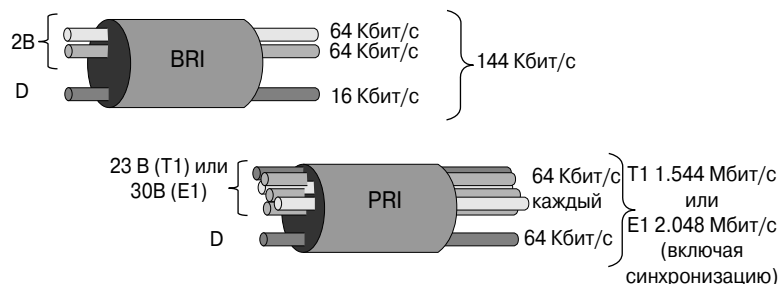


Рис. 12.14. Каналы ISDN

D-канал интерфейса BRI загружен явно недостаточно, поскольку ему требуется управлять лишь двумя В-каналами. Поэтому некоторые провайдеры используют его для передачи данных с небольшими битовыми скоростями, таких, например, как данные соединений X.25 со скоростью 9,6 Кбит/с.

Для небольших WAN-сетей BRI ISDN обеспечивает идеальный механизм связи. Интерфейс BRI имеет небольшое время установки вызова (менее одной секунды), а его В-канал 64 Кбит/с обеспечивает большую пропускную способность, чем аналоговый модемный канал. На рис. 12.15 показана WAN-сеть, в которой используется технология ISDN. Если требуется большая пропускная способность, то возможна активизация второго В-канала, что обеспечивает пропускную способность 128 Кбит/с. Хотя и недоста-

точное для передачи видео, такое повышение позволяет поддерживать в дополнение к передаче данных нескольких телефонных разговоров.

Другим возможным применением технологии ISDN является ее использование при необходимости в качестве дополнительного источника полосы пропускания для уже имеющегося соединения по выделенной линии. Выделенная линия проектируется для основных потоков нагрузки, а ISDN добавляется при пиковых нагрузках. ISDN может быть также использована в качестве резервной линии в случае непредвиденных сбоев в выделенной линии.

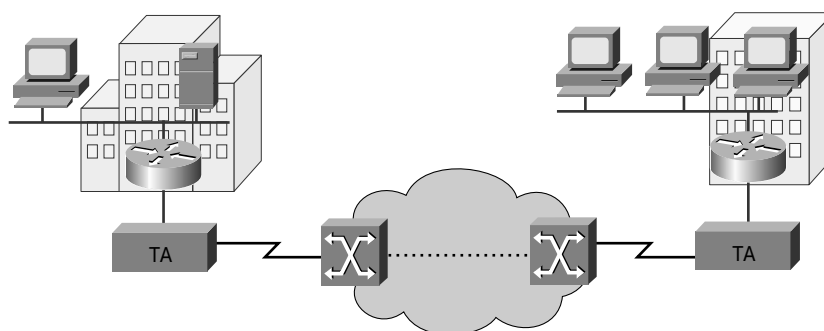


Рис. 12.15. WAN-сеть, использующая технологию ISDN

Тарифы службы ISDN на каждый В-канал аналогичны тарифам голосовых соединений, т.е. два одновременных соединения 64 Кбит/с стоят вдвое больше, чем одно.

При использовании интерфейса PRI ISDN две конечные точки могут быть соединены несколькими В-каналами, что позволяет обеспечить видеоконференцию или несколько широкополосных соединений для передачи данных без задержки или дребезжания. На больших расстояниях использование нескольких соединений может стать весьма дорогостоящим.

Выделенные линии

В тех случаях, когда требуются постоянные выделенные соединения, используются арендуемые линии с пропускной способностью до 2,5 Гбит/с.

Каналы “точка-точка” обеспечивают заранее установленные каналы связи сетей WAN от офиса пользователя к удаленной сети через несущую сеть, такую, например, как сеть телефонной компании. Каналы “точка-точка” обычно арендуются у оператора связи и поэтому часто называются арендованными линиями. Операторы связи предлагают выделенные линии с различными возможными значениями пропускной способности.

Стоимость выделенной линии обычно определяется требуемой полосой пропускания и расстоянием между соединяемыми точками. Каналы “точка-точка” обычно стоят дороже, чем службы совместного использования, такие как Frame Relay. Стоимость решений, использующих выделенные линии, значительно возрастает, если эти линии соединяют большое количество сетевых узлов. Пропускная способность выделенных линий обеспечивает отсутствие задержки и дребезжания. Для некоторых приложений, таких как электронная торговля, существенна постоянная доступность таких соединений.

Для каждого соединения выделенной линии требуется последовательный порт маршрутизатора. Требуются также модули CSU/DSU и канал от провайдера службы. Выделенные линии часто используются для построения WAN-сетей, как показано на рис. 12.16, поскольку обеспечивают постоянную выделенную полосу пропускания. Такие линии традиционно пользуются большим спросом, однако они имеют и ряд недостатков. Объем передачи данных по сети WAN часто изменяется, поэтому полоса пропускания канала редко соответствует конкретным потребностям пользователей. Кроме того, каждой конечной точке требуется отдельный интерфейс маршрутизатора, поэтому маршрутизатор в центральной точке звездообразной топологии оказывается весьма дорогостоящим. Любые изменения параметров выделенной линии, как правило, требуют посещения узла оператором для изменения пропускной способности.

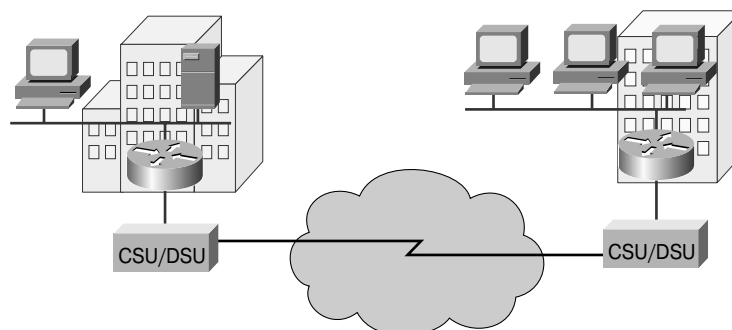


Рис. 12.16. WAN-сети с выделенными линиями

Выделенные линии могут использоваться для создания непосредственных соединений типа “точка-точка” между сетями LAN предприятия. Они также используются для подсоединения отдельных филиалов к сети с коммутацией пакетов. В таком канале могут быть мультиплексированы несколько соединений, что уменьшает длину линии и требования к количеству интерфейсов центральных маршрутизаторов в топологии сети.

Технология X.25

В противовес дорогостоящим выделенным линиям провайдеры служб телекоммуникаций разрабатывают сети с коммутацией пакетов, в которых совместное использование каналов уменьшает затраты пользователей. Первой из таких сетей с коммутацией пакетов была группа протоколов, стандартизованная как X.25. Служба протокола X.25 обеспечивает низкоскоростное совместно используемое соединение с переменной пропускной способностью, которое может быть постоянным или коммутируемым. На рис. 12.17 показана WAN-сеть протокола X.25.

Пользователи службы получают сетевой адрес. В такой сети могут быть созданы виртуальные каналы, по которым получателям передаются пакеты запроса на установку соединения. Созданный канал SVC идентифицируется своим номером. Пакеты данных, отмеченные этим номером, доставляются по соответствующему адресу. В одном соединении могут быть активными несколько каналов.

Абоненты службы подсоединяются к сети X.25 по выделенным линиям или по соединениям удаленного доступа. В сетях X.25 также могут присутствовать предварительно установленные соединения между пользователями, которые представляют собой постоянные каналы PVC.

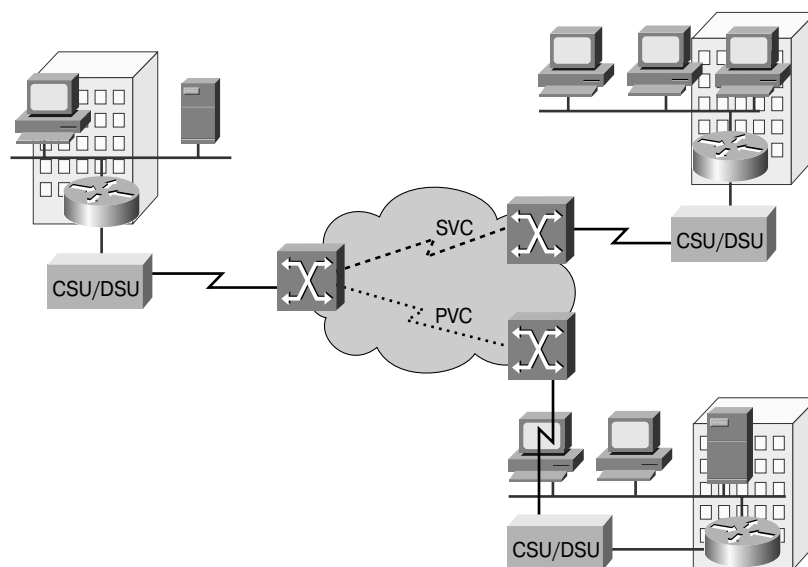


Рис. 12.17. WAN-сеть протокола X.25

Сети X.25 могут оказаться очень эффективными в отношении стоимости, поскольку тарифы в них основаны на объеме переданных данных, а не на расстоянии или времени соединения. Доставка данных может происходить с любой скоростью вплоть до максимальной для данного соединения. Это качество сети обеспечивает определенный уровень гибкости при ее использовании. Сети X.25 обычно имеют невысокую пропускную способность, с максимальным значением равным 48 Кбит/с. Кроме того, передача пакетов данных часто сопровождается задержками, характерными для совместно используемых сетей.

Технология Frame Relay

В связи с увеличением спроса на широкополосную коммутацию пакетов с низкой задержкой провайдеры связи стали использовать технологию Frame Relay (Frame Relay — FR). Хотя общая структура такой сети похожа на сеть X.25, допустимые скорости передачи в ней достигают значений до 4 Мбит/с, а некоторые провайдеры предлагают и большие скорости (рис. 12.18).

Сети Frame Relay отличаются от сетей X.25 в нескольких аспектах. Наиболее важным отличием является то, что Frame Relay использует значительно более простой протокол на канальном уровне. Для обозначения модуля данных на канальном уровне используется термин *фрейм (frame)*.

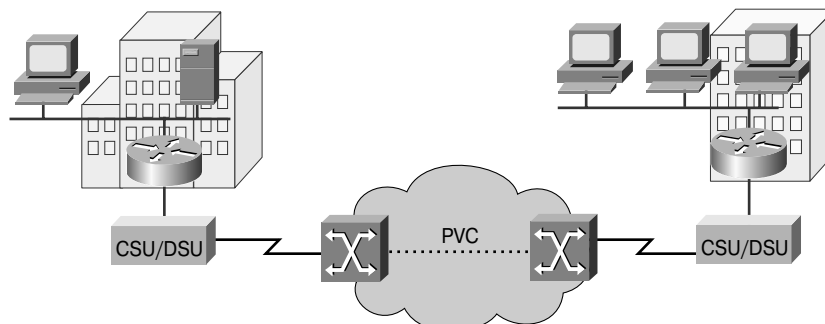


Рис. 12.18. WAN-сети протокола Frame Relay

Протокол Frame Relay не осуществляет контроля ошибок и управления потоками. Благодаря упрощенной обработке фреймов достигается малая задержка. Меры, принимаемые для предотвращения скопления фреймов на промежуточных коммутаторах, помогают уменьшить уровень дребезжания.

Большинство соединений Frame Relay используют постоянные каналы PVC, а не коммутируемые каналы SVC. Соединение с границей сети часто осуществляется по выделенной линии. Для установки канала SVC в одном или более В-каналов используется D-канал ISDN. Тарифы Frame Relay основываются на пропускной способности порта на границе сети и оговоренной в контракте полосе пропускания или согласованной скорости передачи информации (committed information rate — CIR) различных каналов PVC, проходящих через этот порт.

Frame Relay обеспечивает постоянные, совместно используемые соединения со средней шириной полосы пропускания по которым передаются как обычные, так и голосовые данные. Технология Frame Relay является идеальным вариантом для соединения между собой LAN-сетей предприятия. Маршрутизатору LAN-сети требуется только один интерфейс, даже если используются несколько каналов VC, а короткая линия доступа или локальное ответвление к границе сети Frame Relay обеспечивает эффективные с точки зрения финансовых затрат соединения между разделенными большими расстояниями LAN-сетями.

Технология ATM

Параллельно с развитием технологии Frame Relay провайдеры служб связи осознали необходимость в технологии постоянного совместного использования с очень малой задержкой, низким уровнем дребезжания и полосой пропускания, значительно большей, чем была доступна ранее. Таким решением стала технология асинхронного режима передачи (Asynchronous Transfer Mode — ATM). В сетях ATM достигаются скорости передачи до 155 Мбит/с. Как видно из рис. 12.19, структура сети ATM аналогична структурам других сетей совместного доступа, таких как X.25 и Frame Relay, однако технология ATM обеспечивает соединения с очень высокими скоростями передачи данных. Эта технология особенно эффективна при передаче данных, для которых крайне нежелательна задержка, таких как видео.

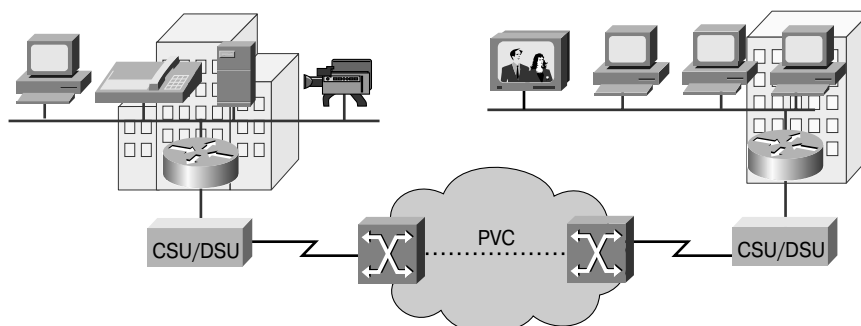


Рис. 12.19. WAN-сеть, в которой используется технология ATM

Режим асинхронной передачи (*Asynchronous Transfer Mode — ATM*) представляет собой технологию, позволяющую передавать голос, видео и обычные данные по открытым (общедоступным) и частным сетям. Основой архитектуры ATM являются не фреймы, а ячейки. Эти ячейки ATM имеют фиксированную длину 53 байта. Такая ячейка включает в себя 5-байтовый ATM-заголовок, за которым следуют 48 байтов полезной нагрузки. Используемые в ATM небольшие ячейки фиксированной длины 53 байта хорошо подходят для передачи голосовых и видеоданных, поскольку для таких данных недопустима задержка. Они не могут ожидать окончания передачи большого пакета данных.

53-байтовая ячейка ATM, в которой на 48 байтов полезной нагрузки приходится 5 байтов служебных данных, менее эффективна, чем имеющие больший размер фреймы и пакеты технологий Frame Relay и X.25. Если в ячейках передаются разбитые на части пакеты сетевого уровня, то уровень служебной нагрузки возрастает, поскольку коммутатор ATM должен быть способен собрать первоначальные пакеты в пункте назначения. Для передачи одного и того же объема данных сетевого уровня типичной линии ATM требуется на 20% большая полоса пропускания, чем каналу Frame Relay.

В технологии ATM используются как каналы PVC, так и каналы SVC, хотя в WAN-сетях чаще используются постоянные каналы PVC. Как и в других технологиях совместного доступа, ATM позволяет реализовать несколько виртуальных каналов в одном соединении по выделенной линии с границей сети.

Технология DSL

Телефонная система налагает ограничения на полосу пропускания локального ответвления. Отделение локального ответвления от телефонной системы позволяет обеспечить значительно большую полосу пропускания без прокладки нового кабеля. На рис. 12.20 показано DSL-соединение.



Рис. 12.20. DSL-соединение

Технология цифрового абонентского канала (Digital Subscriber Line — DSL) позволяет отделить локальное ответвление от коммутатора телефонной станции или аппаратуры локального оператора связи (local exchange). Вместо этого соединение DSL подсоединяет локальное ответвление данного абонента, вместе с локальными ответвлениями других абонентов данной зоны к мультиплексору доступа абонентского цифрового канала (Digital Subscriber Line Access Multiplexor — DSLAM), также расположенному на телефонной станции. Для поддержки обычной телефонной службы мультиплексор DSLAM подсоединяется к коммутатору телефонной станции. Он также обычно подсоединяется, обычно посредством соединения ATM, к Internet-службе провайдера DSL.

Канал DSL поддерживает постоянное соединение. Как только пользователь включает компьютер, подсоединенный к модему DSL, сразу же осуществляется DSL-соединение. При таком подходе не тратится время на набор номера и на установку соединения. Двумя основными типами технологий DSL являются асимметричная (asymmetric — ADSL) и симметричная (symmetric — SDSL). Все формы службы DSL попадают в одну из этих двух категорий; в каждой из них имеется несколько разновидностей. Для обобщенного обозначения всех различных форм службы DSL иногда используется аббревиатура xDSL. Асимметричная служба предоставляет большую полосу пропускания или загрузки в нисходящем направлении (к пользователю), чем в восходящем. Симметричная служба предоставляет одинаковую скорость в обоих направлениях.

Различные разновидности службы DSL предоставляют различную полосу пропускания; при этом у большинства из них полоса пропускания больше, чем у выделенных линий T1 и E1. Достижимая при этом скорость передачи в значительной степени зависит от реальной длины локального ответвления, а также от типа и состояния кабеля. Для удовлетворительного качества службы длина локального ответвления не должна превышать 5,5 км (3,5 мили). Доступность DSL пока далека от универсальной и, вследствие обилия различных типов, уже существующих и разрабатываемых стандартов, служба DSL пока мало распространена в качестве средства связи компьютерных отделов предприятий с домашними работниками. Кроме того, абонент не может непосредственно подсоединиться к сети предприятия; для этого он должен сначала подсоединиться к Internet-провайдеру, а затем создать IP-соединение через сеть Internet с предприятием. Такой способ связи связан с определенным и угрозами безопасности информации.

Кабельные модемы

В городской среде для распространения телевизионных сигналов широко используется коаксиальный кабель. Сеть кабельного телевидения также может быть использована для доступа к сети, предоставляя значительно большую полосу пропускания, чем обычное локальное ответвление телефонной службы. На рис. 12.21 показаны кабельные модемные соединения.

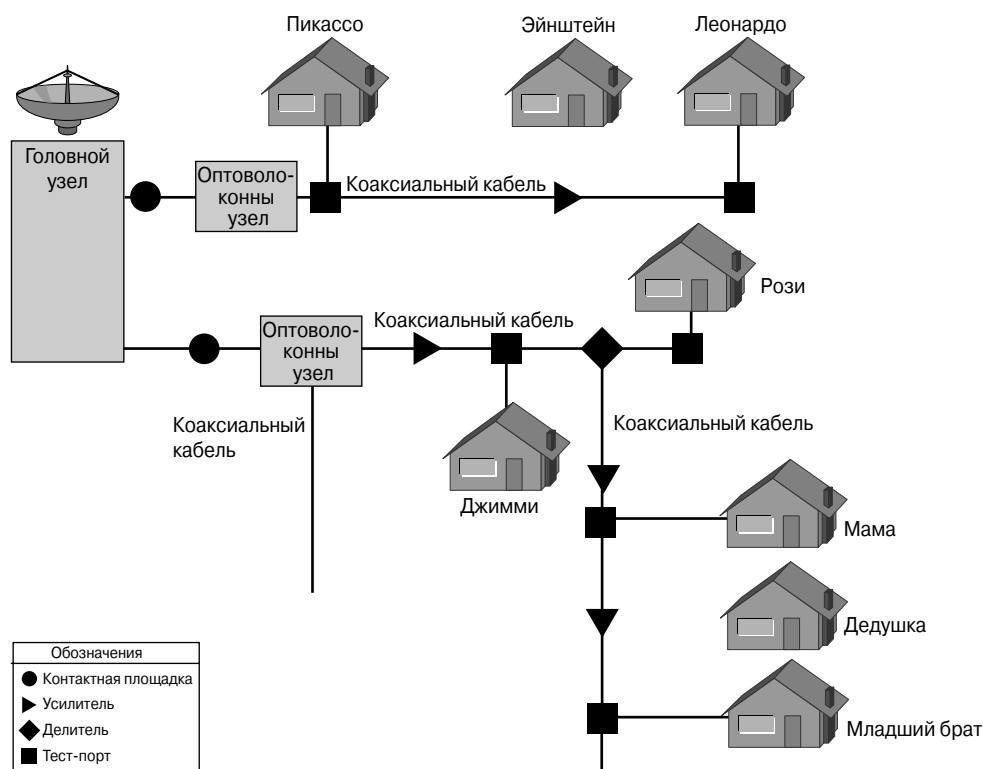


Рис. 12.21. Использование кабельных модемов

Кабельные модемы позволяют осуществлять двустороннюю передачу данных в обоих направлениях, используя те же коаксиальные линии, по которым передается кабельное телевидение. Некоторые провайдеры кабельных служб обещают скорости передачи в 6,5 раз превосходящие скорости выделенных линий T1. Такая скорость делает кабель привлекательной средой для быстрой передачи больших объемов цифровой информации, включая видеоклипы, аудиофайлы и большие объемы обычных цифровых данных. Объем информации, передача которой потребовала бы 2 минут для загрузки с использованием BRI ISDN, при использовании соединения кабельного модема может быть загружен за 2 секунды. Таким образом, кабельные модемы обеспечивают скорости, большие, чем у выделенных линий, с меньшими затратами и более простой установкой. Кабельные модемы обеспечивают круглосуточное соединение. Сразу после включения питания компьютера пользователь оказывается подключенным к сети Internet. Такая установка позволяет экономить время и усилия на набор номера для установки соединения. Однако постоянная включенность (“always-on”) кабельного соединения означает, что подсоединенный компьютер оказывается постоянно уязвимым в отношении атак хакеров и должен быть надежно защищен с помощью брандмауэра.

Кабельный модем способен обеспечить доставку данных со скоростью 30–40 Мбит/с по одному кабельному каналу 6 МГц. Это в 500 раз быстрее, чем модем 56 Кбит/с.

При использовании кабельного модема абонент может продолжать прием кабельного телевидения одновременно с получением данных на персональном компьютере. Это осуществляется с помощью простого делителя “один-к-двум”, как показано на рис. 12.22.

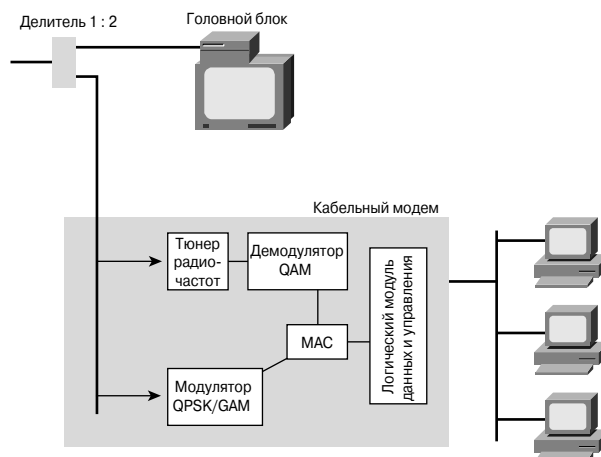


Рис. 12.22. Кабельный модем: двусторонний делитель

Как и в случае использования DSL, у абонента нет другого выбора, кроме как воспользоваться услугами Internet-провайдера (Internet service provider — ISP), предоставляющего службу кабельного модема и подсоединяться к сети своего предприятия с помощью приложения TCP/IP, такого как Telnet. Другим недостатком является то, что все локальные абоненты совместно используют полосу пропускания кабеля, так же, как это происходит в случае коаксиальных соединений Ethernet. По мере того, как к службе подключается все большее количество пользователей, реальная полоса пропускания может оказаться значительно меньшей, чем ожидаемая. Еще более серьезной проблемой является обеспечение необходимого уровня безопасности.

Домашний компьютер пользователя оказывается уязвимым не только для всех пользователей сети Internet, но и для пользователей, подключенных к его собственному кабелю. Поэтому необходим определенный уровень защиты с помощью какого-либо типа брандмауэра.

Для решения проблем безопасности провайдеры модемных кабельных служб предоставляют возможность использования соединений виртуальных частных сетей (Virtual Private Network — VPN) для соединения с сервером VPN, который обычно расположен на корпоративном узле предприятия.

Осуществление связи в распределенных сетях

В настоящее время сетевым администраторам приходится управлять сложными WAN-сетями и обеспечивать работу все большего числа программных приложений, использующих протокол IP (Internet Protocol — IP) и Web. Эти сети предъявляют высокие требования к сетевым ресурсам и требуют высокопроизводительных сетевых технологий. WAN-сети представляют собой сетевые среды, включающие в себя различные среды передачи, разнообразные протоколы и соединения с другими се-

тиями, такими как глобальная сеть Internet. Рост и управляемость таких сетей часто достигается весьма сложным взаимодействием различных протоколов и функций.

Несмотря на повышение производительности используемого оборудования и улучшение свойств передающей среды проектирование WAN-сетей становится все более сложным. Тщательное проектирование сети WAN позволяет уменьшить количество проблем, связанных с ростом сети. Для создания надежной, легко масштабируемой сети WAN сетевой проектировщик должен помнить о том, что каждая WAN-сеть предъявляет свои особые требования к проектированию. В последующих разделах приведен обзор методов, используемых при проектировании WAN-сетей и обеспечения в них надежной связи.

WAN-сети рассматриваются как множество каналов передачи данных, соединяющих маршрутизаторы локальных сетей LAN. Конечные станции пользователей и серверы LAN-сетей осуществляют обмен данными. Маршрутизаторы, при необходимости, передают данные между сетями LAN по каналам связи. Связь по каналам WAN-сетей осуществляется между географически удаленными друг от друга областями. При необходимости осуществить связь локальной станции с удаленной станцией (т.е. с конечной станцией, расположенной в удаленном месте) информация пересылается по одному или более каналам WAN-сетей.

В сети WAN маршрутизаторы играют роль соединительных точек сети. Эти маршрутизаторы определяют оптимальный путь по сети для передаваемого потока данных.

Как правило, финансовые и юридические вопросы, связанные с обслуживанием каналов, образующих сеть WAN, решаются провайдером службы или оператором связи, а требуемые пользователю службы предоставляются предприятию с соответствующей оплатой.

Двумя основными технологиями служб WAN-сетей являются коммутация каналов и коммутация пакетов. Каждая из этих технологий имеет свои достоинства и недостатки. Например, сети с коммутацией каналов предоставляют пользователю выделенную только ему полосу пропускания, которая не может использоваться другими пользователями.

Наоборот, коммутация пакетов является методом, при использовании которого сетевые устройства совместно используют канал типа “точка-точка” для передачи пакетов от источника к получателю по сети оператора связи. Сети с коммутацией пакетов традиционно обладают большей гибкостью и используют полосу пропускания более эффективно, чем сети с коммутацией каналов. Эти каналы, соединяющие между собой локальные сети LAN или подсоединяющие их к другим сетям, обычно имеют значительно меньшую скорость передачи данных (полосу пропускания), чем 100 Мбит/с — значение, типичное для сетей LAN. Оплата канала является основной составляющей стоимости WAN; в процессе проектирования необходимо обеспечить удовлетворительную ширину полосы пропускания с приемлемой стоимостью. В условиях, когда пользователи хотели бы получать доступ к службам с высокими скоростями, а руководство компаний хотело бы удержать затраты в разумных пределах, определение оптимальной конфигурации WAN-сети является для проектировщика непростой задачей. По сетям WAN могут передаваться различные типы данных, такие как голосовые данные, обычные цифровые и видео, поэтому выбранный проект должен обеспечивать достаточную пропускную способность и приемлемое транзитное время, которые будут удовлетворять потребности предприятия. Это будет включать в себя, кроме всего прочего, выбор соответствующей топологии соединений различных узлов между собой и приемлемой пропускной способности.

Традиционные WAN-сети часто состояли из каналов передачи данных, соединяющих географически разделенные компьютеры-мейнфреймы; в современных сетях эти каналы соединяют между собой географически разделенные сети LAN. Рабочие станции конечных пользователей, серверы и маршрутизаторы находятся в этих LAN-сетях, а каналы WAN-сетей заканчиваются на маршрутизаторах. При обмене информацией между соединенными друг с другом LAN-сетями маршрутизаторы определяют оптимальный маршрут по сети для конкретных потоков данных. Маршрутизаторы могут также обеспечивать качество обслуживания (Quality Of Service — QoS) и управлять им, задавая различные приоритеты разным типам данных.

По сравнению с современными WAN-сетями новые WAN-инфраструктуры должны быть более сложными, основываться на новых технологиях и способны работать со все более возрастающим и быстро изменяющимся множеством приложений, обеспечивая требуемый и гарантируемый уровень служб. Кроме того, предполагаемое 300%-возрастание объема передачи данных в ближайшие 5 лет заставит предприятия все более контролировать и сдерживать расходы на WAN-сети.

Сетевые проектировщики используют WAN-технологии для удовлетворения этих новых требований. По соединениям WAN-сетей обычно передается важная информация и их требуется оптимизировать в отношении затрат и ширины полосы пропускания. Например, маршрутизаторы, соединяющие сети кампусов, обычно применяют оптимизацию потоков, избыточные маршруты, резервные соединения удаленного доступа для аварийных ситуаций и QoS для критически важных приложений. В табл. 12.3 приведены обобщенные характеристики WAN-технологий, удовлетворяющих различным требованиям.

Таблица 12.3. Обзор WAN-технологий

WAN-технология	Обычная сфера использования
Выделенная линия	Выделенные линии могут использоваться в сетях типа “точка-точка” (Point-to-Point Protocol — PPP), в звездообразных (hub-and-spokes) топологиях или в качестве резервных соединений для других типов каналов
Цифровая сеть интегрированных служб (Integrated Services Digital Network — ISDN)	Сеть ISDN может быть финансово эффективно использована для получения удаленного доступа к корпоративным сетям. Она поддерживает передачу голоса и видео, а также может быть резервным соединением для других типов каналов
Технология Frame Relay	Frame Relay обеспечивает финансово эффективную, высокоскоростную сеточную топологию с малой величиной задержки соединяющую между собой удаленные узлы. Такие сети могут быть частными или предоставляться операторами связи

Поскольку сеть WAN представляет собой просто набор соединений между расположенными в LAN-сетях маршрутизаторами, в ней отсутствуют какие-либо службы высших уровней и технологии WAN функционируют на трех самых нижних уровнях эталонной модели OSI: физическом, канальном и сетевом, как показано на рис. 12.23. Маршрутизаторы определяют пункт назначения пакетов по заголовку сетевого уровня и передают их на соответствующее соединение канального уровня для доставки по физическому каналу.

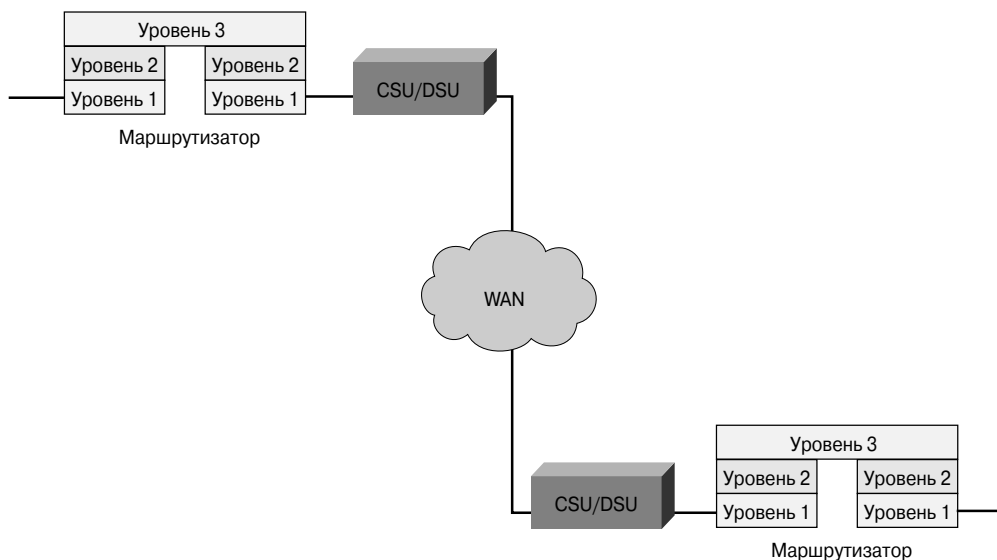


Рис. 12.23. Сети WAN функционируют на 1-м, 2-м и 3-м уровнях

Традиционно WAN-коммуникации характеризовались как имеющие низкую пропускную способность, большую задержку и высокий уровень ошибок. Одной из их характеристик была также стоимость аренды у провайдера службы передающей среды (т.е. кабеля) для соединения между собой двух кампусов. Поскольку инфраструктура WAN часто арендуется у провайдера службы, при проектировании WAN-сети необходимо добиться оптимального сочетания стоимости полосы пропускания и ее эффективности. Например, все технологии и функции, используемые в WAN-сетях, должны удовлетворять следующим требованиям:

- оптимальная полоса пропускания;
- минимальная стоимость;
- максимальная эффективность службы для конечного пользователя.

В последнее время традиционные сети совместного использования стали испытывать перегрузки из-за новых требований к сетям, которые описаны ниже.

- По мере того, как с целью повышения производительности предприятия стали использовать мультимедийные приложения в режиме “клиент-сервер”, нагрузка на сети значительно возросла.
- Скорость повышения требований приложений увеличилась и это, без сомнения, будет продолжаться (например, “подталкивающие” технологии Internet).
- Приложения во все большей степени требуют особого качества обслуживания, вследствие необходимости в службах, которые они предоставляют конечным пользователям.
- Устанавливается беспрецедентное количество соединений между разнообразными офисами, удаленными пользователями, мобильными пользователями, международными узлами, поставщиками/потребителями и соединений через сеть Internet.

- Взрывной рост корпоративных intranet- и extranet-сетей создает все большую потребность в большей полосе пропускания.
- Возрастание количества промышленных серверов позволяет решать коммерческие задачи различных компаний и организаций.

Интеграция локальных и распределенных сетей

Распределенным приложениям требуется все большая полоса пропускания, а взрывной рост использования Internet подводит многие архитектуры LAN-сетей к пределам их возможностей. Значительно возрос объем голосовых коммуникаций, при этом все для обмена вербализованной информацией больший упор делается на централизованных системах “голосовые сообщения — электронная почта”. Сеть стала критически важным инструментом для передачи информационных потоков. В настоящее время от сетей требуется меньшая стоимость и вместе с тем поддержка возникающих приложений и большего числа пользователей с повышающейся производительностью.

До настоящего времени коммуникации локальных и распределенных сетей оставались логически отделенными друг от друга. В сетях LAN полоса пропускания бесплатна, а количество соединений ограничено только аппаратным обеспечением и затратами на реализацию сети. В сетях WAN основные затраты связаны с арендой полосы пропускания, а чувствительные к задержке данные, такие как голос, остаются отделенными от обычных данных.

Internet-приложения, такие как голосовые и видео в реальном времени, требуют большей производительности сети и предсказуемого ее поведения. Эти мультимедийные приложения быстро становятся существенной частью коммерческих средств и инструментов. По мере того, как компании начинают планировать реализацию в своих сетях новые, основанные на intranet, приложения, такие как видеообучение, видеоконференции и передачу голоса по IP, нагрузка, создаваемая ими на уже существующую инфраструктуру сети становится серьезной проблемой. Если ранее компания полагалась на свою корпоративную сеть при передаче критически важных коммерческих данных и сейчас намеревается интегрировать в сеть онлайновое видеообучение, то сеть должна быть способна обеспечить гарантированное качество обслуживания QoS. Эта служба QoS должна обеспечить передачу мультимедийных данных, не позволяя им однако смешиваться с критически важными коммерческими данными. Поэтому сетевому проектировщику при решении многих проблем объединенных сетей требуется проявить большую гибкость чтобы полученное решение не требовало создания нескольких сетей или отказа от использования уже сделанных инвестиций в коммуникации.

После того, как станут понятны требования к сети, необходимо определить и выбрать конкретные возможности, соответствующие данной компьютерной среде. Информация последующих разделов поможет решить эти задачи: особенно задачи выбора типов соединений, структуры каналов между различными местами и выбора для этих каналов технологий, удовлетворяющих требованиям предприятия с приемлемыми затратами. Многие сети WAN используют звездообразную топологию, часто по историческим причинам. По мере роста предприятия и добавления новых подразделений происходило их подсоединение к центральному офису, и создание таким образом традиционной звездообразной топологии. Иногда для большей надежности или уменьшения задержки некоторые конечные точки лучей звезды соединяют друг с другом,

в результате чего создается полносвязная или частично-связная топология. Между звездообразной и полносвязной топологиями находятся много промежуточных возможных способов соединения между собой устройств сети. При проектировании новой сети WAN или в более общем случае, при анализе или модифицировании уже существующей WAN-сети должна быть выбрана новая топология, которая удовлетворяет общим принципам проектирования.

При выборе топологии требуется учесть несколько факторов. С увеличением количества каналов обычно возрастают затраты. Наличие нескольких каналов между конечными точками повышает надежность. Чем больше количество узлов или маршрутизаторов, через которые должны пройти данные, тем большее время для этого требуется, поскольку как правило, поскольку каждый пакет данных должен быть полностью получен на сетевом устройстве, перед тем как он будет отправлен следующему устройству.

В каналах передачи данных может быть использован ряд технологий с различными функциями, как показано в табл. 12.4.

Таблица 12.4. Технологии WAN-сетей

Тип канала передачи данных	Оплата услуг провайдера	Полоса пропускания	Тип соединения
Частная выделенная линия	Расстояние, пропускная способность	Не ограничена	Постоянное/Фиксированная пропускная способность
Телефонный канал	Расстояние, время	33–56 Кбит/с	Коммутируемое, низкая скорость соединения
ISDN	Расстояние, пропускная способность	64–128 Кбит/с	Коммутируемое, средняя скорость соединения
X.25	Объем передаваемых и получаемых данных	Не более 48 Кбит/с	Коммутируемое/Фиксированная пропускная способность
Frame Relay	Пропускная способность	Не более 4 Мбит/с	Постоянное/Фиксированная пропускная способность
ATM	Пропускная способность	Не более 155 Мбит/с	Постоянное/Фиксированная пропускная способность

Технологии, требующие установки соединения перед передачей данных, такие как обычная телефонная линия, ISDN или X.25, не подходят для WAN-сетей, которым требуется малое время отклика или задержки (хотя после установки соединения ISDN и телефонная линия являются соединениями с малым временем отклика и малым дребезжанием). В частности, ISDN часто применяется для соединения малого/домашнего офиса (small/home offices — SOHO) с корпоративной сетью, обеспечивающего быстрое соединение и приемлемую полосу пропускания. ISDN часто отказывается полезной в качестве резервного канала для первичных соединений и для обеспечения соединений по требованию параллельно с первичным соединением. Особенностью этих технологий является то, что они оплачиваются только в том случае, когда они реально используются. Отдельные подразделения предприятия могут быть непосредственно соединены выделенными линиями или могут быть подсоединены с помощью канала доступа к ближайшей точке присутствия (nearest point-of-presence — POP) сети совместного использования. Примерами таких сетей совместного использования являются X.25, Frame Relay ATM.

Выделенные линии обычно длиннее, и, следовательно, дороже каналов доступа, однако предоставляют практически любую ширину полосы пропускания. Они имеют малую задержку и низкий уровень дребезжания.

В сетях ATM, Frame Relay и X.25 передача данных от нескольких пользователей осуществляется по одним и тем же внутренним каналам. Предприятие не может управлять количеством каналов или переходов, по которым должны пройти данные в сети совместного использования или временем ожидания, которое потребуется его данным на каждом устройстве перед тем, как они будут переданы в следующий канал. Такая неопределенность времени задержки и уровня дребезжания делает эти технологии неприемлемыми для некоторых типов передаваемых по сети данных. Однако часто эти недостатки сети совместного использования перевешиваются меньшей стоимостью для каждого из совместно использующих сеть пользователей. Поскольку канал используется несколькими пользователями, расходы каждого из них обычно существенно меньше, чем стоимость непосредственного канала с той пропускной способностью.

Хотя сети технологии ATM и являются сетями совместного доступа, при ее создании ставилась цель достичь минимальной задержки и дребезжания путем использования высокоскоростных внутренних каналов, по которым передаются легко управляемые модули данных, называемые ячейками. Ячейки ATM имеют фиксированную длину 53 байта: 48 для данных и 5 для заголовка. Эта технология широко используется для передачи чувствительных к задержке данных. Технология Frame Relay также может быть использована для передачи чувствительных к задержке данных; при этом часто используется QoS для предоставления более высокого приоритета более чувствительным данным.

Типичная сеть WAN использует комбинацию различных технологий, которые выбираются в зависимости от типа и объема передаваемых данных. Для подсоединения отдельных подразделений в конкретной зоне используются ISDN, Frame Relay или выделенные линии. Для подсоединения зон к магистрали используются технологии Frame Relay, ATM или выделенные линии.

Идентификация и выбор модели сети

Иерархические модели позволяют проектировать сеть на различных уровнях. Для того, чтобы понять важность разбиения на уровни, рассмотрим эталонную модель OSI, уровневую модель, используемую для наглядной иллюстрации компьютерных коммуникаций. Используемые в этой модели уровни упрощают понимание задач, которые требуется решить для того чтобы два компьютера могли осуществить связь. Иерархические модели, применяемые при проектировании сетей, также используют уровни для упрощения решения задач соединения между собой различных сетей.

Каждому уровню могут быть поручены специфичные для него функции, что позволяет сетевому дизайнеру выбрать соответствующие системы и функции для каждого уровня.

Иерархическое проектирование облегчает внесение в сеть изменений. Использование модулей при проектировании сети позволяет создавать элементы проекта, которые могут быть повторены по мере роста сети. Кроме того, поскольку сетям потребуется модернизация его стоимость и сложность ограничены небольшой подсетью всей сети. В крупных, плоских или полносвязных сетях прослеживается тенденция к тому, что изменения затрагивают большое количество систем. Структурирование сети на небольшие, легко понимаемые сегменты также облегчает нахождение точек сбоя в сети. Сетевой менеджер в этом случае легко может найти в сети точки перехода и это позволяет ему впоследствии найти точки сбоя.

Иерархическая модель проектирования сети

При проектировании сети имеется тенденция использования в качестве базовой одной из двух общих стратегий: сеточной или структуры. В сеточной структуре топология сети является плоской, в том смысле, что все узлы имеют одинаковый уровень — все маршрутизаторы выполняют в основном одни и те же функции и нет строгого ответа на вопрос о том, где выполняются какие-либо конкретные функции. Расширение (масштабирование) сети как правило носит полуслучайный, произвольный характер. В иерархической структуре сеть организуется в виде совокупности уровней, каждый из которых выполняет свои конкретные функции. Ниже приводятся преимущества иерархической модели.

- **Масштабируемость.** Сеть, организованная по иерархической модели, может расширяться значительно больше, не жертвуя при этом контролем и управляемостью, поскольку отдельные функции локализованы и потенциальные проблемы легче выявляются. Примером огромной иерархически спроектированной сети является открытая телефонная сеть.
- **Простота реализации.** При иерархической организации сети каждому уровню назначаются определенные функции, что облегчает построение сети.
- **Облегчается поиск и устранение проблем.** Поскольку функции каждого уровня четко определены, упрощаются локализация и изоляция источника проблемы. Временная сегментация сети для уменьшения сферы влияния сбоя также становится более простой.
- **Предсказуемость.** Поведение сети, использующей функциональные уровни, достаточно предсказуемо, что значительно облегчает планирование и расчет пропускной способности при расширении сети; такой подход к проектированию сети также облегчает моделирование сети для аналитических целей.
- **Поддержка различных протоколов.** Совместное использование протоколов и приложений, используемых в настоящее время и будущих значительно облегчается в сетях, следующих принципам иерархической организации, поскольку их структура уже сейчас логически организована.
- **Управляемость.** Все перечисленные выше преимущества значительно повышают управляемость сети.

Трехуровневая модель проектирования

При иерархическом проектировании сеть подразделяется на следующие три уровня:

- Базовый уровень, обеспечивающий оптимальную транспортировку данных между сетевыми центрами;
- Уровень распределения, который осуществляет соединения на основе заданных политик;
- Уровень доступа, обеспечивающий доступ к сети отдельных пользователей и рабочих групп.

На рис. 12.24 показана структура верхних уровней сети при иерархическом проектировании.

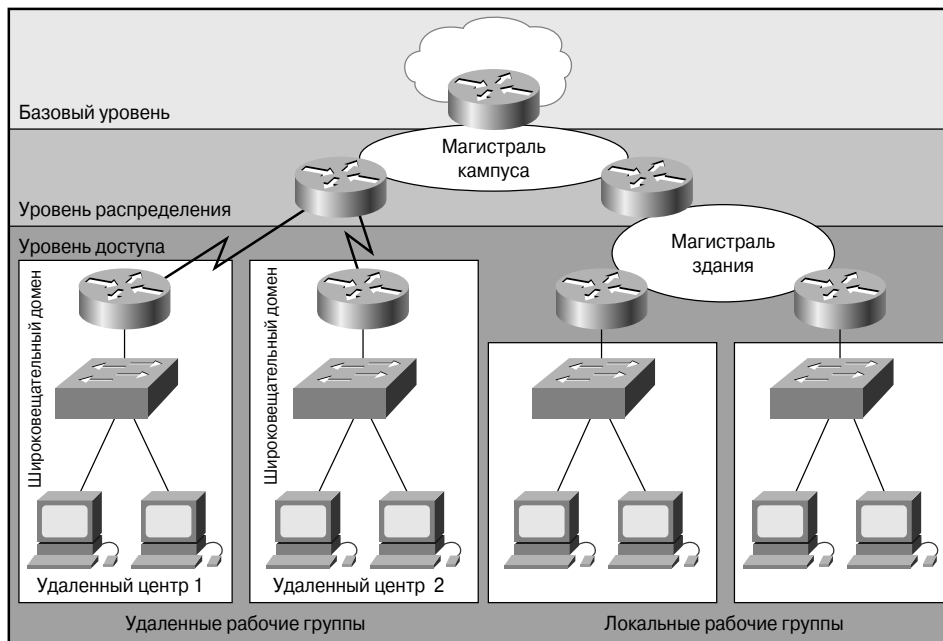


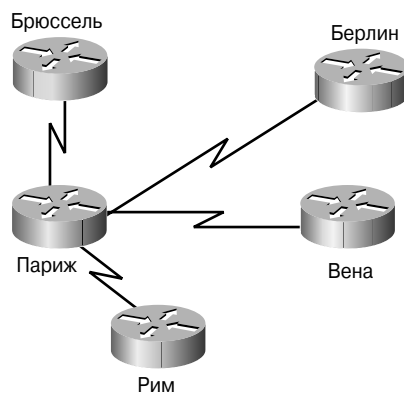
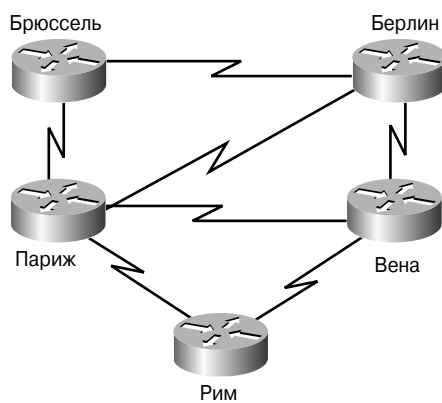
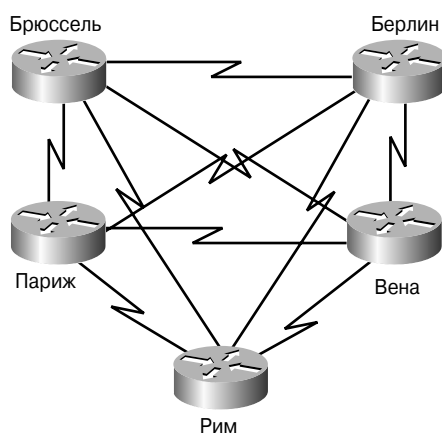
Рис. 12.24. Иерархическое проектирование сети

Предположим, что некоторое, возможно, финансовое предприятие работает во всех странах Европейского Союза и имеет филиалы в каждом городе с населением более 10000 человек. Каждый филиал имеет свою локальную сеть и руководством принято решение соединить между собой все эти локальные сети и создать, таким образом, распределенную сеть WAN. Полносвязное решение явно неприемлемо, поскольку для соединения этих 900 центров потребовалось бы полмиллиона каналов. Простую звездообразную топологию было бы очень трудно реализовать, поскольку потребовался бы маршрутизатор-концентратор с 900 интерфейсами или один интерфейс с 900 виртуальными каналами в сети с коммутацией пакетов.

Рассмотрим вместо этих вариантов иерархическую модель, в которой группа сетей LAN соединяются с образованием зоны, зоны соединяются между собой, образуя регион, а при объединении регионов образуется магистраль WAN-сети.

Зоны могут быть образованы по количеству соединяемых точек, с верхним ограничением 30-50, или следовать устоявшимся географическим границам. Зоны будут иметь звездообразную топологию, как показано на рис. 12.25; точки концентрации соединяются между собой с образованием региона, возможно, вновь со звездообразной топологией. Регионы образуются по географическому принципу, а концентраторы каждого региона могут быть соединены топологией "точка-точка", как показано на рис. 12.26 и 12.27.

Эта трехуровневая модель напоминает иерархическое построение в телефонных системах. Каналы, соединяющие сетевые центры зоны и предоставляющие им доступ к сети предприятия, называются каналами доступа или уровнем доступа сети WAN. Потоки данных между зонами распределяются по каналам распределения и, при необходимости, передаются в магистральные каналы для отправки в другие регионы.

*Рис. 12.25. Иерархическая сеть**Рис. 12.26. Сеть, соединяющая несколько зон (вариант 1)**Рис. 12.27. Сеть, соединяющая несколько зон (вариант 2)*

Такая иерархия часто оказывается полезной в тех случаях, когда структура потоков данных зеркально отражает структуру подразделений предприятия, которое само разделено на регионы, зоны и предприятия. Она также полезна в тех случаях, когда имеется какая-либо центральная служба, к которой должны иметь доступ все подразделения, однако объем передаваемых данных недостаточен для того, чтобы оправдать непосредственное подключение к этой службе каждого подразделения. В этих случаях локальная сеть в концентраторной точке зоны может содержать серверы, предоставляющие службы на уровне зоны и локальные службы. В зависимости от объема и типов передаваемых данных в качестве соединений доступа могут выступать удаленный доступ (dialup), например, соединения ISDN, выделенные линии или соединения протокола Frame Relay. Протокол Frame Relay позволяет создавать частично-связную топологию без дополнительных физических соединений. В качестве каналов распределения могут выступать Frame Relay или ATM, а для магистральных соединений обычно используются каналы ATM или выделенные линии.

Компоненты трехуровневой модели

Под уровнем понимается точка сети, в которой заканчивается граница 3-го уровня эталонной модели OSI. В трехуровневой модели имеются три уровня: магистральный, уровень распределения и уровень доступа, каждый из которых выполняет свои специфические функции.

- **Магистральный уровень.** Магистральный уровень обеспечивает высокоскоростные соединения на больших расстояниях между географически удаленными центрами, связывая между собой ряд сетей кампусов в одну корпоративную или промышленную сеть WAN. Магистральные каналы обычно являются соединениями типа “точка-точка”; в них обычно отсутствуют отдельные узлы. Магистральные службы (например, T1/T3, Frame Relay, SMDS) обычно арендуются у провайдеров телекоммуникационных служб.
- **Уровень распределения.** Уровень распределения предоставляет сетевые службы нескольким LAN-сетям в среде WAN-сети. Обычно на этом уровне находится кампусная магистральная сеть и он обычно базируется на технологии Fast Ethernet. Этот уровень реализуется на крупных узлах и используется для соединения между собой отдельных зданий.
- **Уровень доступа.** На уровне доступа находится LAN-сеть или группа таких сетей, обычно Ethernet или Token Ring, предоставляющие доступ переднего плана к сетевым службам. На уровне доступа происходит подключение к сети всех узлов, включая серверы всех типов и рабочие станции пользователей. Проектированию уровня доступа посвящена глава 5.

Трехуровневая модель способна удовлетворить потребности большинства промышленных сетей. Однако не все сетевые среды требуют использования полной трехуровневой иерархии. В некоторых случаях достаточно двухуровневой модели или даже одноуровневой плоской модели. В некоторых случаях однако, иерархическая структура должна быть потенциально заложена в проектируемую сеть для возможного расширения модели до трех уровней при необходимости. В последующих разделах рассматриваются более подробно каждого из этих трех уровней. После этого рассматриваются иерархии из одного или двух уровней.

Функции магистрального уровня

Функция магистрального уровня состоит в обеспечении быстрого перемещения данных между удаленными центрами, как показано на рис. 12.28. Этот уровень не должен выполнять никаких операций с пакетами, таких как анализ списков доступа или фильтрация, поскольку они замедлили бы коммутацию пакетов. Магистральный уровень обычно реализуется как распределенная сеть WAN. Эта сеть WAN должна иметь избыточные маршруты для того, чтобы ее работоспособность сохранялась и в случае краткосрочных сбоев в каналах. Важными задачами при проектировании являются также распределение нагрузки и быстрая конвергенция протоколов маршрутизации. Эффективное использование полосы пропускания всегда является непростой задачей.

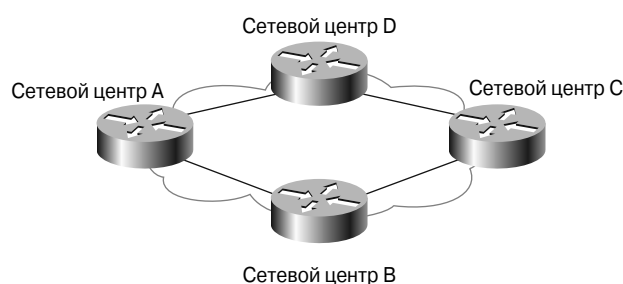


Рис. 12.28. Магистральный уровень

Функции уровня распределения

Уровень распределения в сети является демаркационной точкой между уровнем доступа и магистральным уровнем и выполняет функции определения и дифференциации магистрального уровня. Назначение этого уровня состоит в определении границ и именно на этом уровне происходят операции обработки пакетов. В среде WAN-сети уровень распределения может выполнять несколько функций, включая следующие:

- агрегирование адресов или зон;
- доступ пользователей отдела или рабочей группы к магистральному уровню;
- определение широковещательного домена или домена многоадресной рассылки;
- маршрутизация в виртуальных сетях LAN (Virtual LAN — VLAN));
- все требуемые переходы из одной среды передачи в другую;
- меры обеспечения безопасности.

Уровень распределения включает в себя магистраль кампуса со всеми подсоединенными к нему маршрутизаторами. Поскольку политики обычно реализуются на этом уровне, можно сказать, что уровню распределения обеспечивает основанные на политиках соединения. Термин “основанные на политиках соединения” означает, что маршрутизаторы сконфигурированы таким образом, что они допускают прохождение по сетевой магистрали только допустимых данных. Следует отметить, что полезным правилом проектирования является неразмещение конечных станций (таких как серверы) на магистрали. Отсутствие на магистрали конечных станций позволяет освободить магистраль от нерациональных для нее функций и функционировать только как транзитный маршрут передачи данных между рабочими группами и серверами масштаба кампуса.



Рис. 12.29. Уровень распределения

В средах отличных от среды кампуса может быть точкой, в которой удаленные узлы получают доступ к корпоративной сети. В целом уровень распределения можно охарактеризовать как уровень, обеспечивающий основанные на политиках соединения.

Функции уровня доступа

Уровень доступа является точкой, в которой локальные конечные пользователи получают доступ к сети, как показано на рис. 12.30. На этом уровне могут также применяться списки управления доступом или фильтры, которые используются для дальнейшей оптимизации потребностей конкретной группы пользователей. В среде кампуса функциями уровня доступа являются следующие:

- совместное использование полосы пропускания;
- коммутируемая полоса пропускания;
- фильтрация на MAC-уровне;
- микросегментация.

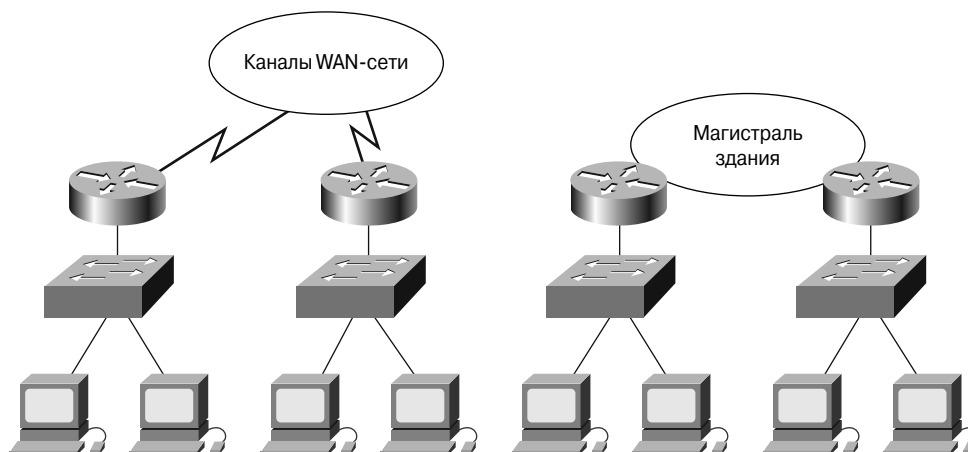


Рис. 12.30. Уровень доступа

На уровне доступа происходит подключение пользователей к локальным сетям LAN и самих сетей LAN к магистралям WAN-сетей или к WAN-каналам. Такой подход позволяет проектировщикам распределить службы устройств, функционирующих на данном уровне. Уровень доступа позволяет осуществить логическую сегментацию сети

и группировку пользователей в соответствии с выполняемыми ими функциями. Традиционно такая сегментация основывается на организационных границах (таких как отдел маркетинга, администрация или инженерный отдел). Однако с точки зрения управления сетью главной функцией уровня доступа является ограничение распространения широковещательных данных границами отдельной рабочей группы или локальной сети LAN. в средах, отличных от среды кампуса, уровень доступа может предоставлять удаленным узлам доступ к корпоративной сети с помощью какой-либо технологии распределенных сетей, такой как Frame Relay, ISDN или выделенные линии.

Преимущества иерархического подхода к проектированию сети WAN

Одним из преимуществ иерархического проектирования WAN-сети является то, что оно предоставляет метод управления характером передачи данных путем размещения точек маршрутизации на 3-м уровне по всей сети. Поскольку маршрутизаторы обладают способностью определять маршруты от узла-источника до узла получателя на основе адресации 3-го уровня, потоки данных перемещаются по иерархически организованной сети только по тем маршрутам, которые необходимы для того, чтобы эти данные достигли получателя, как показано на рис. 12.31.

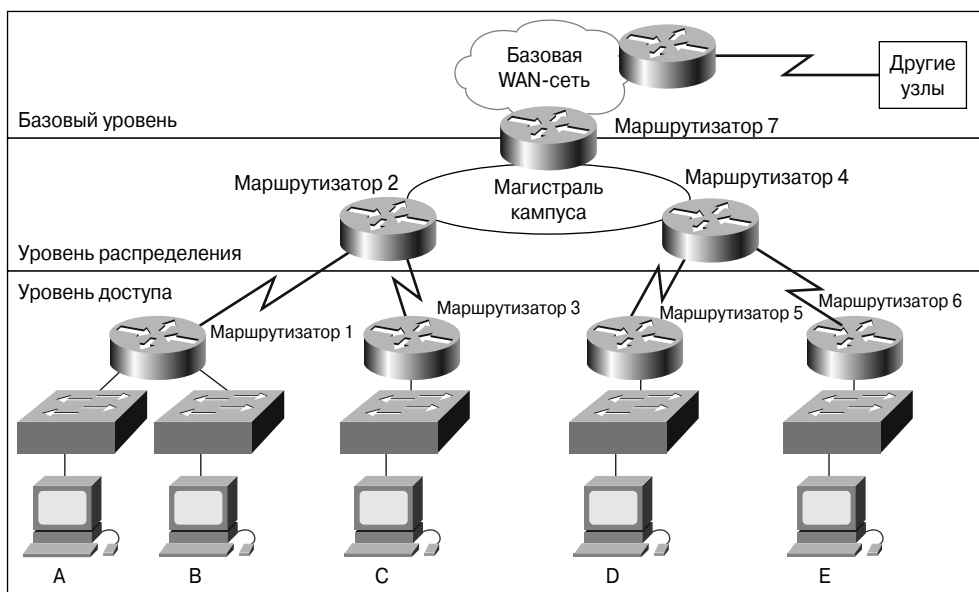


Рис. 12.31. Маршрутизаторы — точки, в которых принимаются решения о маршрутах

Если узлу A требуется установить соединение с узлом B, то потоки данных этого соединения будут передаваться маршрутизатору 1 и в обратном направлении узлу B. Следует обратить внимание на то, что на рис. 12.32 соединение не требует, чтобы все потоки данных помещались в канал между маршрутизаторами 1 и 2, что экономит полосу пропускания канала.

В иерархической структуре WAN-сети, состоящей из двух уровней, как показано на рис. 12.33, потоки данных перемещаются по ней только в восходящем направлении, как это требуется для достижения пункта назначения, что сохраняет полосу пропускания на других WAN-каналах.

Размещение серверов

Размещение серверов в соответствии с потребностями пользователей, имеющих к ним доступ, влияет на характер передачи данных по WAN-сети. Как показано на рис. 12.34, если разместить сервер предприятия на уровне доступа сетевого центра 1, то всем потокам данных, предназначенным этому серверу, придется проходить по каналам, находящимся между маршрутизаторами 1 и 2. Это приведет к потере значительной части полосы пропускания от центра 1.

Однако если разместить сервер предприятия на более высоком уровне иерархической структуры, как показано на рис. 12.35, то поток данных по каналу между маршрутизаторами 1 и 2 уменьшится и пользователи центра 1 смогут получить доступ к другим службам. На рис. 12.36 сервер рабочей группы размещен на уровне доступа центра, где имеется наибольшая плотность пользователей, и тем самым будет ограничено перемещение потоков данных, пересекающих WAN-канал для получения доступа к этому серверу. Таким образом, большая часть полосы пропускания станет доступной для получения доступа к ресурсам вне данного центра.

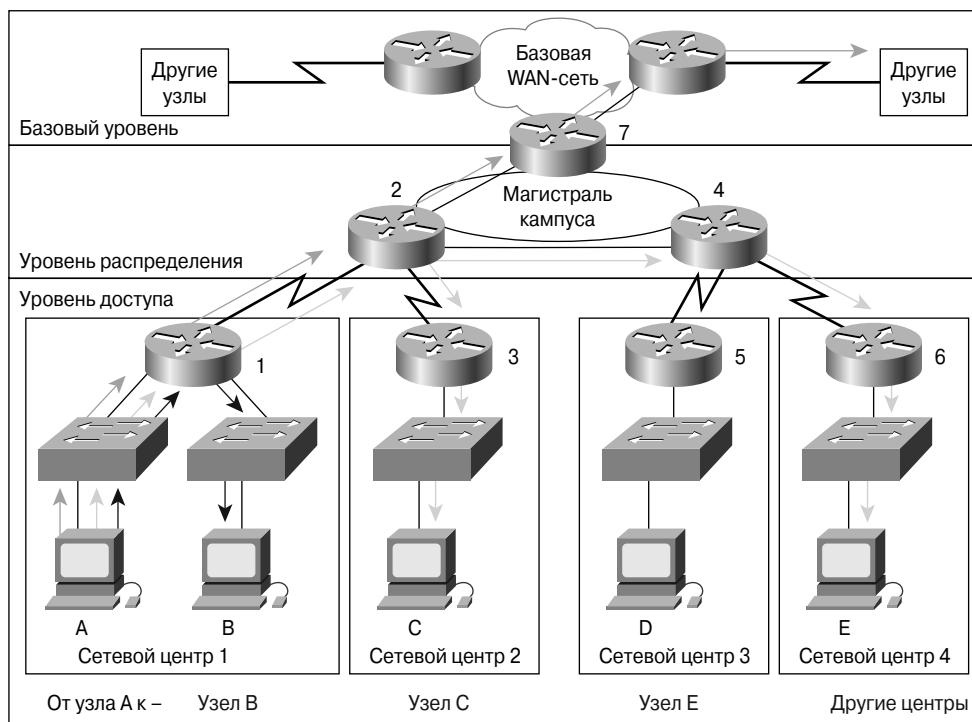


Рис. 12.32. Перемещение потоков данных, основанное на адресах источника и получателя

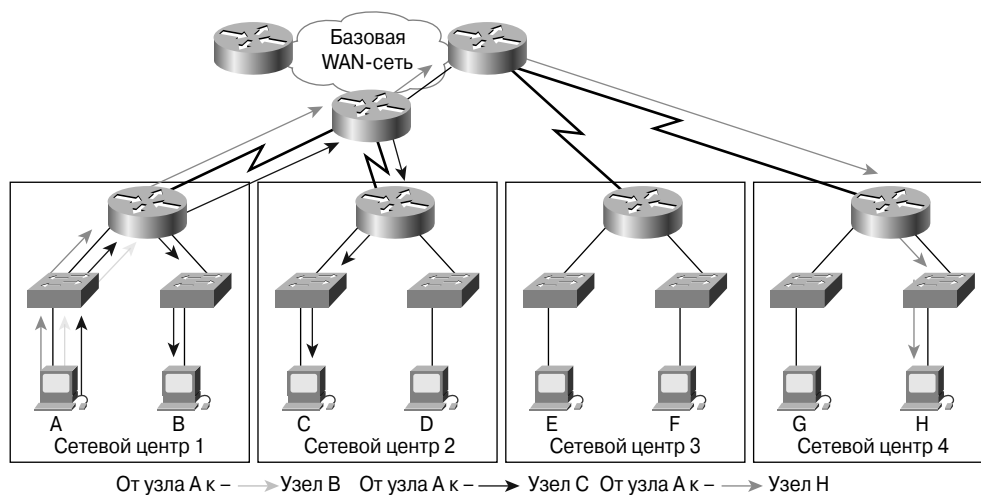


Рис. 12.33. Иерархическая структура WAN-сети, состоящая из двух уровней

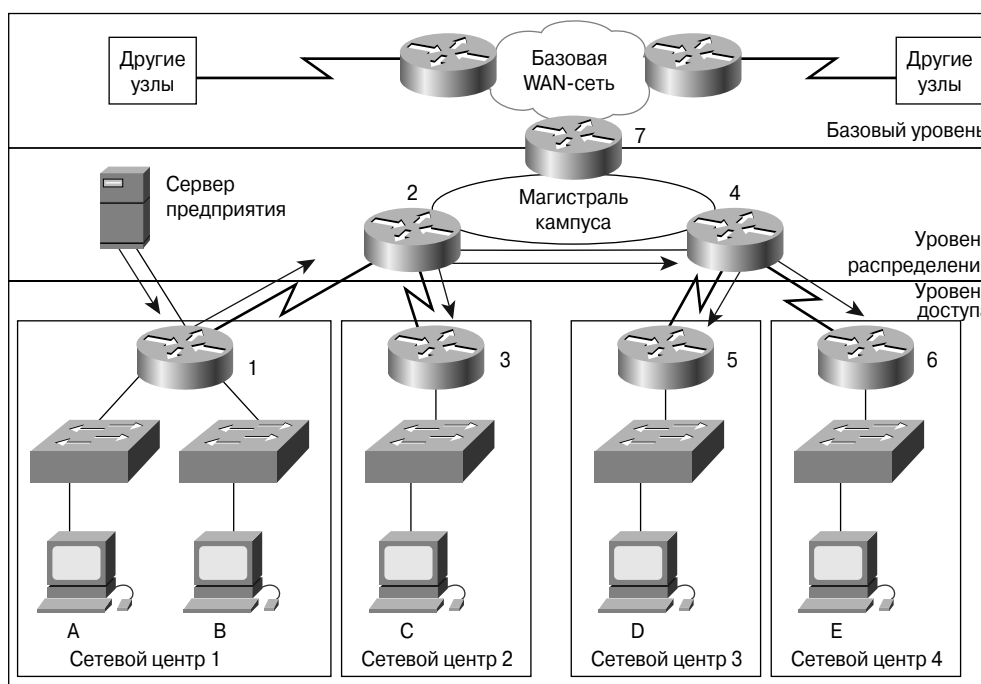


Рис. 12.34. Размещение сервера предприятия на уровне доступа

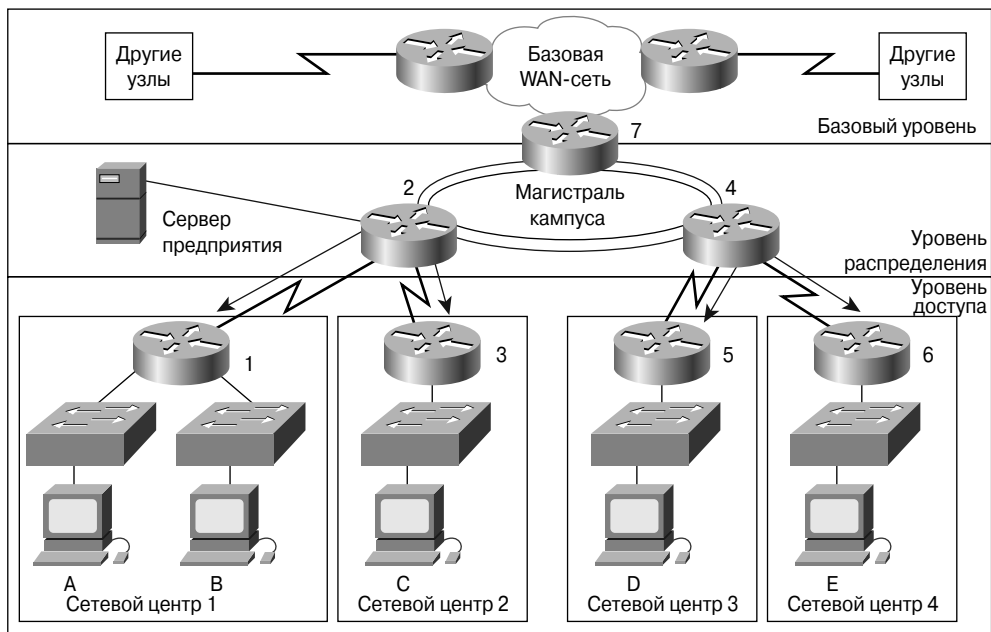


Рис. 12.35. Размещение сервера предприятия на более высоком уровне

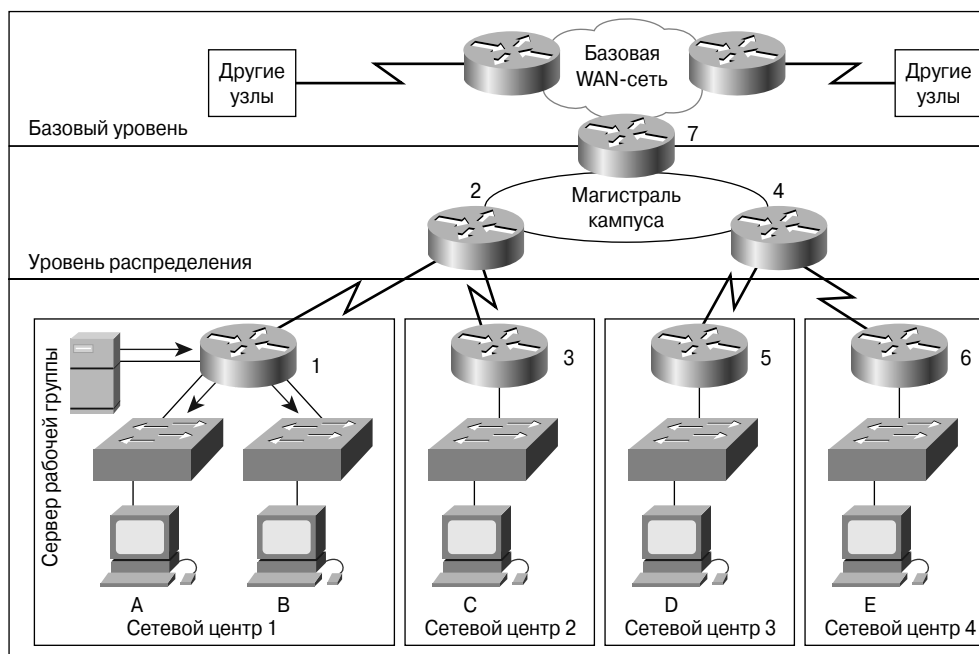


Рис. 12.36. Размещение сервера рабочей группы

Проектирование распределенных сетей WAN

Если передача данных происходит только между устройствами, находящимися в одном здании, то для нее достаточно создать локальную сеть LAN. Если некоторые данные требуется передавать между различными зданиями отдельного кампуса, то эти здания можно соединить между собой высокоскоростными каналами передачи данных и образовать LAN-сеть кампуса. Доступ отдельных индивидуальных пользователей к этой сети LAN и подключение этой сети к Internet являются отдельными темами и не являются предметом рассмотрения настоящей главы. Однако если требуется передача данных между географически удаленными друг от друга отдельными локальными сетями, то для ее реализации требуется использование распределенной сети WAN.

Большинству студентов вряд ли представится возможность проектировать новую WAN-сеть, однако многим придется принимать участие в проектировании расширений для уже существующих WAN-сетей или их модернизации и у них будет возможность применить на практике знания, полученные в результате изучения данной главы.

Этапы проектирования распределенной сети WAN

Проектирование WAN сети может оказаться нелегкой задачей. Систематический подход к проектированию сети позволяет добиться большей производительности сети и уменьшения расходов, связанных с ее созданием и обслуживанием. Многие WAN-сети были первоначально спроектированы без учета излагаемых ниже принципов и с течением времени эволюционировали. Однако каждый раз, когда рассматривается вопрос о модификации уже существующей WAN-сети, необходимо выполнить ряд действий, описанных ниже. Модификация сети может быть вызвана происшедшими изменениями, такими как расширение предприятия, которое данная сеть обслуживает или изменившиеся рабочие принципы или методы ведения бизнеса. Предприятия и корпорации устанавливают WAN-сети в тех случаях, когда им требуется регулярная и своевременная передача данных между различными подразделениями предприятия. Удовлетворение этих производственных требований требует расходов, которые в основном связаны с техническим обеспечением каналов передачи данных и с управлением сетью.

Для того чтобы оптимально спроектировать WAN-сеть, необходимо знать какие данные будут по ней передаваться, от каких источников и каким получателям. По сетям WAN передаются самые разные типы данных, которые предъявляют различные требования к полосе пропускания, задержке и уровню дребезжания. Для каждой пары конечных точек и каждого типа данных желательно знать характеристики передаваемых потоков данных. Их определение может потребовать обширных исследований и консультаций с пользователями сети. Проектирование часто включает в себя обновление, расширение или модификацию уже существующей WAN-сети. Многие требуемые данные можно получить из уже существующей статистики управления сетью.

Знание конечных пользователей позволяет выбрать топологию и расположение устройств для проектируемой сети. На выбор топологии оказывают влияние географические обстоятельства, а также такие требования, как доступность сети. Например, повышенные требования к доступности сети требуют создания дополнительных каналов для обеспечения альтернативных маршрутов передачи данных.

После того, как выбраны конечные точки и соединяющие их каналы, можно оценить для них требуемую пропускную способность с учетом того, что некоторые каналы передают только свои собственные данные, а другие также агрегированные потоки данных от нескольких источников.

К передаче данных по каналам WAN-сети могут предъявляться различные требования в отношении задержки и уровня дребезжания и эти требования, в совокупности с уже определенной потребностью в полосе пропускания, позволяют выбрать для каналов сети соответствующие технологии. После этого можно оценить расходы по установке и поддержке WAN-сети и сравнить их с производственными потребностями, которые вызывают необходимость в модернизации сети.

Последующее обсуждение должно выявить несколько ключевых областей, которые должны быть рассмотрены особенно тщательно при планировании и реализации WAN-сети. Выполнение описанных ниже действий позволит добиться эффективной работы сети с наименьшими затратами. Предприятия могут постоянно улучшать свои WAN-сети путем включения этих действий в планы предприятия.

Ниже рассмотрены два первичных фактора, который являются основными мотивами при проектировании и реализации WAN-сети.

- **Доступность приложений** — по сетям передается информация приложений от одного компьютера к другому. Если приложения оказываются недоступными пользователям сети, то она не выполняет требуемых от нее функций.
- **Общие затраты** — бюджеты соответствующих департаментов информационных систем (Information Systems — IS) часто достигают миллионов долларов. По мере того, как крупные коммерческие предприятия во всей большей степени полагаются на электронные средства для управления коммерческими операциями, связанная с этим стоимость использования компьютерных ресурсов продолжает, соответственно, возрастать. Рациональное проектирование WAN-сети помогает сбалансировать эти две цели — высокую эффективность и минимальную стоимость. При правильной реализации инфраструктура WAN-сети может оптимизировать доступность приложений и финансово эффективно использование уже существующих сетевых ресурсов.

В общем случае при проектировании WAN-сети необходимо принять во внимание описанные ниже три ключевых фактора.

- **Внешние физические условия** — эти условия включают в себя размещение узлов, серверов, терминалов и других конечных устройств, а также предполагаемый характер передачи данных в этой среде и предполагаемые затраты для достижения различных уровней предоставляемых служб.
- **Факторы, ограничивающие производительность сети** — эти факторы включают в себя надежность сети, пропускную способность и скорости передачи данных между клиентами и серверами (например, скорости сетевых адаптеров и скорости доступа к жестким дискам).
- **Сетевые факторы** — эти факторы связаны с параметрами сети и включают в себя сетевую топологию, пропускную способность каналов и тип передаваемых данных. Использование характеристик передаваемых по сети потоков данных критически важно для успешного планирования WAN-сети, однако немногие проектировщики выполняют этот этап, а часто и вообще его не осуществляют.

При проектировании WAN-сети нет более важного аспекта, чем получение и использование характеристик типов данных, которые будут передаваться по WAN-сети. Ниже приведены различные типы передаваемых данных.

- Голосовые и факсимильные данные.
- Данные транзакций (например, SNA).
- Данные сеансов связи “клиент-сервер”.
- Сообщения (например, электронная почта).
- Передача файлов.
- Пакетные данные.
- Данные управления сетью.
- Данные видеоконференций.

Анализ и отнесение к разным категориям сетевых данных является основой для принятия важнейших решений в процессе проектирования сети. Характер данных определяет требуемую пропускную способность, которая, в свою очередь, определяет требуемые затраты. Проверенные временем методы измерения и оценки характера передаваемых данных существуют для традиционных сетей, однако для WAN-сетей такие методы на данный момент отсутствуют.

Среди характеристик потоков данных можно выделить следующие:

- средние и пиковые нагрузки (объемы передачи);
- соединения и объемы потоков;
- ориентация соединений;
- допустимая задержка, включая ее длительность и вариацию;
- необходимый уровень доступа;
- допустимый уровень ошибок;
- приоритеты;
- тип протокола;
- средний размер пакета.

Поскольку многие сетевые планировщики не обладают необходимой техникой для работы со сложностями и неопределенностями, связанными с анализом характера потоков данных в WAN-сети, они обычно исходят из интуитивных представлений о требуемой пропускной способности, что приводит к созданию дорогостоящих, с излишней избыточностью сетей или малопродуктивных сетей с недостаточным техническим обеспечением.

Общей целью проектирования WAN-сети является минимизация ее стоимости на основе упомянутых выше принципов, обеспечивая вместе с тем уровень служб, соответствующий установленным требованиям доступности. При этом требуется решить две главных проблемы: доступность и минимальная стоимость. Решение какой-либо из этих проблем обычно не позволяет решать другую. Любое повышение уровня доступности обычно выражается в повышении стоимости. Поэтому необходимо тщательно взвесить относительную важность требований доступности ресурсов и минимизации стоимости.

Первым шагом в процессе проектирования является осознание и формулировка коммерческих производственных требований; этот процесс описан в последующих разделах. Требования к WAN-сети должны отражать цели, характеристики, коммерческие процессы и политику предприятия, на котором будет функционировать сеть.

Сбор требований

При проектировании WAN-сети в качестве первого этапа требуется собрать данные о структуре предприятия и его производственных процессах. После этого необходимо определить наиболее важных сотрудников предприятия, которые смогут помочь в процессе проектирования. Проектировщику следует обсудить с основными пользователями их потребности, узнать их географическое расположение и используемые приложения. Будущий проект сети должен учитывать требования пользователей.

Как правило, пользователям в первую очередь требуется доступность приложений. Главными компонентами этой доступности являются время отклика, пропускная способность и надежность.

- Под временем отклика понимается временной интервал между вводом команды или нажатием клавиши и выполнением системой узла этой команды или получение иного ответа. Приложениями, в которых короткое время отклика является ключевым фактором, являются интерактивные онлайн-сервисы, такие как автоответчики и кассовые терминалы.
- Работа приложений, требующих большой пропускной способности, обычно связана с передачей файлов. Однако часто такие приложения требуют также и короткого времени отклика. Часто удается организовать их работу в то время, когда объем передачи чувствительных ко времени данных невелик (например, после обычного рабочего дня).
- Хотя надежность передачи всегда является важным фактором, некоторые приложения предъявляют в этом вопросе особые требования, превышающие обычные. Организации, вся деятельность которых связана с онлайн-режимом или телефонной связью, требуют почти 100%-й активности сети. Примерами таких служб являются финансовые службы, рынок акций, службы чрезвычайных ситуаций, полиция и военные операции. В таких ситуациях требуется высокий уровень аппаратного обеспечения и избыточности. Определение убытков, возникающих в результате простоя сети является существенным фактором при определении требований к надежности проектируемой сети.

Выяснить требования пользователей можно различными способами. Чем больше пользователей вовлечено в процесс проектирования, тем более вероятно, что оценка окажется правильной. В общем для получения этой информации предлагается использовать описанные ниже методы.

- **Использование профилей сообщества пользователей.** Следует определить потребности различных групп пользователей. Хотя у многих обычных пользователей одинаковые потребности в отношении электронной почты, у них могут и свои индивидуальные требования, например, совместного использования локальных серверов печати в их зоне. Интервью, фокусные группы и обзоры образуют информационную базу для проектирования и реализации сети.

Возможно, что некоторым группам потребуется доступ к общим серверам. Другим, возможно, потребуется внешний доступ к конкретным внутренним вычислительным ресурсам.

Некоторым организациям может потребоваться особое управление системами поддержки IS в соответствии с каким-либо внешним стандартом.

Самым неформальным способом получения информации является проведение интервью с основными группами пользователей. Возможен также сбор фокус-групп для сбора информации и общей дискуссии между представителями различных организаций с аналогичными (или отличающимися) интересами.

Ко всему перечисленному выше стоит добавить использование формальных обзоров для получения статистической картины мнений пользователей, касающихся определенного уровня службы.

- **Тестирование человеческого фактора.** Наиболее затратным, требующим времени, но и, вероятно, наиболее эффективным способом оценки требований² пользователей является проведение тестов с представителями пользователей в лабораторной обстановке. Этот способ находит наибольшее применение в тех случаях, когда требуется оценить требования к времени отклика сети. Например, можно создать типовую рабочую обстановку и предложить пользователям осуществлять обычные действия удаленного доступа в лабораторной сети. Оценивая реакцию пользователей на изменения моделируемого времени отклика можно составить представление о граничных его значениях, обеспечивающих приемлемую производительность.

После сбора данных о структуре корпоративной сети необходимо определить маршруты перемещения информационных потоков в компании. Следует выяснить где находятся совместно используемые данные и кто ими пользуется.

Необходимо также узнать, требуется ли доступ к данным сети извне.

Перед проектированием сети необходимо составить себе четкое представление о проблемах, связанных с производительностью уже существующей сети. Если позволяет время, то следует проанализировать причины проблем с производительностью данной сети.

Анализ требований пользователей

Проектировщик должен проанализировать требования к сети, включая проблемы потребителей и технические задачи. Какие новые приложения будут реализованы в будущем? Есть ли приложения, работа которых требует выхода в Internet? К каким новым сетям потребуется обеспечить доступ? Каковы критерии успешного проектирования? (Как выяснить, был ли новый проект успешным?) Полезность сети определяется ее доступностью. На доступность влияют различные факторы, такие как пропускная способность, время отклика и доступ к ресурсам. У каждого потребителя имеется свое представление о доступности. Доступность может быть повышена путем увеличения ресурсов, однако дополнительные ресурсы требуют дополнительных затрат. Целью сетевого проекта является достижение максимальной доступности при минимальных затратах. Целью анализа требований является определение средних и пиковых скоростей передачи для каждого источника с течением времени. Следует попытаться охарактеризовать требуемую пропускную способность в течение обычного рабочего дня в отно-

шении передаваемых данных, уровня потоков, времени отклика узлов и времени, которое требуется для передачи файлов. В течение периода тестирования можно также оценить уровень использования существующего сетевого оборудования. В зависимости от типа передаваемых данных рекомендуется использовать один из приведенных ниже четырех методов анализа и измерения объема передаваемых данных.

- **Программное обеспечение управления сетью.** Для некоторых типов данных анализа статистики передачи данных может быть выполнен с помощью программного обеспечения управления сетью.
- **Уже существующие измерения.** На серверах может быть установлено специальное оборудование для анализа пакетных потоков на основе статистики маршрутизатора для имеющихся сетевых сегментов.
- **Оценка процесса.** В тех случаях, когда имеющиеся измерения недоступны (например, приложение еще не существует), могут быть использованы экспертные оценки. Для оценки скорости осуществления транзакций, длины пакетов и объема потоков рекомендуется работать в тесном контакте с разработчиками приложений и сетевыми администраторами.
- **Сравнительные источники.** Можно найти известные источники с аналогичными характеристиками и использовать имеющуюся для них статистику с соответствующими поправками.

Если характеристики тестируемой сети близки к характеристикам новой сети, то можно оценить требования новой сети на основе предполагаемого количества пользователей, характера приложений и топологии сети. В случае отсутствия средств точного измерения объемов и характера передаваемых данных этот метод является наилучшим способом оценки потоков данных в сети. В дополнение к мониторингу уже существующей сети можно замерить активность и объемы передачи, создаваемые известным количеством пользователей, подсоединенных к тестируемой сети, а затем использовать эти результаты для предсказания активности и объемов передачи предполагаемого количества пользователей.

При определении рабочей нагрузки возникает проблема, состоящая в том, что оказывается весьма трудно точно зарегистрировать нагрузку при передаче и производительность сетевых устройств как функцию количества пользователей, типа приложений и географического расположения. Это становится особенно трудным в том случае, когда реальной сети еще не существует.

Ниже приведены факторы, влияющие на динамические параметры сети.

- **Зависимость параметров доступа к сети от времени.** Периоды пиковых нагрузок могут приходиться на разное время суток, поэтому измерения должны включать в себя ряд измерений, включая периоды пиковых нагрузок.
- **Различия, связанные с типом передаваемых данных.** Потоки данных, управляемые на 3-м, сетевом уровне (маршрутизаторами) и на 2-м, канальном уровне (коммутаторами) предъявляют различные требования к сетевым устройствам и протоколам; некоторые протоколы чувствительны к отброшенным или утерянным пакетам, другие требуют большей полосы пропускания.
- **Случайный характер объема передаваемых потоков данных в сети.** Точное время поступления и конкретный тип потоков данных непредсказуемы.

Каждый источник данных имеет свою собственную метрику и все они должны быть преобразованы в единицу измерения “битов в секунду, бит/с”. Для получения и сравнения данных по отдельным пользователям необходимо стандартизировать единицу измерения объема передаваемых данных. В заключение отметим необходимость ввести коэффициент, учитывающий служебную нагрузку протокола, фрагментацию пакетов, возможное увеличение объема передачи и обеспечение безопасности. Варьируя этот коэффициент можно смоделировать различные возможные ситуации в сети. Например, можно запустить на сервере программу Microsoft Office и проанализировать объемы передачи данных, сгенерированных пользователями, совместно использующими это приложение. Полученное таким образом значение поможет определить требования к полосе пропускания и серверу при установке в сети приложения Microsoft Office.

Тестирование чувствительности сети

С практической точки зрения тестирование чувствительности сети включает в себя создание ситуации обрыва устойчивого канала и наблюдение возникающих последствий такого обрыва. При работе с тестовой сетью это сделать сравнительно легко. Можно внести изменение в работу сети удалив активный интерфейс и наблюдать реакцию сети на это событие. Можно также изменить уровень передачи данных сети для определения реакции сети на ситуацию когда объемы передачи данных приближаются к пределу возможностей передающей среды.

Топологии распределенных сетей

Под топологией сети понимается совокупность ее соединений и их взаимное расположение. Хотя возможны многие варианты топологий, все они основаны на нескольких основных типах.

При соединении непосредственным соединении двух LAN-сетей отдельным каналом образуется топология, принадлежащая к типу “точка-точка”, показанная на рис. 12.37. К такому соединению могут быть подсоединены дополнительные LAN-сети с сохранением топологии “точка-точка”. Такая топология легко реализуется, однако она имеет недостаток: на маршруте от отправителя к получателю все данные должны пройти через все промежуточные узлы. Ее преимуществом является то, что это, вероятно обеспечивает кратчайший маршрут, соединяющий все узлы, что является важным фактором в случае использования выделенных линий.

Для минимизации задержки при передаче данных из одной LAN-сети в другую соединения между узлами могут быть преобразованы таким образом, что они будут образовывать звезду. При этом количество каналов остается тем же самым, однако в такой топологии от одного узла до любого другого имеется только два перехода. Длина каналов, вероятно, увеличится и, соответственно, возрастут затраты. Маршрутизатору, находящемуся в центре звезды, потребуется по одному интерфейсу для каждого подсоединенного к нему узла, однако этим узлам потребуется только один WAN-интерфейс.

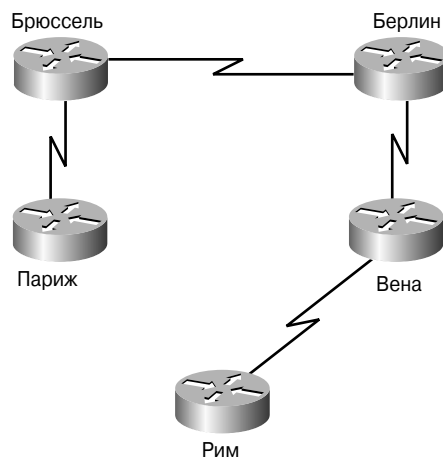


Рис. 12.37. Топология “точка-точка” в распределенной сети

Если требуется избыточность или минимальная задержка, то можно добавить дополнительные каналы, в результате чего образуется полносвязная топология, как показано на рис. 12.38. Теперь каждая LAN-сеть находится на расстоянии лишь одного перехода от любой другой сети и сеть становится более надежной и устойчивой, поскольку выход из строя любого отдельного узла не препятствует передаче данных другими узлами. Однако малая задержка и высокая надежность потребуют дополнительных затрат, поскольку потребуется значительно большее количество интерфейсов и каналов.

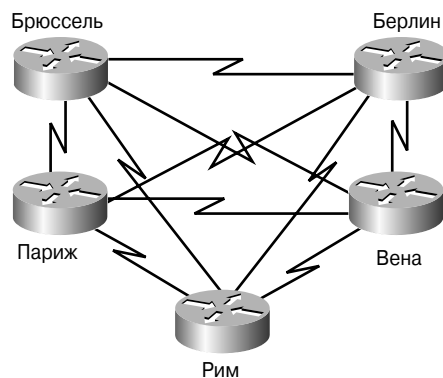


Рис. 12.38. WAN-сеть с полносвязной топологией

Количество каналов для топологии типа “точка-точка” или для звездообразной топологии на единицу меньше общего количества узлов, т.е. для N узлов потребуется $(N - 1)$ каналов. Для полносвязной топологии требуемое количество каналов вычисляется по формуле $N \times (N - 1) / 2$. Таким образом, сети с 50 узлами потребуется 49 каналов при звездообразной топологии и 1225 каналов для полносвязной. Полносвязная топология может быть экономичной лишь в очень небольших сетях.

Возможны также различные комбинации этих топологий. Часто базовая топология является звездообразной, однако некоторые вторичные узлы могут быть со-

единены между собой с образованием частично-связной топологии (рис. 12.39), которая обеспечивает определенную избыточность на случай сбоя. При росте сети эти базовые топологии с трудом поддаются масштабированию и в больших сетях требуется более структурированный подход. Иерархическая топология рассматривается в следующем разделе.

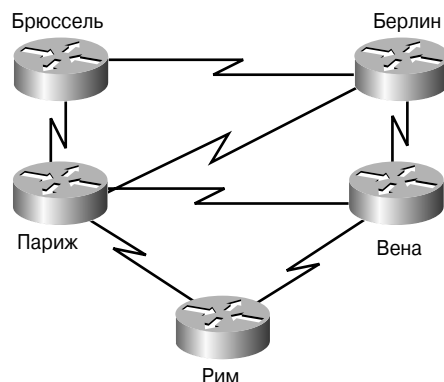


Рис. 12.39. WAN-сеть с частично-связной топологией

Идентификация сети и выбор сетевых возможностей

Проектирование WAN-сети состоит главным образом в выборе способа соединения между собой сетевых устройств и топологии каналов соединяющих географически удаленные друг от друга сети, а также в выборе для этих каналов технологий, удовлетворяющих потребности предприятия с приемлемыми затратами. Все технологии, за исключением использования телефонной сети, ISDN, DSL и кабельной сети, требуют использования выделенных линий. Выделенные линии могут непосредственно соединять отдельные подразделения предприятия или соединять их с ближайшей точкой присутствия (Point Of Presence — POP) сети совместного использования, такой как X.25, Frame Relay или ATM.

Непосредственные соединения как правило имеют гораздо большую протяженность и, соответственно, обходятся гораздо дороже, однако они доступны с практически любой полосой пропускания. Такие выделенные соединения обеспечивают очень маленькую задержку и низкий уровень дребезжания.

Сети ATM, Frame Relay и X.25 передают данные многих пользователей по одним и тем же внутренним каналам. Предприятие не имеет возможностей влиять на количество каналов или переходов, которые требуется пересечь данным в сети совместного использования или времени ожидания на каждом сетевом устройстве перед пересылкой их на следующий канал. Эта неопределенность задержки и дребезжания делает эти технологии неприемлемыми для некоторых типов передаваемых по сети данных. Однако эти недостатки совместно используемой сети часто перевешиваются меньшими затратами каждого отдельного пользователя, поскольку общие страты сети распределяются между многими пользователями.

Поскольку канал совместно используется несколькими пользователями, расходы каждого из них обычно существенно меньше тех, которые пришлось бы нести в случае использования выделенной линии с такой же пропускной способностью.

Хотя сети ATM являются сетями совместного использования, при их разработке ставилась цель обеспечить минимальную задержку и низкий уровень дребезжания, что достигается путем использования фреймов данных (ячеек) очень малой длины и высокоскоростных внутренних каналов. Такие сети часто используются для передачи чувствительных к задержке данных. Для передачи таких данных может быть также использована технология Frame Relay, в которой часто используются механизмы качества обслуживания QoS, которые предоставляют более высокий приоритет чувствительным к задержке данным.

Типичная WAN-сеть использует некоторую комбинацию технологий, которые обычно выбираются в зависимости от типа передаваемых данных и их объема. Для подсоединения отдельных подразделений предприятия к зоне используются технологии ISDN, Frame Relay или выделенные линии. Технологии Frame Relay, ATM и выделенные линии используются для подсоединения зон к магистрали; для создания WAN-магистрали используются ATM или выделенные линии.

Другие аспекты проектирования WAN-сети

Многим предприятиям требуются WAN-соединения с глобальной сетью Internet. Это создает проблемы обеспечения безопасности, однако предоставляет альтернативный вариант передачи данных между подразделениями предприятия. Часть данных, передача которых должна быть учтена в проекте, будет передаваться в сеть Internet или получаться из нее.

Поскольку доступ к Internet имеется, по-видимому, везде, где предприятие имеет локальную сеть LAN, эти данные и могут быть переданы двумя принципиально различными способами. Каждая локальная сеть может иметь соединение со своим локальным Internet-провайдером (ISP) или может существовать отдельное соединение между одним из базовых маршрутизаторов и Internet-провайдером. Преимущество первого подхода состоит в том, что потоки данных Internet передаются по сети Internet, а не по сети предприятия, что снижает требования к полосе пропускания. Однако недостаток использования нескольких каналов состоит в том, что вся WAN-сеть предприятия оказывается открытой для атак из Internet, а задача мониторинга и обеспечения безопасности многих точек соединений оказывается достаточно трудной. Для отдельной точки соединения легче применить соответствующую политику и обеспечить безопасность, несмотря на то, что WAN-сеть предприятия будет передавать данные, которые в противном случае были бы переданы по сети Internet.

Если каждая LAN-сеть предприятия имеет отдельное соединение с Internet, то для WAN-сети предприятия открывается другая возможность. В тех случаях, когда объем передаваемых данных относительно мал, сама сеть Internet может быть использована как WAN-сеть предприятия; при этом передача всех данных между подразделениями предприятия происходит через Internet. Обеспечение безопасности различных LAN-сетей может оказаться сложным вопросом, однако экономия на WAN-соединениях может компенсировать дополнительные расходы на обеспечение безопасности.

Насколько это возможно, серверы должны размещаться в тех точках сети, где они наиболее часто и интенсивно используются. Частое дублирование серверов, с использованием обновлений для серверов уменьшает требования к пропускной способности канала. Расположение доступных из Internet служб зависит от характера службы, предполагаемого объема передачи данных, от проблем с безопасностью и т.д. Эти задачи составляют особый предмет рассмотрения при проектировании сетей и в данной главе не рассматриваются.

Резюме

В данной главе были рассмотрены приведенные ниже ключевые вопросы.

- Существует много различных способов построения распределенных сетей.
- WAN-сети передают данные между географически удаленными друг от друга локальными сетями LAN.
- Обычно каналы передачи данных, используемые в WAN-сетях, принадлежат провайдером служб или операторам связи и предоставляются предприятиям за соответствующую оплату.
- WAN-сети могут передавать данные различных типов, такие как голос, видео и обычные данные, поэтому при соответствующем проектировании WAN-сети она должна обеспечивать требуемые предприятию параметры связи, такие как пропускная способность и время транзитных переходов.
- Поскольку сеть WAN является просто совокупностью соединений между расположенными в LAN-сетях базовыми маршрутизаторами, технологии WAN-сетей функционируют на трех самых нижних уровнях эталонной модели OSI.
- Проектирование WAN-сети часто включает в себя модификацию, расширение или модернизацию уже существующей WAN-сети.
- В WAN-сетях возможно использование различных топологий, таких как “точка-точка”, звездообразная и сеточная.
- Типичная WAN-сеть использует сочетание таких технологий как обновление уже существующей ISDN, Frame Relay, ATM и выделенные линии.
- При проектировании крупных WAN-сетей трехуровневое иерархическое проектирование предоставляет значительные преимущества.
- Подсоединение WAN-сетей предприятия к Internet является альтернативным решением для передачи потоков данных между филиалами предприятия.
- Удаленный доступ отдельного сотрудника из домашнего офиса к корпоративной сети предприятия можно осуществить с помощью аналогового модема, ISDN, DSL или кабельного модема.
- Аналоговые соединения, а также соединения ISDN и DSL, используют существующие телефонные линии, в то время как кабельные модемы используют отдельную коаксиальную кабельную сеть.
- Аналоговые соединения и соединения ISDN требуют набора номера получателя и обеспечивают соединения только в том случае когда оно требуется. DSL-соединения и соединения через кабельный модем функционируют все время пока компьютер включен.
- Ширина полосы пропускания у различных технологий отличается; при этом скорости передачи DSL и кабельного модема значительно превосходят скорости аналоговых соединений и соединений ISDN.

В дополнение к материалу, изложенному в настоящей главе, рекомендуется ознакомиться с лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

Асинхронный режим передачи (Asynchronous Transfer Mode — ATM). Международный стандарт пересылки ячеек, в котором данные различных служб, таких как голос, видео и обычные данные, передаются в ячейках фиксированной длины (53 байта). Фиксированная длина ячеек позволяет обрабатывать их аппаратным обеспечением, тем самым сокращая транзитную задержку. Технология ATM позволяет воспользоваться преимуществам высокоскоростных передающих сред, таких как E3, SONET и T3.

Коммутация каналов (circuit switching). Способ коммутации, при использовании которого между отправителем и получателем на время “вызова” должен существовать выделенный физический маршрут. Этот тип коммутации широко используется в телефонных сетях.

Коммутация пакетов (packet switching). Способ коммутации, при использовании которого узлы сети совместно используют общую полосу пропускания, рассылая друг другу пакеты.

Коммутируемые виртуальные каналы (switched virtual circuits — SVCs). Такие виртуальные каналы устанавливаются по требованию и разрываются после окончания передачи. Каналы SVC используются когда передача данных имеет спорадический характер. В терминологии ATM называются коммутируемыми виртуальными соединениями.

Модуль DSU также несет ответственность за выполнение такой функции, как синхронизация сигнала. В ссылках часто упоминается вместе с модулем CSU как CSU/DSU.

Модуль канальной службы (channel service unit — CSU). Устройство цифрового интерфейса, соединяющее оборудование конечного пользователя с локальным ответвлением цифровой телефонной станции. Часто в ссылках объединяется с модулем DSU (CSU/DSU).

Модуль цифровой службы (digital service unit — DSU). Устройство, используемое при передаче цифровых данных, которое адаптирует физический интерфейс устройства DTE к среде передачи, такой как T1 или E1.

Мультиплексирование с разделением времени (time-division multiplexing — TDM). Способ мультиплексирования, при использовании которого информации из нескольких каналов может предоставляться полоса пропускания в одном кабеле на основе установленных заранее временных отрезков, называемых тайм-слотами (time slot). Соответствующая часть полосы пропускания выделяется каждому каналу, независимо от того, имеет ли он данные для передачи.

Оборудование пользователя (customer premises equipment — CPE). Оконечное оборудование, такое как терминалы, телефоны и модемы, предоставляемое телефонной компанией, устанавливаемое на узле пользователя и подсоединенное к сети телефонной компании.

Оборудование терминала данных (data terminal equipment — DTE). Устройство интерфейса “пользователь-сеть” со стороны пользователя, которое выступает в качестве источника данных, получателя или их обоих. Устройство DTE подсоединяется к сети данных через устройств DCE и обычно использует синхронизирующие сигналы, генерируемые устройством DCE. К оборудованию DTE относятся такие устройства, как компьютеры, трансляторы протоколов и мультиплексоры.

Постоянный виртуальный канал (permanent virtual circuits — PVCs). Виртуальный канал, который постоянно находится в установленном состоянии. Использование каналов PVC

позволяет экономить полосу пропускания, затрачиваемую на установку и разрыв соединения в ситуациях, когда некоторые виртуальные каналы должны существовать постоянно. В терминологии АТМ называются постоянными виртуальными соединениями.

Терминальное оборудование канала передачи данных (data circuit-terminating equipment, data communications equipment — DCE). Устройства и соединения коммуникационной сети, представляющие собой конечную сетевую часть интерфейса “пользователь-сеть”. Устройства DCE обеспечивают физическое соединение с сетью, пересылают потоки данных и обеспечивают подачу синхронизирующего сигнала, используемого для согласования процессов обмена данными между устройствами DCE и DTE. Примерами устройств DCE могут служить модемы и карты сетевого интерфейса (сетевые адаптеры).

Центральный офис телефонной компании или телефонная станция (central office — CO). Офис местной телефонной компании, к которому подсоединены все локальные ответвления данного района и в котором происходит коммутация каналов, соединяющих станцию с абонентами.

Контрольные вопросы

1. Для какого из перечисленных ниже типов данных аналоговые соединения удаленного доступа являются неподходящим решением?
 - A. Сообщения электронной почты (E-mail)
 - B. Передача файлов небольшого объема
 - C. Отчеты
 - D. Видео
2. Какое из приведенных ниже утверждений, относящихся к технологии ISDN, справедливо?
 - A. BRI ISDN предоставляет пользователю два В-канала и один D-канал
 - B. D-канал, работающий на скорости 16 Кбит/с, предназначен для передачи данных пользователя
 - C. BRI ISDN предоставляет пользователю два В-канала и один D-канал в Северной Америке
 - D. Общая битовая скорость BRI ISDN составляет 2,533 Мбит/с
3. Выделенная линия представляет собой канал типа _____, который обеспечивает отдельный ранее установленный маршрут коммуникации в распределенной сети WAN от пользователя к удаленной сети.
 - A. “точка-точка”
 - B. “точка-несколько точек”
 - C. аналоговое соединение
 - D. цифровое соединение
4. Какое из приведенных ниже утверждений о сетях X.25 не является истинным?
 - A. Скорость передачи является низкой
 - B. Пакеты данных не подвержены задержке
 - C. Широко используются в приложениях EDI
 - D. Оплата службы определяется объемом переданных и полученных данных

5. Каким образом Frame Relay одновременно обрабатывает несколько сеансов связи по одному физическому соединению?
 - A. Frame Relay мультиплексирует отдельные каналы
 - B. Несколько одновременных сеансов связи не допускаются
 - C. Frame Relay дуплексирует сеанс связи
 - D. Frame Relay преобразует их в ячейки ATM
6. Какое из приведенных ниже утверждений о технологии ATM не является истинным?
 - A. Она позволяет передавать голос, видео и обычные данные
 - B. ATM предоставляет большую полосу пропускания, чем технология Frame Relay.
 - C. Она в большей степени базируется на архитектуре ячеек, чем на архитектуре фреймов
 - D. Ячейки ATM имеют фиксированную длину в 35 байтов
7. Оборудование, расположенное в помещениях пользователя, подключаемое к центральному офису провайдера службы, называется:
 - A. DTE
 - B. DCE
 - C. CPE
 - D. Ничто из вышеперечисленного
8. Устройства, передающие данные в локальное ответвление, называются :
 - A. DTE
 - B. DCE
 - C. CPE
 - D. Ничто из вышеперечисленного
9. Устройства пользователя, передающие данные в DCE, называются:
 - A. DTE
 - B. DCE
 - C. CPE
 - D. Ничто из вышеперечисленного
10. Для передачи данных по цифровым каналам требуется _____ и _____.
 - A. CSU и DSU
 - B. DTE и DCE
 - C. T1 и E1
 - D. Ничто из вышеперечисленного
11. Для аналоговых WAN-служб требуется _____.
 - A. оборудование DCE
 - B. оборудование DTE
 - C. Модем
 - D. Адаптер NIC
12. Какая из перечисленных ниже технологий не использует коммутацию каналов?

- A. Общедоступная коммутируемая телефонная сеть (Public Switched Telephone Network — PSTN)
 - B. Интерфейс базовой скорости ISDN (ISDN Basic Rate Interface — BRI)
 - C. Интерфейс первичной скорости ISDN (ISDN Primary Rate Interface — PRI)
 - D. SONET
13. В сетях с коммутацией пакетов устанавливаемые при включении коммутаторов маршруты называются:
- A. Постоянными виртуальными каналами (Permanent virtual circuits — PVCs)
 - B. Коммутируемыми виртуальными каналами (Switched virtual circuits — SVC)
 - C. Постоянной виртуальной службой (Permanent virtual service — PVS)
 - D. Коммутируемой виртуальной службой (Switched virtual service — SVS)
14. В сетях с коммутацией пакетов маршруты, устанавливаемые по требованию называются:
- A. Постоянными виртуальными каналами (Permanent virtual circuits — PVCs)
 - B. Коммутируемыми виртуальными каналами (Switched virtual circuits — SVC)
 - C. Постоянной виртуальной службой (Permanent virtual service — PVS)
 - D. Коммутируемой виртуальной службой (Switched virtual service — SVS)
15. Какой из приведенных ниже типов службы характерен для соединений ISDN?
- A. Асинхронное соединение удаленного доступа
 - B. Асинхронная выделенная линия
 - C. Синхронное соединение удаленного доступа
 - D. Синхронная выделенная линия
16. Какое из приведенных ниже устройств относится к оборудованию DCE?
- A. Маршрутизатор
 - B. Модем
 - C. Коммутатор
 - D. Концентратор
17. На каком уровне эталонной модели OSI функционирует протокол PPP?
- A. На сетевом
 - B. На канальном
 - C. На уровне приложений
 - D. На транспортном уровне
18. На каком уровне эталонной модели OSI функционирует протокол Frame Relay?
- A. На 1-м уровне
 - B. На 2-м уровне
 - C. На 4-м уровне
 - D. На 3-м уровне
19. Интерфейс BRI ISDN состоит из:
- A. 2-х В-каналов и 2-х D-каналов
 - B. 2-х В-каналов и 1-го D-канала
 - C. 23 В-каналов и 1-го D-канала
 - D. 30 В-каналов и 1-го D-канала



В этой главе...

- Определяются и описываются базовые компоненты, определяющие характер связи по протоколу “точка-точка” (Point-to-Point Protocol — PPP)
- Определено и описано использование фреймов протокола управления каналом (link control protocol — LCP) и протокола управления сетью (Network Control Protocol — NCP) в протоколе PPP
- Рассмотрено конфигурирование и тестирование протокола PPP
- Описана аутентификация в протоколе PPP
- Определена и описана аутентификация по паролю
- Описано использование протокола аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol — CHAP)

Протокол PPP

В настоящей главе описаны базовые компоненты, процессы и операции, определяющие связь по протоколу PPP (PPP). Кроме этого, описано использование фреймов протоколов LCP и Network Control Protocol в протоколе PPP. В заключение рассмотрено конфигурирование и тестирование протокола PPP. Наряду с аутентификацией протокола PPP рассмотрено использование протокола аутентификации по паролю (Password Authentication Protocol — PAP) и протокола CHAP.

Протокол PPP, описанный в RFC 1661, является эффективным решением для удаленных соединений с сетью Internet, включая соединения цифровой сети интегрированных служб (Integrated Services Digital Network — ISDN). Протокол PPP является уровневым протоколом и его функционирование начинается с включения протокола LCP для установки канала, его конфигурирования и тестирования. После инициализации протокола LCP для передачи данных в соответствии с каким-либо стеком протоколов может быть использован один или несколько протоколов управления сетью (Network Control Protocols). В частности, управляющий протокол IP (IP Control Protocol — IPCP) описанный в RFC 1332, позволяет передавать IP-пакеты по каналам PPP. Другие протоколы NCP используются для протоколов AppleTalk (RFC 1378), OSI (RFC 1377), DECnet Phase IV (RFC 1762), Vines (RFC 1763), XNS (RFC 1764) и для прозрачных мостовых соединений Ethernet (RFC 1638).

Ниже приведены некоторые ключевые функции, которые будут обсуждаться далее в настоящей главе.

- **Уведомление об адресе** — эта функция позволяет серверу информировать удаленного клиента о его IP-адресе для данного канала, однако механизм позволяет также клиенту самому запрашивать IP-адреса и поддерживать конфигурацию в случае сбоя в сети. В протоколе SLIP требовалось, чтобы пользователь конфигурировал эту информацию вручную. В RFC 1877 предусмотрены опции уведомления об адресах сервера имен, как для Internet, так и для NetBIOS.
- **Аутентификация** — эта функция может выполняться с протоколами PAP и CHAP. Оба этих протокола описаны в RFC 1334.
- **Поддержка нескольких протоколов** — на одном канале могут одновременно выполняться несколько протоколов; для этого требуется лишь запуск дополнительных протоколов NCP. Например, по одному и тому же каналу PPP могут передаваться потоки данных протоколов IP и IPX.
- **Мониторинг канала** — эта функция включает в себя рассылку эхо-сообщений, которые могут периодически регистрировать состояние канала.

Рекомендуется также выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Уровневая архитектура протокола PPP

Протокол PPP обеспечивает соединения маршрутизатор-маршрутизатор и узел-сеть как по синхронным, так и по асинхронным каналам. На рис. 13.1 показана инкапсуляция протокола PPP, используемая в сетях WAN. PPP является одним из наиболее популярных и широко используемых протоколов, благодаря тому, что он предлагает пользователям следующие функции:

- контроль установки канала передачи данных;
- назначение IP-адресов и управление ими;
- мультиплексирование данных от нескольких сетевых протоколов;
- конфигурирование канала и его тестирование его качества;
- обнаружение ошибок в конфигурации.



Рис. 13.1. Протокол “точка-точка” в распределенной сети WAN

Протокол PPP имеет структуру, включающую в себя несколько уровней. Использование уровней облегчает описание связи между связанными между собой уровнями. Эталонная модель OSI представляет собой уровневую архитектуру, используемую для описания работы сетей. Протокол PPP предоставляет метод инкапсуляции дейтаграмм различных протоколов для передачи по каналу типа “точка-точка” и использует канальный уровень для тестирования соединения. Из этого следует, что протокол PPP в своей архитектуре использует три уровня модели OSI. На рис. 13.2 показана сфера действия протокола PPP в эталонной модели OSI. На рис. 13.3 показаны функции протокола PPP на различных уровнях.

- Физический уровень используется для реального физического соединения типа “точка-точка” и передачи по нему данных.
- Канальный уровень используется для установки и конфигурирования этого соединения.
- Сетевой уровень используется для конфигурирования различных протоколов сетевого уровня.

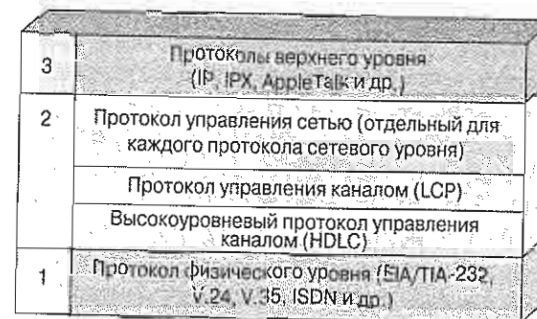


Рис. 13.2. Протокол PPP и эталонная модель OSI

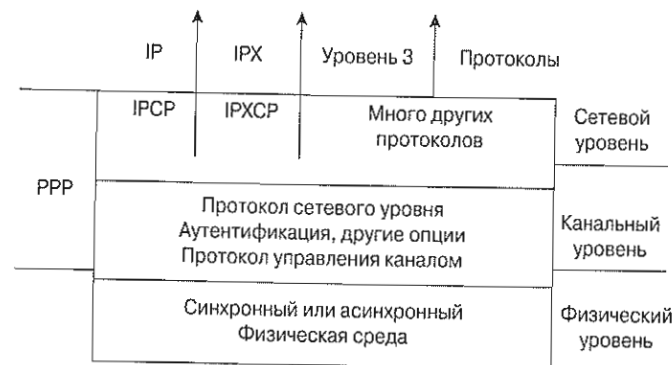


Рис. 13.3. Функции протокола PPP на различных уровнях

Протокол PPP может быть сконфигурирован на следующих типах физических интерфейсов:

- последовательный асинхронный;
- последовательный синхронный;
- высокоскоростной последовательный интерфейс (High-Speed Serial Interface — HSSI);
- ISDN.

Протокол PPP использует свой протокол LCP для обсуждения параметров и установки опций управления каналом распределенной сети WAN. Программный компонент управления сетью (Network Control Program) используется протоколом PPP для инкапсуляции и обсуждения опций для нескольких протоколов сетевого уровня. Протокол LCP находится в верхней части физического уровня и используется для установки, конфигурирования и тестирования канала передачи данных. Протокол PPP также использует LCP для автоматического согласования перечисленных ниже опций формата инкапсуляции.

- **Аутентификация** — опции аутентификации требуют, чтобы вызывающая сторона канала ввела информацию, которая позволяет убедиться, что вызывающая сторона имеет разрешение сетевого администратора на вызов (рис. 13.4). Сообщениями аутентификации обмениваются маршрутизаторы одного ранга. Ниже описаны две возможных альтернативы.

- Протокол PAP
- Протокол CHAP



Рис. 13.4. Аутентификация

- **Сжатие** — опции сжатия увеличивают эффективную полосу пропускания соединений PPP путем уменьшения объема данных во фрейме, которые передаются по каналу. У получателя происходит декомпрессия (распаковка) данных (рис. 13.5). На маршрутизаторах Cisco имеются два алгоритма сжатия: Stacker и Predictor.



Рис. 13.5. Сжатие

- **Обнаружение ошибок** — механизмы обнаружения ошибок протокола PPP позволяют процессу обнаруживать признаки сбоев. Опции Quality и Magic Number позволяют поддерживать надежные, свободные от петель каналы.
- **Многоканальность** — версии IOS Cisco 11.1 и более поздние поддерживают многоканальность. Эта альтернатива позволяет осуществлять перераспределение нагрузки на интерфейсы маршрутизатора, используемые протоколом PPP (рис. 13.6).



Рис. 13.6. Многоканальность

- **Обратный вызов по протоколу PPP** — для дальнейшего повышения уровня безопасности IOS Cisco версии 11.1 предлагает функцию обратного вызова по протоколу PPP. При использовании этой опции маршрутизатор Cisco может выступать в качестве клиента обратного вызова или сервера обратного вызова. Клиент делает первоначальный вызов, запрашивает вызов от другой стороны, а затем прекращает первоначальный вызов. Маршрутизатор, выполняющий обратный вызов, отвечает на первоначальный вызов и делает обратный вызов клиента на основе директив в своей собственной конфигурации.

Протокол LCP также выбирает максимальный из возможных размеров пакета, обнаруживает типичные ошибки конфигурирования, закрывает канал, а также определяет, нормально ли функционирует канал или в нем возник сбой. Протокол PPP позволяет нескольким сетевым протоколам функционировать на одном и том же канале связи. Для каждого протокола сетевого уровня устанавливается отдельный протокол управления сетью. Например, Internet Protocol (IP) использует IPCP, а протокол Internetwork Packet Exchange (IPX) использует IPCP. Протоколы NCP включают в себя функциональные поля, которые содержат стандартизированные коды, указывающие тип протокола сетевого уровня, использованный при PPP-инкапсуляции. Поля фрейма PPP показаны на рис. 13.7 и описаны ниже.

- **Поле флага** — это поле указывает на начало или конец фрейма и представляет собой бинарную последовательность 01111110.
- **Поле адреса** — состоит из стандартного широковещательного адреса, который представляется бинарной последовательностью 11111111. Протокол PPP не назначает станциям индивидуальных адресов.
- **Управляющее поле** — это поле длиной один байт содержит бинарную последовательность 00000011, которая требует передачи данных пользователя в непосредственном фрейме.
- **Протокол** — два байта, определяющих тип протокола, данные которого находятся во фрейме (табл. 13.1).

Таблица 13.1. Некоторые типы протоколов, поддерживаемые протоколом PPP

Значение (шестнадцатеричное)	Название протокола
8021	IPCP
8023	OSI Network Layer Control Protocol
8029	AppleTalk Control Protocol
802b	Novell IPX Control Protocol
c021	LCP
c023	PAP
c223	CHAP

Дополнительная информация

Дополнительные значения полей протокола PPP, не включенные в приведенную выше таблицу, можно узнать по адресу <http://www.iana.org/assignments/ppp-numbers>.

- **Данные** — 0 или более байтов, содержащих данные дейтаграммы для протокола, указанного в поле протокола. Конец поля данных указывается закрывающим флагом, за которым следуют два байта поля контрольной суммы (frame check sequence — FCS). По умолчанию длина поля данных равна 1500 байтов.
- **Поле контрольной суммы (FCS)** — обычно длина этого поля равна 16 битам (2 байта). Эти дополнительные символы добавляются к фрейму для контроля ошибок передачи.

Длина поля
в байтах

1	1	1	2	Переменной длины	2 или 4
Флаг	Адрес	Управление	Протокол	Данные	FCS

Рис. 13.7. Формат фрейма протокола PPP

Установка сеанса протокола PPP

Протокол PPP предоставляет средства установки, конфигурирования, поддержки и закрытия соединения типа “точка-точка”. Процесс установки связи по каналу “точка-точка” протокола PPP состоит из четырех этапов, описанных ниже.

- 1. Создание канала и согласование конфигурации.** Иницирующий узел протокола PPP посылает LCP-фреймы для конфигурирования и тестирования канала передачи данных.
- 2. Проверка качества работы канала.** На этом этапе канал тестируется для проверки того, что его качество достаточно для включения протоколов сетевого уровня. Отметим, что эта стадия не является обязательной.
- 3. Согласование конфигурации протокола сетевого уровня.** Иницирующий узел протокола PPP рассылает NCP-фреймы для выбора и установки конфигурирования протоколов сетевого уровня, таких как TCP/IP, Novell IPX и Apple-Talk. После того, как протоколы сконфигурированы, по каналу могут пересылаться пакеты этих протоколов сетевого уровня.
- 4. Окончание работы канала.** Конфигурация канала связи сохраняется до тех пор, пока LCP- или NCP-фреймы не закроют канал, или до какого-либо внешнего события (например, истечения времени таймера простоя или вмешательства пользователя).

Используются три типа LCP-фреймов.

- **Фреймы установки канала связи.** Используются для создания и конфигурирования канала.
- **Фреймы закрытия канала.** Используются для прекращения работы канала.
- **Фреймы поддержки работы канала.** Используются для отладки канала и для управления им.

LCP-фреймы используются на всех четырех стадиях работы протокола LCP, описанных в последующих разделах.

Пример согласования параметров канала приведен на рис. 13.8.



Рис. 13.8. Согласование параметров канала PPP

В табл. 13.2 описаны этапы установки соединения PPP.

Таблица 13.2 Этапы установки соединения PPP

Этап	Описание
1. Установка канала	На этом этапе каждое устройство PPP посылает фреймы протокола LCP для конфигурирования и тестирования канала передачи данных. Фреймы LCP содержат поле опций конфигурации, которое позволяет устройствам обсуждать использование таких опций, как максимальный размер передаваемого блока (модуля) (maximum transmit unit — MTU), сжатие некоторых полей протокола PPP и протокол аутентификация для данного канала. Если опция конфигурации не включена в пакет LCP, то для нее принимается значение по умолчанию. До того, как начнется обмен пакетами сетевого уровня, протокол LCP должен сначала открыть соединение и обсудить параметры конфигурации. Этот этап заканчивается, после того, как был отправлен фрейм подтверждения конфигурации и на него получен ответ
2. Определение качества канала	После того, как канал установлен и был выбран протокол аутентификации, происходит аутентификация партнера по связи. Аутентификация, если она используется, происходит до того, как начнется этап работы сетевого протокола. В качестве элемента этого этапа протокол LCP позволяет выполнить необязательную проверку качества работы канала. На этой стадии канал тестируется с целью выяснения, обеспечивает ли он достаточное качество для работы протоколов сетевого уровня.
3. Протокол сетевого уровня	На этой стадии устройства PPP рассылает пакеты NCP для выбора и конфигурирования одного или нескольких протоколов сетевого уровня (таких как IP). После того как установлены параметры конфигурации всех выбранных протоколов сетевого уровня, от каждого из них по каналу могут быть отправлены дейтаграммы. Если LCP закрывает какой-либо из каналов, то об этом информируются все остальные протоколы сетевого уровня, которые могут в этом случае предпринять соответствующие действия. После того как произведена настройка параметров протокола PPP, проверка состояния LCP и NCP может быть выполнена с помощью команды show interfaces
4. Закрытие канала	Протокол LCP может закрыть канал в любое время. Обычно это делается по запросу пользователя, но может также произойти вследствие некоторого физического события, например в связи с повреждением носителя или истечением заданного промежутка времени

Протоколы аутентификации сеанса PPP

Как было сказано ранее, стадия аутентификации сеанса PPP не является обязательной. После установления связи и принятия решения о протоколе аутентификации может быть выполнена проверка подлинности другой стороны, участвующей в сеансе связи. Если такая проверка выполняется, то она проводится до начала установки параметров конфигурации протокола сетевого уровня.

Опции аутентификации требуют, чтобы вызывающая сторона канала ввела информацию по проверке подлинности, которая позволит убедиться, что данный пользователь имеет разрешение сетевого администратора на вход в сеть. Маршрутизаторы одного ранга обмениваются сообщениями об аутентификации.

При настройке параметров аутентификации протокола PPP можно выбрать проверку с помощью протоколов PAP или CHAP. Как правило, предпочтение отдается протоколу CHAP. В целом на практике предпочтение обычно отдается протоколу CHAP.

Протокол аутентификации по паролю PAP

Протокол PAP предоставляет удаленному узлу простой способ подтвердить свою идентичность путем использования двухэтапного квитирования (handshake). После того как стадия создания PPP-канала закончена, удаленный узел регулярно посылает по каналу имя пользователя и его пароль до тех пор, пока идентичность не будет подтверждена или канал не будет закрыт. Пример работы протокола PAP приведен на рис. 13.9.

Протокол PAP не является строгим протоколом аутентификации. Пароли передаются по каналу в виде открытого текста, и отсутствует защита от повторного воспроизведения или повторных атак с целью случайным образом пробиться в сеть. Однако попытки подключения, их частота и время регистрируются удаленным узлом.

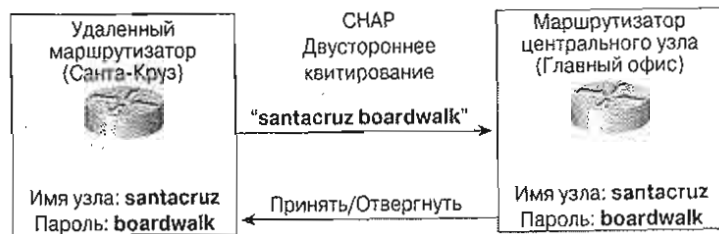


Рис. 13.9. Аутентификация по протоколу PAP

CHAP

Протокол CHAP используется для периодической проверки подлинности удаленного узла с использованием метода трехэтапного квитирования. Такая проверка осуществляется после создания первоначального канала и может быть повторена в любой момент времени.

После создания канала PPP хост посылает сообщение о вызове на удаленный узел. Удаленный узел посылает в ответ соответствующее значение. Хост сравнивает его с имеющимся у него значением и, если они совпадают, подлинность подтверждается. В противном случае связь прекращается. Пример работы протокола CHAP приведен на рис. 13.10.

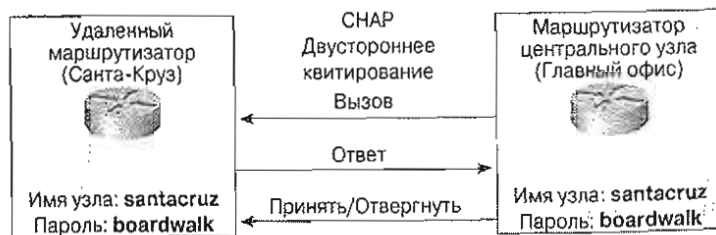


Рис. 13.10. Аутентификация по протоколу CHAP

Протокол CHAP обеспечивает защиту от атак повторного воспроизведения путем использования значения переменной вызова, которое уникально и непредсказуемо. Повторные вызовы применяются для уменьшения до минимума периода уязвимости при попытке несанкционированного входа в сеть. Локальные маршрутизаторы или серверы проверки аутентичности фиксируют частоту и время поступления вызовов.

Инкапсуляция протокола PPP и процесс аутентификации

При конфигурировании аутентификации протокола PPP можно выбрать протокол PAP или протокол CHAP. Тип аутентификации определяется с помощью команды `encapsulation ppp`. Если аутентификации не требуется, то протокол PPP начинает сеанс немедленно. В противном случае процесс переходит на следующую стадию. Процесс аутентификации проиллюстрирован на рис. 13.11.

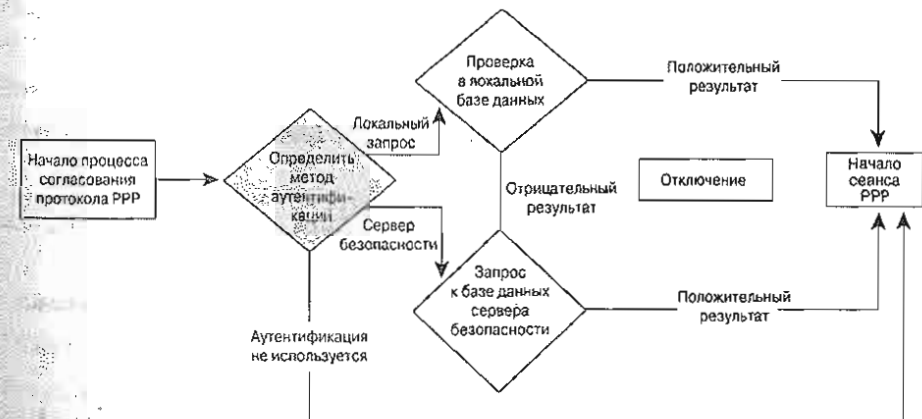


Рис. 13.11. Процесс аутентификации

При этом процесс определяет используемый метод аутентификации. Проверяются данные в локальной базе данных или на сервере безопасности с целью проверки, соответствуют ли полученные имя и пароль пользователя имеющимся данным.

После этого процесс проверяет ответ на запрос аутентификации полученный из локальной базы данных. Если ответ положителен, то начинается сеанс протокола PPP. Если ответ отрицателен, то пользователь немедленно получает отказ в доступе.

После того, как этап установки соединения PPP в протоколе PAP завершен, удаленный узел повторно посылает пару значений "имя пользователя-пароль" маршрутизатору до тех пор, пока аутентификация не будет подтверждена или не будет прекращено соединение.

В протоколе CHAP после этапа установки соединения PPP локальный маршрутизатор посылает сообщение-вызов удаленному узлу. Удаленный узел отвечает значением, вычисленным с помощью односторонней хэш-функции (обычно MD5). Локальный маршрутизатор сверяет этот ответ со своим собственным вычисленным хеш-значением. Если эти значения совпадают, то результат аутентификации считается положительным и подтверждается. В противном случае соединение немедленно прерывается.

Приведенные ниже описание этапов и рисунки иллюстрируют последовательность событий, которые происходят в процессе аутентификации по протоколу CHAP между двумя маршрутизаторами. Однако они не соответствуют реальным сообщениям, содержащимся в выводе по команде **debug ppp negotiation**. Дополнительная информация содержится в документе “Understanding debug ppp negotiation Output”, который можно просмотреть по адресу www.cisco.com/warp/public/471/debug_ppp_negotiation.html.

На рис. 13.12 показаны следующие этапы процесса аутентификации.

Этап 1. Вызов поступает на устройство 3640-1. Входной интерфейс сконфигурирован с помощью команды **ppp authentication chap**.

Этап 2. Протокол LCP согласовывает опции CHAP и MD5.

Этап 3. При этом вызове требуется вызов CHAP от 3640-1 к вызывающему маршрутизатору.

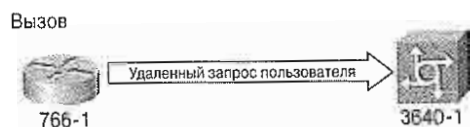


Рис. 13.12. Первый этап процесса аутентификации по протоколу CHAP

На рис. 13.13 проиллюстрированы следующие этапы процесса аутентификации CHAP между двумя маршрутизаторами:

Этап 1. Создается пакет протокола CHAP со следующими характеристиками:

- 01 = идентификатор типа пакета вызова
- id = порядковый номер вызова
- random = случайное число, генерируемое маршрутизатором
- 3640-1 = аутентификационное имя вызывающей стороны

Этап 2. Значения id и random хранятся на вызываемом маршрутизаторе

Этап 3. Пакет вызова посылается вызывающему маршрутизатору. Поддерживается список ожидающих вызовов.

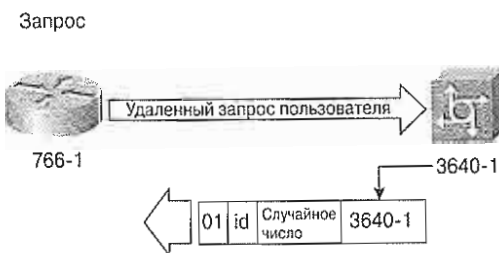


Рис. 13.13. Второй этап процесса аутентификации протокола CHAP

На рис. 13.14 проиллюстрирован прием пакета вызова от взаимодействующего устройства и его обработка алгоритмом MD5

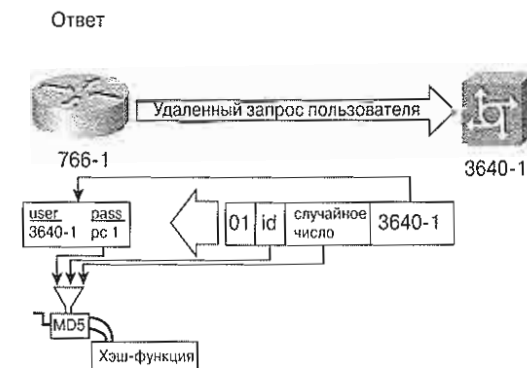


Рис. 13.14. Третий этап процесса аутентификации протокола CHAP

Маршрутизатор обрабатывает входящий пакет вызова протокола CHAP следующим образом.

Этап 1. Значение идентификатора id подается на хеш-генератор алгоритма MD5.

Этап 2. Выбранное случайным образом значение подается на хеш-генератор алгоритма MD5.

Этап 3. Имя 3640-1 используется для поиска пароля. При этом маршрутизатор ищет позицию, которая соответствует имени пользователя в пакете вызова. В данном примере он ищет следующую информацию:

`username 3640-1 password pc1`

Этап 4. Этот пароль подается на хеш-генератор алгоритма MD5.

Результатом является обработанный односторонней хэш-функцией алгоритма MD5 вызов протокола CHAP, который будет отправлен в ответе протокола CHAP.

На рис. 13.15 показан процесс создания ответного пакета протокола CHAP, отправляемого аутентификатору. На этом рисунке отображены следующие этапы.

Этап 1. Ответный пакет собирается из следующих компонентов:

- 02 = идентификатор типа ответного пакета протокола CHAP
- id = копируется из пакета вызова
- hash = выдаваемое хеш-генератором MD5 значение (обработанная хэш-функцией информация пакета вызова)
- 766-1 = Имя устройства для процесса идентификации. Оно требуется взаимодействующему устройству для поиска имени пользователя и его пароля, которые необходимы для проверки идентичности (она будет более подробно рассмотрена далее).

Этап 2. Пакет ответа посылается инициатору вызова.

Ответ (продолжение)

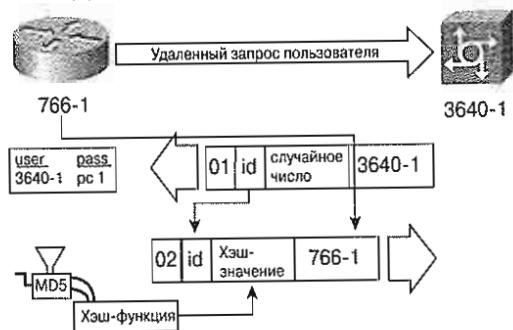


Рис. 13.15. 4-й этап процесса аутентификации протокола CHAP

На рис. 13.16 показано, каким образом инициатор вызова обрабатывает пакет ответа на свой запрос.

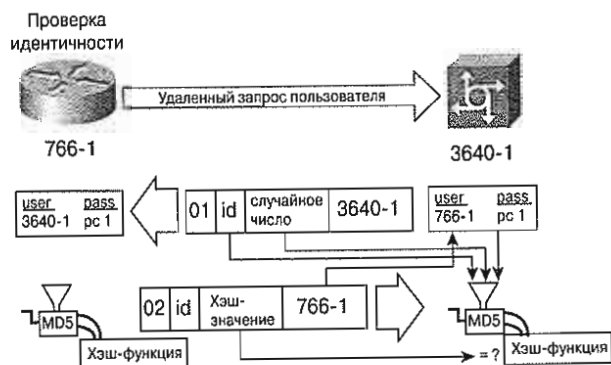


Рис. 13.16. 5-й этап процесса аутентификации протокола CHAP

Ответный пакет протокола CHAP обрабатывается (аутентификатором) следующим образом.

- Этап 1.** Идентификатор id используется для нахождения первоначального пакета вызова.
- Этап 2.** Идентификатор id подается на хеш-генератор алгоритма MD5.
- Этап 3.** Случайное значение первоначального вызова подается на хеш-генератор алгоритма MD5.
- Этап 4.** Имя 766-1 используется для поиска пароля в одном из следующих источников:

- Локальная база данных, содержащая имена пользователей и их пароли;
- Сервер службы удаленной аутентификации удаленного пользователя (Remote Authentication Dial-In User Service — RADIUS) или сервер управляющей системы терминального доступа (Controller Access Control System — TACACS+)

Этап 5. Пароль подается на хеш-генератор MD5.

Этап 6. Хеш-значение, полученное в ответном пакете, сравнивается с вычисленным хеш-значением алгоритма MD5. CHAP-аутентификация считается успешной, если вычисленное и полученное значения равны.

На рис. 13.17 проиллюстрировано сообщение об успешной аутентификации, посылаемое вызывающему маршрутизатору.

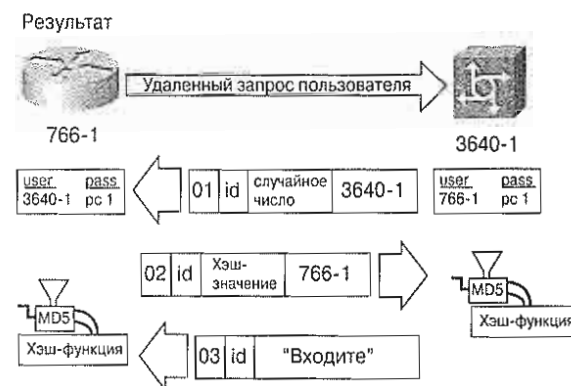


Рис. 13.17. Шестой этап процесса аутентификации протокола CHAP

Если аутентификация прошла успешно, то пакет протокола CHAP создается из следующих компонентов:

- 03 = тип сообщения об успешной аутентификации протокола CHAP.
- id = Копируется из ответного пакета.
- "Welcome in" — просто текстовое сообщение, содержащее понятное пользователю объяснение.

Если результат аутентификации отрицателен, то соответствующий пакет протокола CHAP создается из следующих компонентов:

- 04 = тип сообщения об отрицательном результате аутентификации протокола CHAP;
- id = Копируется из ответного пакета;

"Authentication failure" или другое текстовое сообщение, содержащее понятное пользователю объяснение. Пакет успешной аутентификации или отрицательный ответ направляется вызывающему маршрутизатору.

Последовательные каналы типа "точка-точка"

Почти все WAN-технологии основаны на последовательной передаче на физическом уровне. Это означает, что биты фрейма передаются в физическую среду по очереди.

и поддерживается оператором связи. Это позволяет телекоммуникационной компании активно управлять локальным ответвлением и устранять в нем неисправности. В этом случае точка демаркации находится после устройства NT1. Пользователь подсоединяет устройство CPE — обычно маршрутизатор или устройство доступа Frame Relay, к устройству NT1, как правило используя последовательный интерфейс, такой как V.35 or RS-232. Пример точки демаркации показан на рис. 13.20.



Рис. 13.20. Точка демаркации

Устройства DTE и DCE

У любого WAN-соединения на обоих его концах находятся некоторые устройства. На обоих концах соединения находятся устройство DTE и терминальное оборудование канала передачи данных (Data Communications Equipment — DCE), как показано на рис. 13.21. Соединение между двумя устройствами DCE осуществляет сеть передачи данных провайдера службы WAN. Устройство пользователя CPE, которое часть представляет собой маршрутизатор, является устройством DTE. Другими примерами устройств DTE могут служить терминал, компьютер, принтер или факс.

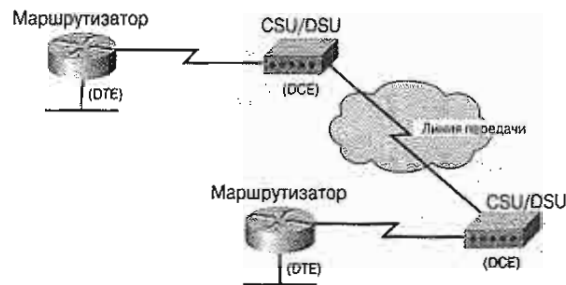


Рис. 13.21. Терминальное оборудование канала передачи данных

Устройство DCE, которое обычно является модемом или модулем обслуживания канала/модулем обработки данных, используется для преобразования данных пользователя от устройства DTE в форму, приемлемую для канала передачи провайдера службы WAN. Этот сигнал принимается на удаленном устройстве DCE, которое декодирует сигнал в последовательность битов, которые, в свою очередь, передаются удаленному устройству DTE. Оба устройства DCE должны быть сконфигурированы таким образом, чтобы они понимали друг друга. Иными словами, они должны использовать одну и ту же схему кодировки и скорость передачи данных. Для того, что-

бы устройства DTE могли осуществлять связь с устройствами DTE, были разработаны многочисленные стандарты.

Наиболее активное участие в разработке этих стандартов приняли такие организации, как Ассоциация электронной индустрии (Electronic Industries Association — EIA) и сектор стандартизации международного союза телекоммуникаций (International Telecommunication Union Telecommunication Standardization Sector — ITU-T). Примеры сетевых соединений CSU/DSU приведены на рис. 13.22.

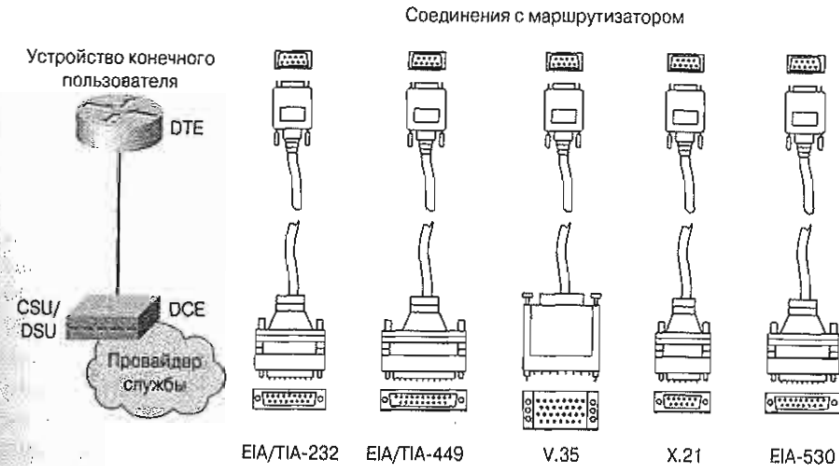


Рис. 13.22. Сетевые соединения CSU/DSU

Интерфейс DTE-DCE для конкретного стандарта определяет следующие спецификации.

- **Механические** — физические данные: количество контактов, тип штекера и т.д.
- **Электрические** — определяют уровни напряжения для сигналов 0/1.
- **Функциональные** — определяют выполняемые функции путем задания определенных значений линиям сигнализации интерфейса. Например, в EIA/TIA-232 и DB-25, линия 2 осуществляет передачу от устройства DTE к устройству DCE; линия 3 принимает на устройстве DTE данные от устройства DCE; линия 15 осуществляет синхронизацию передатчика.
- **Процедурные** — задают последовательность действий при передаче данных.

Предположим, что требуется соединить два устройства DTE, например, два компьютера или два маршрутизатора в лаборатории. Для того, чтобы устранить необходимость в устройствах DCE, требуется нуль-модемный кабель (который в действительности представляет собой два кабеля, преобразованных в один кабель). Для синхронных соединений, в которых необходим синхронизирующий сигнал, для его генерации используется внешнее устройство или одно устройств DTE. Обычно эта функция выполняется устройством DCE.

Синхронный последовательный порт маршрутизатора конфигурируется как устройство DTE или DCE. Если этот порт конфигурируется как устройство DTE, что является установкой по умолчанию, то требуется внешняя синхронизация от модуля CSU/DSU или другого устройства DCE.

Для соединения между собой устройств DTE и DCE используется экранированный последовательный переходный кабель. Со стороны маршрутизатора этот экранированный последовательный переходный кабель может заканчиваться штекером DB-60, который подсоединяется к порту DB-60 последовательной карты WAN-интерфейса. Другой конец кабеля заканчивается штекером, соответствующим используемому стандарту. Тип кабеля обычно задается провайдером WAN-сети или модулем CSU/DSU. Устройства Cisco поддерживают последовательные стандарты EIA/TIA-232, EIA/TIA-449, V.35, X.21 и EIA/TIA-530.

Для поддержки большей плотности портов с меньшими размерами корпорация Cisco ввела в употребление гладкий последовательный кабель. На последовательном конце гладкого последовательного кабеля находится 26-контактный штекер, который имеет значительно меньшие размеры по сравнению со штекером DB-60.

Инкапсуляция по протоколу HDLC

Первоначальные последовательные коммуникации были ориентированы на передачу символов (character-oriented). Такой способ связи более эффективен, однако первые протоколы были ориентированы на передачу битов (character-oriented). В 1979 году международная организация по стандартизации (International Organization for Standardization — ISO) утвердила высокоуровневый протокол управления на канальном уровне (High-Level Data Link Control — HDLC) в качестве стандартного бит-ориентированного протокола канального уровня для инкапсуляции данных в к синхронных последовательных каналах передачи данных. Такая стандартизация привела к тому, что и другие комитеты приняли и расширили этот протокол. С 1981 года союз ITU-T разработал ряд производных от HDLC протоколов, называемых протоколами канального доступа. Примерами таких протоколов являются протокол сбалансированной процедуры доступа к каналу (Link Access Procedure, Balanced — LAPB) для X.25, процедура доступа к каналу по D-каналу (Link Access Procedure on the D channel — LAPD) для ISDN, процедура доступа к каналу для модемов (Link Access Procedure for Modems — LAPM), протокол PPP для модемов и процедура доступа к каналу для протокола Frame Relay (Link Access Procedure for Frame Relay — LAPF).

В протоколе HDLC используется синхронная последовательная передача. Он обеспечивает свободную от ошибок связь между двумя точками на ненадежном физическом уровне. Протокол HDLC определяет структуру создания фреймов на 2-м уровне, которая позволяет осуществлять управление потоками и контроль ошибок с помощью механизмов подтверждений и схемы создания окон. Все фреймы имеют один и тот же формат, независимо от того, является ли фрейм фреймом данных или управляющим фреймом.

Стандартный протокол HDLC изначально не поддерживает несколько протоколов на одном канале, поскольку у него нет средств указать, данные какого протокола передаются по каналу. Корпорация Cisco предлагает фирменную версию протокола HDLC. Фрейм протокола HDLC Cisco имеет фирменное поле типа протокола, что делает возможным использование одного и того же последовательного канала несколькими сетевыми протоколами. Протокол HDLC принимается по умолчанию в качестве протокола 2-го уровня для последовательных интерфейсов маршрутизаторов Cisco.

Как показано на рис. 13.23, протокол HDLC определяет три типа фреймов, каждый из которых имеет отличный от других форматов управляющего поля.

- **Информационные фреймы (I-фреймы)** — передают данные, предназначенные станции-получателю. К информационному фрейму могут быть добавлены данные управления потоком и контроля ошибок.
- **Фреймы супервизора (S-фреймы)** — обеспечивают механизмы запроса/ответа на запрос в тех случаях когда не используется механизм дополнительных полей.
- **Ненумерованные фреймы (U-фреймы)** — обеспечивают выполнение дополнительных функций управления каналом, таких как установка соединения. Поле кода идентифицирует тип U-фрейма.

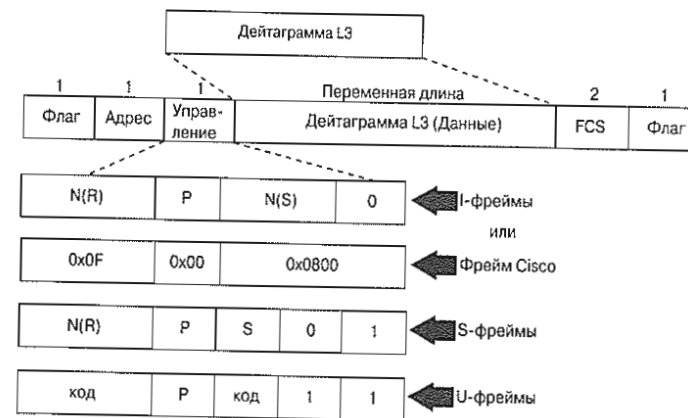


Рис. 13.23. Фреймы протокола HDLC

Первые один или два бита управляющего поля используются для задания типа фрейма. В управляющем поле информационного (I) фрейма номер в последовательности отправки (send-sequence number) указывает номер фрейма, который будет отправлен следующим. Номер в последовательности приема (receive-sequence number) указывает номер фрейма, который будет принят следующим. Номера фреймов, являющихся следующими при отправке и приеме поддерживаются как отправителем, так и получателем.

Конфигурирование инкапсуляции протокола HDLC

По умолчанию устройства Cisco в качестве метода последовательной инкапсуляции используют фирменный протокол HDLC корпорации Cisco. Однако если последовательный интерфейс сконфигурирован для другого протокола инкапсуляции и требуется вернуть инкапсуляцию HDLC, то необходимо войти в режим конфигурирования на последовательном интерфейсе. Затем следует ввести команду конфигурирования интерфейса `encapsulation hdlc` для задания на интерфейсе инкапсуляции HDLC.

```
Router(config-if)#encapsulation hdlc
```

Фирменный протокол HDLC Cisco является протоколом типа “точка-точка”, который может быть использован на выделенных линиях между двумя устройствами Cisco. При установке связи с устройством, отличным от устройств Cisco, более подходящим решением является синхронный протокол PPP.

Устранение ошибок и неисправностей на серийном интерфейсе

Вывод по команде **show interfaces serial** отображает информацию относящуюся к конкретным интерфейсам. Эту команду **show interface serial** следует использовать для проверки правильности конфигурирования инкапсуляции протоколов HDLC или PPP. При конфигурировании протокола HDLC в выводе по команде **show interface serial** должна присутствовать строка "Encapsulation HDLC".

При конфигурировании протокола PPP можно проверить состояние LCP and NCP с помощью команды **show interface serial**, как показано в примере 13.1. В первом примере показана инкапсуляция протокола HDLC, а во втором — инкапсуляция протокола PPP.

Пример 13.1 Вывод по команде show interface s0/0

```
Router#show interface s0/0
Serial 0 is up, line protocol is up
Hardware is MCI Serial
Internet address is 131.108.156.98, subnet mask is 255.255.255.240
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters never
--- пропущено ---
```

```
Router#show interface s0/0
Serial0 is up, line protocol is up
Hardware is HD64570
Internet address is 10.140.1.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load
1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input 00:00:05, output 00:00:05, output hang never
Last clearing of "show interface" counters never
--- пропущено ---
```

В табл. 13.3 приведены состояния, соответствующие возможным проблемам, о которых можно узнать в строке состояния интерфейса при отображении вывода по команде **show interfaces serial**.

```
Serial x is down, line protocol is down
Serial x is up, line protocol is down
Serial x is up, line protocol is up (looped)
Serial x is up, line protocol is down (disabled)
Serial x is administratively down, line protocol is down
```

Таблица 13.3. Возможные проблемные состояния

Строка состояния	Возможное состояние	Способ решения проблемы
Последовательный канал x активен, протокол канала активен	Это нормальное состояние строки состояния канала.	Никаких действий не требуется.
Последовательный канал x неактивен, протокол канала отключен (режим DTE)	Маршрутизатор не воспринимает CD-сигнал (т.е. CD неактивен). Возникли проблемы у телефонной компании; канал отключен или не подсоединен к CSU/DSU. Обрыв в кабеле или кабель не соответствует требованиям соединения. Сбой в аппаратном обеспечении (CSU/DSU).	<ol style="list-style-type: none"> 1. Проверить показания индикаторов на устройствах CSU/DSU и проверить что CD активен, или вставить детектор обрывов в канал для проверки CD-сигнала. 2. Проверить, что используется соответствующий кабель и интерфейс. (Следует прочитать документацию по установке устройств) 3. Вставить детектор обрывов и проверить все управляющие индикаторы. 4. Связаться с оператором, предоставляющим выделенную линию или иную службу и выяснить, не возникли ли у него проблемы. 5. Заменить вышедшие из строя детали. 6. Если есть основания предполагать, что неисправен маршрутизатор, то следует переключить последовательный канал на другой порт. Если после этого соединение начинает функционировать, то на ранее использовавшемся интерфейсе имеется повреждение.

Продолжение табл. 13.3

Строка состояния	Возможное состояние	Способ решения проблемы
Последовательный канал x активен, протокол канала отключен (режим DTE)	Конфигурация локального или удаленного маршрутизатора содержит ошибки. Удаленный маршрутизатор не посылает сообщений об активности. Возникла проблема в выделенной линии. Возникла проблема в выделенной линии или другая проблема у оператора связи (шумы в линии, неправильное конфигурирование или вышел из строя коммутатор). В кабеле возникла проблема синхронизации (на модуле CSU/DSU не установлен SCTE). Вышел из строя локальный или удаленный модуль CSU/DSU. Вышло из строя аппаратное обеспечение маршрутизатора (локального или удаленного).	<ol style="list-style-type: none"> 1. Перевести модем, CSU или DSU в режим локального петлевого интерфейса и использовать команду show interfaces serial для выяснения, работает ли протокол канала. Если протокол работает, то проблема, вероятно, связана с телефонной компанией или вышедшим из строя удаленным маршрутизатором. 2. Если создается впечатление, что проблема возникла на удаленном конце, то следует повторить этап 1 на удаленном модеме, CSU, или DSU. 3. Проверить все кабели. Убедиться в том, что кабель подключен к нужному интерфейсу, правильному CSU/DSU и к нужной терминирующей точке сети телефонной компании. Использовать команду EXEC-режима show controllers для определения того, какой кабель подключен к какому интерфейсу. 4. Выполнить команду EXEC-режима debug serial interface. 5. Если протокол канала не начинает работать в режиме локального петлевого интерфейса, а вывод по команде EXEC-режима debug serial interface показывает, что значения счетчика сообщений об активности не увеличиваются, то, вероятно, имеется проблема с аппаратной частью маршрутизатора. Следует поменять местами аппаратное обеспечение интерфейса маршрутизатора. 6. Если протокол канала начинает работать и значения счетчика сообщений об активности увеличиваются, то проблема не связана с локальным маршрутизатором. 7. Если есть основания предполагать, что вышло из строя аппаратная часть маршрутизатора, то следует сменить последовательный канал и переместить его на неиспользуемый порт. Если соединение начинает работать, то проблема связана с ранее подсоединенным интерфейсом.

Продолжение табл. 13.3

Строка состояния	Возможное состояние	Способ решения проблемы
Последовательный канал x включен, протокол канала отключен (режим DCE)	Отсутствует команда конфигурирования интерфейса clockrate . Устройство DTE не поддерживает режим SCTE или не задано использование этого режима (терминальная сигнализация). Вышел из строя удаленный модуль CSU или DSU.	<ol style="list-style-type: none"> 1. Добавить на последовательном интерфейсе команду конфигурирования интерфейса clock rate bps где bps — желаемая скорость в битах в секунду: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000 или 8000000 2. Если возможно, установить устройство DTE на внешний последовательный модем (serial clock transmit external — SCTE). Если модуль CSU/DSU не поддерживает SCTE, то, возможно, придется отключить SCTE на интерфейсе маршрутизатора Cisco 3. Проверить, что используется правильный кабель 4. Если протокол канала по-прежнему не функционирует, то, вероятно, имеется повреждение в аппаратном обеспечении или проблема с кабелями. 5. При необходимости заменить дефектные детали.
Последовательный канал x включен, протокол канала выключен (образует петлю)	В канале имеется петля. Последовательный номер в пакете сообщения об активности при первоначальном обнаружении петли сменяется случайным числом. Если по каналу возвращается одно и то же случайное число, то это свидетельствует о существовании петли.	<ol style="list-style-type: none"> 1. Следует использовать команду show running-config привилегированного EXEC-режима для поиска записи с командой конфигурирования интерфейса loopback 2. Если найдена запись с командой конфигурирования интерфейса loopback, то для удаления петли следует использовать команду конфигурирования интерфейса no loopback. 3. Если запись с командой конфигурирования интерфейса loopback не найдена, то следует исследовать модули CSU/DSU для выяснения, были ли они сконфигурированы вручную в режиме петли. Если это так, то следует отключить ручную петлю. 4. Переустановить CSU или DSU и выяснить состояние канала. Если протокол канала работает, то других действий не требуется. 5. Если CSU и DSU не были сконфигурированы в режиме ручной петли, то следует связаться с владельцем арендованной линии или другим оператором связи с просьбой оказать помощь в поиске неисправности в канале.

Строка состояния	Возможное состояние	Способ решения проблемы
Последовательный канал x работает, протокол канала не функционирует (отключен).	В канале имеется высокий уровень ошибок в связи с проблемами службы телефонной компании. Есть проблемы в аппаратной части модулей CSU или DSU. Аппаратная часть маршрутизатора (интерфейс) неисправна.	<ol style="list-style-type: none"> 1. Проверить канал с помощью последовательного анализатора и детектора обрывов. Выполнить поиск переключения между сигналами Clear to Send и Data set ready (Data set ready — DSR) 2. Создать петлевое соединение CSU/DSU (петля DTE). Если проблема не решается, то она, вероятно, связана с аппаратным обеспечением. Если проблема исчезает, то, она, по-видимому, связана с телефонной компанией. 3. Заменить дефектное аппаратное обеспечение (CSU, DSU, коммутатор, локальный или удаленный маршрутизатор).
Последовательный канал x отключен администратором, протокол канала не функционирует	В конфигурации маршрутизатора имеется команда конфигурирования интерфейса shutdown . Имеется дублирование IP-адреса.	<p>Проверить, не содержит ли конфигурация маршрутизатора команду shutdown.</p> <p>Использовать команду конфигурирования интерфейса no shutdown для удаления команды shutdown. Проверить, нет ли одинаковых IP-адресов, использующих команду привилегированного EXEC-режима show runningconfig или команду show interfaces EXEC-режима.</p> <p>Если имеются дублированные адреса, то следует разрешить конфликт адресов, изменив один из них.</p>

Пример 13.2 Вывод по команде show controllers

```
Router#show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
idb at 0x81414E2C, driver data structure at 0x8141753C
SCC Registers:
General [GSMR]=0x2:0x00000030, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x06
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
```

Вывод по команде **show controllers** отображает состояние каналов интерфейса и показывает, подсоединен ли кабель к интерфейсу. Следует обратить внимание на то, что к последовательному интерфейсу 0/0 подсоединяется кабель V.35 DTE.

Если электрический интерфейс отображается как UNKNOWN (неизвестный), а не V.35, EIA/TIA-449 или какой-либо другой тип электрического интерфейса, то вероятной причиной возникшей проблемы является неправильно подсоединенный кабель. Возможно также, то причиной является неправильное подсоединение к сетевому адаптеру внутренних проводов. Если тип электрического интерфейса неизвестен, то соответствующий вывод по команде EXEC-режима **show interfaces** показывает, что интерфейс и протокол канала не функционируют.

Ниже приведены несколько команд **debug**, полезных для решения проблем в последовательных каналах и распределенных сетях WAN.

- **debug serial interface** — проверяет, увеличивается ли количество пакетов сообщений об активности протокола HDLC. Если оно не увеличивается, то, возможно, существует проблема синхронизации на карте сетевого интерфейса или в сети. В примере 13.3 показан отладочный вывод сети.
- **debug arp** — показывает, отправляет ли и получает ли маршрутизатор (с помощью пакетов ARP) информацию о маршрутизаторах на другой стороне среды распределенной сети WAN. Эту команду следует использовать в тех случаях, когда некоторые узлы сети протокола TCP/IP отвечают, а другие не отвечают на посылаемые им запросы.
- **debug frame-relay lmi** — с помощью этой команды можно получить информацию об интерфейсе локального управления (Local Management Interface — LMI), для выяснения того, коммутатор Frame Relay и маршрутизатор посылают и получают пакеты интерфейса LMI.
- **debug frame-relay events** — определяет, происходит ли обмен между маршрутизатором и коммутатором Frame Relay.
- **debug ppp negotiation** — отображает пакеты PPP, передаваемые при запуске протокола PPP, когда обсуждаются опции протокола PPP.
- **debug ppp packet** — отображает посылаемые и получаемые пакеты PPP. Эта команда отображает дампы пакетов нижнего уровня.
- **debug ppp errors** — отображает ошибки протокола PPP (такие как нелегитимные или неправильно отформатированные фреймы), связанные с обсуждением соединений PPP и его функционированием.
- **debug ppp chap** — отображает обмен пакетами протоколов PAP и CHAP.

ПРИМЕЧАНИЕ

Поскольку выводу данных отладки в процессе работы процессора назначается высокий приоритет, он может сделать систему неработоспособной. Поэтому команды отладки следует использовать только для решения конкретных проблем или во время сеансов поиска и устранения ошибок техническим персоналом корпорации Cisco. Более того, команды отладки лучше выполнять в периоды небольшой нагрузки в сети и небольшого количества пользователей в ней. Отладка в такие периоды уменьшает вероятность того, что возросшие затраты ресурсов на отладку неблагоприятно повлияют на производительность сети.

Пример 13.3 Команда debug serial interface

```
Router#debug serial interface
```

```
Serial network interface debugging is on
Router#
```

```
00:06:47: Serial0/0: HDLC myseq 29, mineseen 29*, yourseen 29, line up
00:06:57: Serial0/0: HDLC myseq 30, mineseen 30*, yourseen 30, line up
00:07:07: Serial0/0: HDLC myseq 31, mineseen 31*, yourseen 31, line up
00:07:17: Serial0/0: HDLC myseq 32, mineseen 32*, yourseen 32, line up
```



```
Router#undebug all
All possible debugging has been turned off
Router#
```



Лабораторная работа: устранение ошибок на последовательном интерфейсе

В этой лабораторной работе требуется сконфигурировать последовательные интерфейсы на последовательных интерфейсах двух маршрутизаторов. После этого следует с помощью команд **show** решить проблемы, возникшие в соединениях.

Конфигурирование протокола PPP

Различные аспекты конфигурирования протокола PPP включают в себя методы аутентификации, сжатия и обнаружения ошибок, а также решение вопроса о поддержке многоканальности. В настоящей главе описаны различные варианты конфигурирования протокола PPP.

Маршрутизаторы Cisco, использующие инкапсуляцию PPP, имеют опции LCP-конфигурации, приведенные в табл. 13.4.

Таблица 13.4. Опции конфигурирования протокола LCP

Опция	Выполняемая функция	Протокол	Команда
Аутентификация	Опция использования аутентификации требует, чтобы вызывающая сторона канала ввела информацию, которая позволит удостовериться в том, что она имеет разрешение системного администратора на осуществление вызова. Сообщениями аутентификации обмениваются взаимодействующие маршрутизаторы. Двумя возможными альтернативами являются протоколы PAP и CHAP	PAP CHAP	<code>ppp authentication pap</code> <code>ppp authentication chap</code>
Сжатие	Опции сжатия увеличивают эффективную пропускную способность соединений протокола PPP за счет уменьшения количества данных в первоначальном фрейме, который должен быть передан по каналу. В пункте назначения протокол выполняет декомпрессию этого фрейма. На маршрутизаторах Cisco доступны два протокола сжатия: Stacker and Predictor.	Stacker или Predictor	<code>ppp compress stacker</code> <code>ppp compress predictor</code>
Обнаружение ошибок	Механизмы обнаружения ошибок протокола PPP запускают процесс для идентификации условий возникновения ошибок. Опции Quality и Magic Number помогают обеспечить надежный, свободный от петель канал.	Quality, Magic Number	<code>ppp quality number_1-100</code>

Окончание табл. 13.4

Опция	Выполняемая функция	Протокол	Команда
Много-канальность	Программное обеспечение IOS Cisco версии 11.1 и более поздние поддерживают многоканальный протокол PPP (PPP Multilink Protocol — MP). Эту функцию иногда называют многоканальным PPP. Эта альтернатива обеспечивает балансирование нагрузки на интерфейсах маршрутизатора, используемых протоколом PPP. Протокол MP обеспечивает фрагментацию пакетов и их упорядочивание, которые расщепляют нагрузку для протокола PPP и отправляют фрагменты по параллельным каналам. В некоторых случаях такая “связка” каналов функционирует как один логический канал, улучшая пропускную способность и уменьшая задержку при прохождении между взаимодействующими маршрутизаторами.	MP	<code>ppp multilink</code>

Конфигурирование инкапсуляции протокола PPP

Приведенные ниже команды задают инкапсуляцию протокола PPP на последовательном интерфейсе 0.

```
Router# config terminal
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
```

На последовательном интерфейсе, использующем инкапсуляцию PPP может быть сконфигурировано программное сжатие данных. Сжатие осуществляется программным обеспечением и может серьезно повлиять на производительность системы. Если большая часть передаваемых данных представляет собой уже сжатые файлы, то использовать сжатие не рекомендуется.

Для того, чтобы сконфигурировать сжатие PPP необходимо выполнить в режиме конфигурирования интерфейса приведенные ниже команды.

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
Router(config-if)# compress [predictor | stac]
```

Для того, чтобы осуществлять мониторинг данных, потерянных в канале, и не допустить перемещения фреймов по петлевому маршруту, следует выполнить следующие команды:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp quality number_1-100
```

Приведенные ниже команды осуществляют балансирование нагрузки между несколькими каналами:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
Router(config-if)# ppp multilink
```



Лабораторная работа: конфигурирование инкапсуляции протокола PPP

В этой лабораторной работе требуется сконфигурировать инкапсуляцию PPP на последовательных интерфейсах двух маршрутизаторов, а затем протестировать канал.

Конфигурирование аутентификации протокола PPP

Приведенные в табл. 13.5 процедуры описывают конфигурирование инкапсуляции протокола PPP и аутентификацию протоколов PAP/CHAP.

Таблица 13.5. Конфигурирование протоколов PAP/CHAP

Этап	Действие	Результаты и примечания
1.	В режиме глобального конфигурирования задать имя узла с помощью команды hostname name : Router(config)#hostname SantaCruz	Это имя должно соответствовать имени пользователя, которое ожидает маршрутизатор, находящийся на другом конце канала. Примечание: команда hostname чувствительна к регистру.
2.	В режиме глобального конфигурирования задать имя пользователя и пароль, ожидаемые от удаленного маршрутизатора с помощью команды username name password password : Router(config)#username HQ password cisco. На маршрутизаторах Cisco пароль на обоих маршрутизаторах должен быть одним и тем же. В версиях, предшествовавших версии 11.2, это пароль был зашифрованным и секретным. Для зашифровки паролей на маршрутизаторах Cisco используется команда service password-encryption , которая вводится в режиме глобального конфигурирования.	
3.	В режиме конфигурирования интерфейса включить инкапсуляцию PPP на соответствующем интерфейсе с помощью команды encapsulation ppp : Router(config-if)#encapsulation ppp	Для включения PPP на асинхронном последовательном интерфейсе требуется дополнительное конфигурирование.
4.	В режиме конфигурирования интерфейса включить задать аутентификацию протокола PPP с помощью команды ppp authentication {chap chap pap pap chap pap} Router(config-if)#ppp authentication chap	Если задано использование обоих методов, то при обсуждении параметров канала запрос будет сделан относительно первого из указанных методов. Если партнер по связи предлагает использовать второй метод или просто отказывается использовать первый, то делается попытка использовать второй метод.
5.	Проверить правильность конфигурации с помощью команды show interface : Router#show interface s0	После того, как протокол PPP сконфигурирован, с помощью этой команды можно проверить состояние протоколов LCP и NCP.

Правильность конфигурации весьма существенна, поскольку протоколы PAP и CHAP используют эти параметры для аутентификации.

На рис. 13.24 приведен пример конфигурирования двусторонней PAP-аутентификации. Оба маршрутизатора проходят аутентификацию и сами ее осуществляют, поэтому команды PAP-аутентификации являются зеркальным отражением друг друга. Имя пользователя и его пароль в протоколе PAP, посылаемые каждым маршрутизатором, должны соответствовать тем, которые указаны в командах **username name password password** другого маршрутизатора.

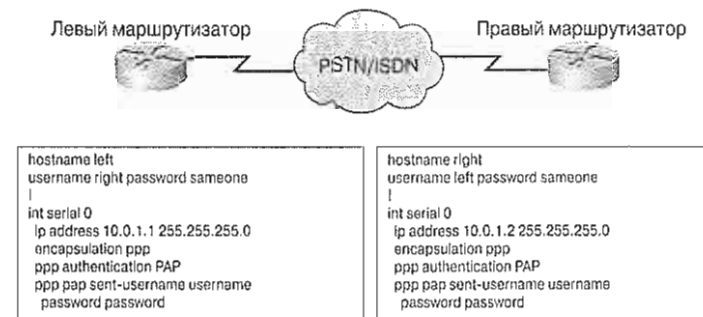


Рис. 13.24. Конфигурирование протокола PPP

На рис. 13.25 показана двусторонняя аутентификация протокола CHAP. Имя узла на одном маршрутизаторе должно соответствовать имени пользователя, сконфигурированному на другом маршрутизаторе. Пароли также должны соответствовать друг другу.

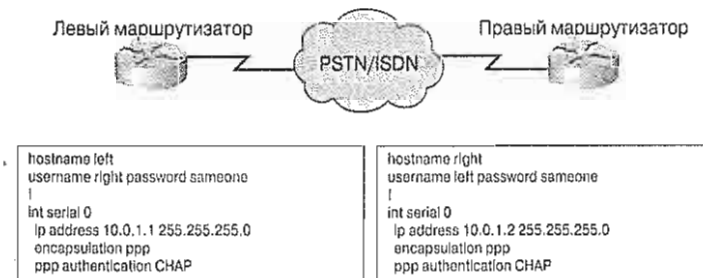



Рис. 13.25. Конфигурирование протокола CHAP

Для упрощения задач конфигурирования протокола CHAP могут быть использованы описанные ниже методы.

- На нескольких маршрутизаторах можно использовать одно и то же имя узла — если желательно, чтобы у удаленных пользователей создавалось впечатление, что при аутентификации они подсоединяются к одному и тому же маршрутизатору, то следует сконфигурировать одно и то же имя узла на каждом маршрутизаторе.
Router(config-if)# **ppp chap hostname hostname**
- Для аутентификации неизвестного узла можно использовать пароль — эта операция используется для ограничения количества записей “имя пользователя/пароль” на маршрутизаторе. Для ее выполнения следует сконфигурировать пароль, который будет посылаться узлам, которые хотят аутентифицировать этот маршрутизатор:
Router(config-if)# **ppp chap password secret**



Лабораторная работа: конфигурирование аутентификации протокола CHAP
В этой лабораторной работе требуется сконфигурировать аутентификацию PPP путем использования протокола CHAP на двух маршрутизаторах

Тестирование конфигурации инкапсуляции PPP в последовательном канале

Как показано в примере 13.4, команда **show interface** используется для тестирования правильности конфигурирования инкапсуляции протоколов HDLC или PPP. Если сконфигурирован протокол HDLC, то в выводе по команде **show interface** должна присутствовать строка “Encapsulation HDLC”. Если сконфигурирован протокол PPP, то эту команду можно использовать для проверки состояний LCP и NCP.


Пример 13.4. Тестирование конфигурации инкапсуляции PPP в последовательном канале

```
Router# show interface s0
Serial0 is up, line protocol is up
Hardware is HD64570
Internet address is 10.140.1.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input 00:00:05, output 00:00:05, output hang never
Last clearing of "show interface" counters never
--- output omitted ---
```

В табл. 13.6 перечислены команды, которые используются для включения, конфигурирования и тестирования протокола PPP.

Таблица 13.6. Команды протокола PPP

Команда	Описание
<code>encapsulation ppp</code>	Включает на интерфейсе протокол PPP
<code>ppp authentication pap</code>	Включает на интерфейсе аутентификацию протокола PAP
<code>ppp authentication chap</code>	Включает на интерфейсе аутентификацию протокола CHAP
<code>username username password password</code>	Устанавливает систему аутентификации, основанную на имени пользователя
<code>show interfaces</code>	Отображает статистику для всех интерфейсов, сконфигурированных на маршрутизаторе или сервере доступа
<code>debug ppp authentication</code>	Включает режим отладки для процессов аутентификации протоколов PAP или CHAP
<code>undebug all</code>	Выключает режим отладки и вывод на экран соответствующей информации



Лабораторная работа: Тестирование конфигурации протокола PPP
В этой лабораторной работе требуется сконфигурировать протокол PPP на последовательных интерфейсах двух маршрутизаторов, а затем протестировать канал.

Устранение ошибок конфигурирования инкапсуляции PPP в последовательном канале

Команда **debug ppp authentication** отображает последовательность сообщений, которыми обмениваются маршрутизаторы при аутентификации. В примере 13.5 приведен вывод на левом маршрутизаторе при CHAP-аутентификации, выполняемой правым маршрутизатором при вводе команды **debug ppp authentication**. Если сконфигурирована двусторонняя аутентификация, то каждый маршрутизатор выполняет аутентификацию другого и сообщения появляются как для маршрутизатора, который выполняет аутентификацию, так и для маршрутизатора в отношении которого она выполняется. Протокол CHAP определен как односторонний метод аутентификации. Однако при его использовании в обоих направлениях получается двусторонняя аутентификация. Поэтому при двусторонней CHAP-аутентификации каждая сторона инициирует отдельное трехстороннее квитирование. Эта команда может быть использована для отображения последовательности обмена сообщениями, которая реально происходит.

Пример 13.5. Устранение ошибок в последовательном канале протокола PPP

```
*4d20h: %LINK-3-UPDOWN: Interface Serial0, changed state to up
*4d20h: Se0 PPP: Treating connection as a dedicated line
*4d20h: Se0 PPP: Phase is AUTHENTICATING, by both
*4d20h: Se0 CHAP: O CHALLENGE id 2 len 28 from "left"
*4d20h: Se0 CHAP: I CHALLENGE id 3 len 28 from "right"
*4d20h: Se0 CHAP: O RESPONSE id 3 len 28 from "left"
*4d20h: Se0 CHAP: I RESPONSE id 2 len 28 from "right"
*4d20h: Se0 CHAP: O SUCCESS id 2 len 4
*4d20h: Se0 CHAP: I SUCCESS id 3 len 4
*4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0,
changed state to up
```

В табл. 13.7 приведен вывод на левом маршрутизаторе для двусторонней PAP-аутентификации.

Таблица 13.7. Аутентификация протокола PAP

Вывод	Описание
<code>Se0 PPP: Phase is AUTHENTICATING, by both</code>	Двусторонняя аутентификация
<code>Se0 PAP: O AUTH-REQ id 4 len 18 from "left"</code>	Исходящий запрос аутентификации
<code>Se0 PAP: I AUTH-REQ id 1 len 18 from "right"</code>	Исходящий запрос аутентификации
<code>Se0 PAP: Authenticating peer right</code>	Входная аутентификация
<code>Se0 PAP: O AUTH-ACK id 1 len 5</code>	Исходящее подтверждение
<code>Se0 PAP: I AUTH-ACK id 4 len 5</code>	Входящее подтверждение

Команда **debug ppp** используется для отображения информации о функционировании протокола PPP. Форма этой команды с ключевым словом **no** отключает отладочный вывод. В табл. 13.8 приведены различные опции, которые могут быть использованы для расширения возможностей команды **debug ppp**.

```
debug ppp {packet | negotiation | error | chap}
no debug ppp {packet | negotiation | error | chap}
```

Таблица 13.8. Опции команды **debug ppp**

Опция команды	Определение
packet	Используется вместе с командой debug ppp для отображения получаемых и отправляемых пакетов протокола PPP
negotiation	Используется вместе с командой debug ppp для отображения пакетов протокола PPP, передаваемых при запуске протокола PPP, когда обсуждаются опции этого протокола
error	Используется вместе с командой debug ppp для отображения ошибок протокола и статистики ошибок, связанных с обсуждением и функционированием соединения протокола PPP
chap	Используется вместе с командой debug ppp для отображения обмена пакетами протоколов CHAP и PAP



Лабораторная работа: Устранение ошибок в конфигурации протокола PPP

В этой лабораторной работе требуется сконфигурировать протокол PPP на двух маршрутизаторах, а затем использовать команды **show** и **debug** для решения возникающих в соединениях проблем.

Резюме

В этой главе были рассмотрены следующие основные положения:

- протокол PPP является наиболее широко используемым протоколом распределенных сетей WAN;
- протокол PPP решает проблемы Internet-соединений предоставляя LCP и семейство NCP для обсуждения необязательных параметров конфигурации и других возможностей;
- сеанс протокол PPP состоит из четырех этапов:
 - установка канала;
 - определение качества канала;
 - обсуждение конфигурации протокола сетевого уровня;
 - ликвидация канала.
- при конфигурировании PPP-аутентификации можно выбрать протокол PAP или протокол CHAP;
- протокол PAP не является строгим протоколом аутентификации;
- протокол CHAP обеспечивает защиту от атаки воспроизведения путем использования переменного вызываемого значения, которое является уникальным и непредсказуемым;

- сконфигурировать на интерфейсе инкапсуляцию PPP можно с помощью команды **encapsulation ppp**;
- после того, как протокол PPP сконфигурирован, состояния LCP и NCP можно проверить с помощью команды **show interfaces**.

В дополнение к изложенному в настоящей главе материалу рекомендуется изучить относящиеся к ней видеоклипы, фотографии и выполнить лабораторные работы, находящиеся на компакт-диске CD-ROM, прилагаемом к книге.

Глоссарий

Протокол логического канала (logical link protocol — LLC). Верхний из двух подуровней канального уровня, определенных IEEE. Подуровень LLC выполняет контроль ошибок, управление потоком, создание фреймов и адресацию MAC-подуровня. Наиболее часто используется LLC-протокол IEEE 802.2, который существует в двух вариантах: с установлением соединения и без него.

Протокол аутентификации паролем (Password Authentication Protocol — PAP). Протокол проверки подлинности, который позволяет устройствам одного ранга распознать друг друга. От удаленного маршрутизатора, который пытается подсоединиться к локальному маршрутизатору, требуется, чтобы он послал запрос на проверку подлинности. В отличие от CHAP, PAP передает пароль, имя узла или имя пользователя в виде открытого текста (т.е. незашифрованным). Сам по себе PAP не предотвращает несанкционированный доступ, но идентифицирует пункт назначения; после этого маршрутизатор или сервер доступа определяет, разрешен ли доступ данному пользователю. PAP поддерживается только на линиях PPP.

Протокол аутентификации с предварительным согласованием вызова (Challenge Handshake Authentication Protocol — CHAP). Средство обеспечения безопасности, которое предотвращает несанкционированный доступ за счет использования инкапсуляции PPP. Сам по себе CHAP не предотвращает несанкционированный доступ, но идентифицирует удаленный пункт назначения; после этого маршрутизатор или сервер доступа определяет, разрешен ли доступ данному пользователю.

Протокол типа “точка-точка” (Point-to-point Protocol — PPP). Разработанный как замена протокола SLIP, протокол PPP обеспечивает соединение между маршрутизаторами и соединение узла с сетью по синхронным и асинхронным каналам.

Протокол управления каналом (Link Control Protocol — LCP). Протокол, обеспечивающий средства установки, поддержки и окончания соединения типа “точка-точка”.

Протокол управления сетью (Network Control Protocol — NCP). Протокол, осуществляющий маршрутизацию и управление потоком данных между коммуникационным контроллером и другими сетевыми ресурсами.

Контрольные вопросы

1. Что из перечисленного ниже является первым этапом установки соединения по каналу PPP?
 - A. Иницирующий соединение узел PPP посылает сообщение о начале сеанса ближайшему соседнему устройству PPP.

- В. Маршрутизаторы, находящиеся на маршруте перед активизацией канала PPP обсуждают средства аутентификации
 - С. Узлы протокола PPP запрашивают динамическое выделение адресов или запрашивают назначение адресов у серверов
 - Д. Иницирующий соединение узел посылает фреймы протокола LCP для того, чтобы сконфигурировать канал передачи данных
2. При использовании протокола PPP, что происходит если протокол LCP закрывает канал?
- А. Узел-получатель пытается установить новый канал
 - В. Протокол NCP посылает фрейм поддержки канала.
 - С. Иницирующий узел вновь устанавливает сеансы соединений.
 - Д. Протокол LCP информирует протоколы сетевого уровня.
3. Какой из перечисленных ниже протоколов сетевого уровня поддерживается протоколом PPP?
- А. Novell IPX
 - В. IP
 - С. AppleTalk
 - Д. Все вышеперечисленные
4. Для чего из перечисленного ниже протокол PPP использует протоколы NCP?
- А. Для установки каналов
 - В. Для инкапсуляции данных нескольких протоколов
 - С. Для преобразования пакетов в ячейки
 - Д. Для установки соединения
5. Какое из полей фрейма PPP указывает, данные какого протокола были инкапсулированы — протокола IPX или протокола IP?
- А. Поле флага
 - В. Поле управления
 - С. Поле протокола
 - Д. Поле контрольной суммы FCS
6. В каком из перечисленных ниже случаев наиболее вероятно использование протокола PPP в качестве локальной рабочей станции для выхода в Internet?
- А. Когда рабочая станция непосредственно подсоединена к локальной сети LAN.
 - В. Когда рабочая станция непосредственно подсоединена к маршрутизатору.
 - С. Когда рабочей станции требуется удаленный доступ к сети Internet.
 - Д. Протокол PPP никогда не используется на рабочих станциях.
7. За что из перечисленного ниже отвечает протокол LCP при работе с протоколом PPP?
- А. За установку, поддержку и закрытие соединений типа “точка-точка”
 - В. За поддержку нескольких каналов
 - С. За рассылку обновлений маршрутов
 - Д. За сжатие данных

8. Сколько этапов включает в себя установка сеанса PPP?
- А. Два
 - В. Три
 - С. Четыре
 - Д. Один
9. Какой тип квитирования используется если в качестве протокола аутентификации PPP выбран протокол PAP?
- А. Одностороннее
 - В. Двустороннее
 - С. Трехстороннее
 - Д. Четырехстороннее
10. Какая команда на маршрутизаторе может быть использована на маршрутизаторе для проверки состояния протоколов LCP и NCP для протокола PPP?
- А. `router> show interfaces`
 - В. `router(config)# show interfaces`
 - С. `router# show interfaces`
 - Д. `router(config-if)# show interfaces`
11. Какой протокол следует использовать для установки удаленного соединения по каналу ISDN?
- А. PPP
 - В. SLIP
 - С. PAP
 - Д. CHAP
12. Какая функция используется протоколом PPP для распределения нагрузки по нескольким каналам?
- А. Протокол PAP
 - В. Протокол Stacker
 - С. Сжатие данных
 - Д. Многоканальность
13. Что должен делать протокол LCP после открытия соединения при установке канала PPP?
- А. Согласовать параметры конфигурации, а затем послать и получить фрейм подтверждения выбранной конфигурации.
 - В. Протестировать канал и определить достаточно ли его качество для включения протоколов сетевого уровня.
 - С. Опросить узлы протокола PPP и выяснить существует ли уже маршрут к серверу протокола управления сетью (Network Control Protocol).
 - Д. Запросить у ближайшего смежного в восходящем направлении соседнего устройства метрики маршрутизации (такие как количество переходов).



В этой главе...

- Описана архитектура цифровой сети интегрированных служб (Integrated Services Digital Network — ISDN)
- Описаны уровни протокола ISDN
- Описано конфигурирование ISDN
- Описано конфигурирование маршрутизации по требованию (dial-on-demand routing — DDR)
- Описано тестирование ISDN и устранение ошибок
- Описано тестирование DDR и устранение ошибок

Технология ISDN и маршрутизация DDR

В настоящей главе описывается группа технологий, называемая в целом технологией ISDN, появившаяся более 30 лет назад. Осознавая ограничения, внутренние присущие общедоступной коммутируемой телефонной сети (Public Switched Telephone Network — PSTN), разработчики ISDN ставили своей целью создать цифровой канал передачи, который обеспечивал бы интегрированный доступ к широкому диапазону служб. Предполагалось, что эти службы будут включать в себя передачу голосовых данных, коммутацию пакетов и даже передачу видеоданных.

Наряду с изучением материала главы рекомендуется выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Стандарты ISDN

За прошедшие годы были согласованы и приняты многие стандарты ISDN. Они обещали приход высокоскоростной цифровой службы в дома и на предприятия. Несмотря на наличие большого количества стандартов ISDN, операторы связи не всегда одинаково практически воплощали эту технологию. Вследствие этого конфигурации сетей ISDN и уровень оплаты в различных регионах могут значительно отличаться друг от друга. В настоящее время потребители используют ISDN прежде всего как резервную технологию для распределенных сетей (wide-area network — WAN) и для осуществления удаленного доступа к телеработникам и малым офисам, как показано на рис. 14.1.

Провайдеры служб и крупные компании используют интерфейс первичной скорости передачи ISDN (*Primary Rate Interface — PRI*) или интерфейс базовой скорости передачи (*Basic Rate Interface — BRI*) для поддержки нескольких вызовов по общедоступной сети POTS (аналоговый модем). Несмотря на то, что ISDN значительно быстрее устанавливает соединение и обеспечивает более высокую пропускную способность, чем сеть POTS, многие потенциальные пользователи BRI-интерфейса предпочитают использовать современные технологии цифрового абонентского канала (*digital subscriber line — DSL*) или кабельные технологии. Эти технологии, как правило, обеспечивают большую пропускную способность и с меньшей стоимостью.

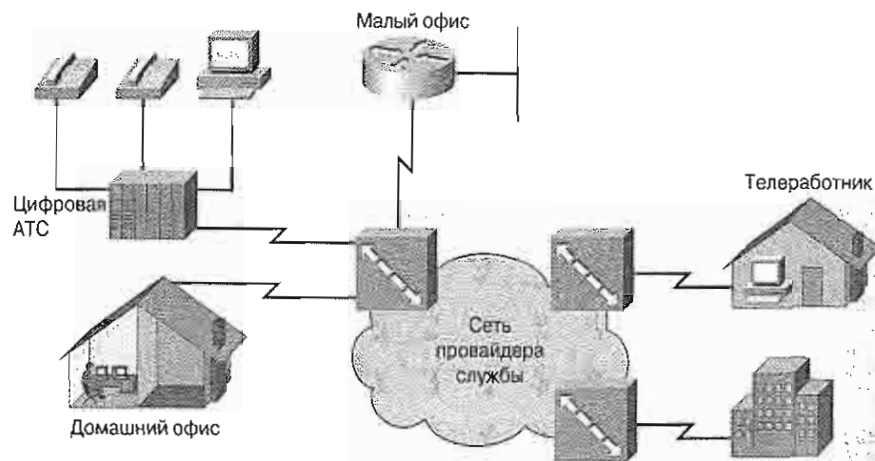


Рис. 14.1. Интегрированные службы

Несмотря на появление этих развивающихся технологий, ISDN остается жизнеспособным средством удаленного доступа по следующим причинам.

- В США ISDN более распространена, чем каналы DSL или кабельный доступ.
- Многие компании и провайдеры служб осуществили большие вложения в оборудование ISDN и обучение персонала и планируют дальнейшее развитие на базе этих инвестиций.
- Удаленные офисы, использующие ISDN, могут подсоединяться к центральным офисам (central office — CO) непосредственно, минуя общедоступный Internet.
- Большинство каналов DSL и кабельных сетей требуют, чтобы удаленный узел осуществлял связь с центральным узлом с помощью виртуальной частной сети (Virtual Private Network — VPN) через сеть Internet.

Обзор технологии ISDN

Для осуществления доступа к сети из удаленного места используются несколько WAN-технологий. В настоящей главе описываются службы, стандарты, компоненты, функционирование и конфигурирование соединений ISDN. Технология ISDN специально предназначена для решения проблем, связанных с недостаточностью полосы пропускания, с которой сталкиваются малые офисы или пользователи удаленного доступа при получении удаленного доступа с помощью традиционных телефонных служб.

Традиционная сеть PSTN основана на аналоговом соединении между помещением пользователя и локальным оператором. Это соединение также называется локальным ответвлением и показано на рис. 14.2. Такая аналоговая сигнализация налагает ограничения на ширину полосы пропускания, которая может быть достигнута в локальном ответвлении. Ограничения полосы пропускания не позволяют передавать аналоговые данные с частотой выше 3000 Гц. Снятие ограничений на полосу пропускания позволило использовать в локальном ответвлении цифровую сигнализацию, что привело к увеличению скоростей доступа для удаленных пользователей.

как показано на рис. 14.3. Однако пользователи, имеющие аналоговые модемы, по-прежнему используют полосу пропускания 3000 Гц аналоговой голосовой системы локального ответвления, что ограничивает скорость передачи значением примерно 56 Кбит/с в нисходящем направлении и значением 33 Кбит/с в восходящем.

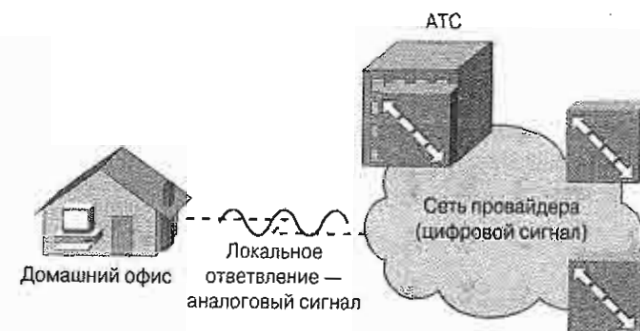


Рис. 14.2. Локальное ответвление

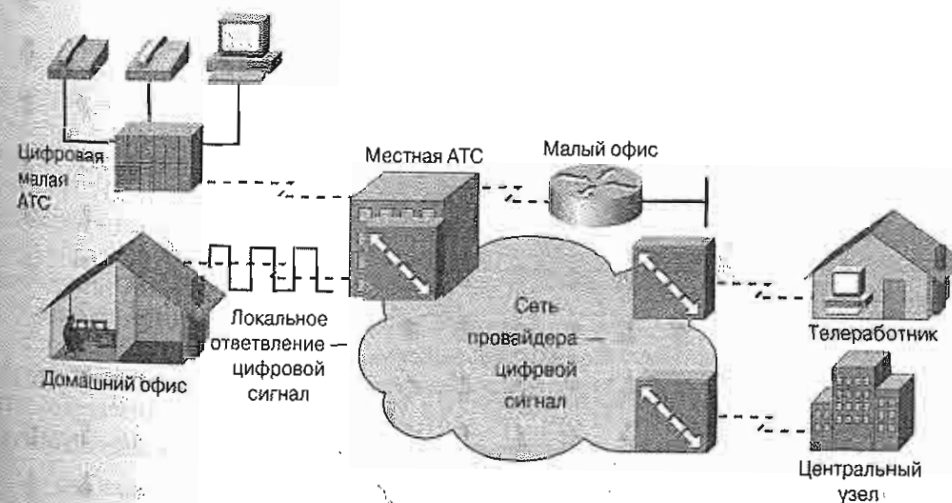


Рис. 14.3. Цифровая коммуникация с помощью ISDN

Телефонные компании разрабатывали ISDN с намерением создать полностью цифровую сеть. Технология ISDN позволяет передавать цифровые сигналы по существующим телефонным проводам. Это стало возможным, когда коммутаторы телефонных компаний были модернизированы для обработки цифровых сигналов. ISDN обычно используется для связи телеработников, малых и удаленных офисов с корпоративной сетью предприятия.

Телефонные компании разрабатывали ISDN как часть программы стандартизации служб клиентов. Частью этой разработки был интерфейс «пользователь-сеть» (User-Network Interface — UNI), более известный как локальное ответвление. Стандарты ISDN определяют характеристики аппаратного обеспечения и схемы установки вызова для сквозных цифровых соединений, которые помогают достичь главной цели — всемирной связи, которая обеспечивается, в частности, возможностью сетей ISDN легко связывать-

ся друг с другом. В сети ISDN переход к цифровой форме сигналов происходит, как правило, уже на узле пользователя, а не на узле телефонной компании.

Как указывает само название, ISDN использует цифровую технологию. ISDN заменяет традиционное аналоговое телефонное оборудование высокоскоростным цифровым оборудованием, которое создает для пользователя цифровое локальное ответвление. На рис. 14.4 выполнено сравнение схем аналогового и цифрового ответвления. Поскольку сеть POTS использует аналоговое локальное ответвление, носитель должен использовать импульсно-кодовую модуляцию (pulse code modulation — PCM) для кодирования аналоговых сигналов при передаче их по цифровым линиям связи. Такой тип аналогово-цифрового преобразования приносит нежелательную задержку и, потенциально, шум.

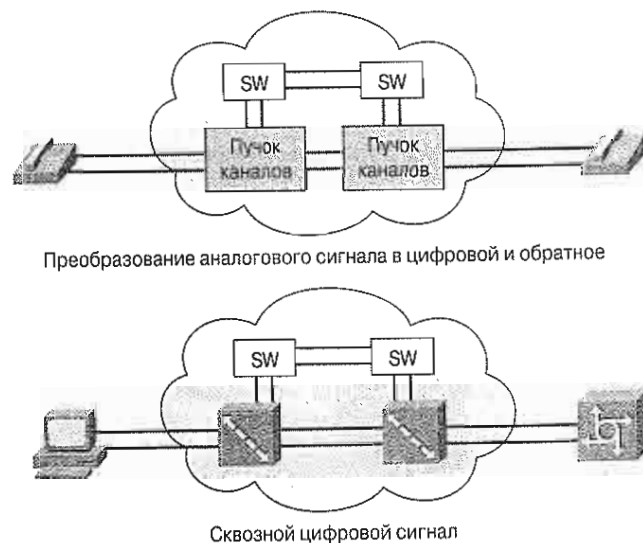


Рис. 14.4. Сравнение аналогового и цифрового соединения

Технология ISDN позволяет продолжить цифровое соединение до локального узла, что дает много преимуществ, включая следующие.

- Позволяет передавать данные различных типов (таких как обычные данные, голосовые и видеоданные).
- Позволяет быстрее устанавливать вызов, чем это делает обычная телефонная служба.
- Обеспечивает более высокую скорость передачи, чем у традиционных модемов.

Пользователи могут подсоединяться к носителю ISDN через два разных физических интерфейса: BRI и PRI. Отдельный интерфейс BRI или PRI обеспечивает передачу данных по пучку мультиплексированных В-каналов и D канал, как показано на рис. 14.5.

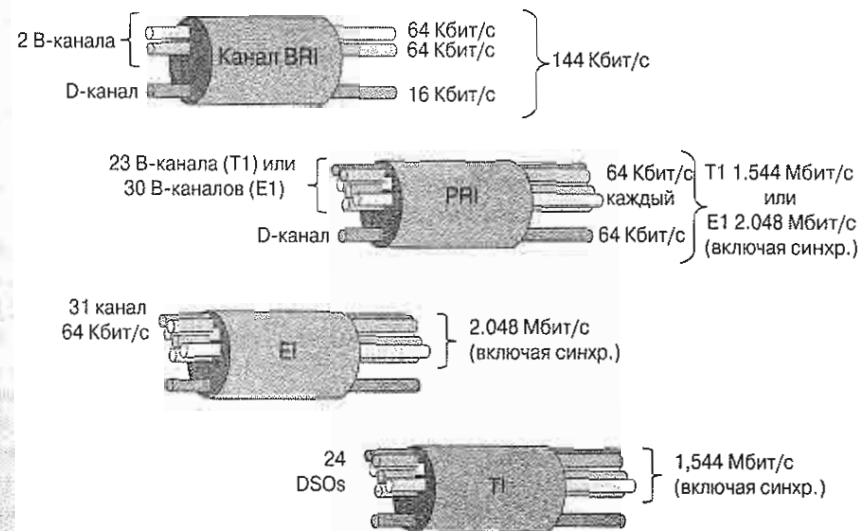


Рис. 14.5. Услуги ISDN

В-каналы ISDN называются каналами носителя, потому что по ним передаются обычные данные, голосовые и факсимильные данные. По В-каналам информация передается в виде фреймов с использованием в качестве протоколов 2-го (канального) уровня высокоуровневого протокола управления каналом (High-Level Data Link Control — HDLC) или протокола “точка-точка” (Point-to-Point Protocol — PPP). D-канал, или дельта-канал, используется для внеполосной сигнализации. По D-каналу передаются управляющие сообщения, такие как сообщения об установке канала или его отключении. Обычно D-канал использует на 2-м уровне протокол процедуры доступа к D-каналу (Link Access Procedure on the D channel — LAPD).

Служба BRI предоставляется по медному проводу локального ответвления, который обычно используется для аналоговой телефонной службы. Максимальная длина локального ответвления в Северной Америке составляет около 18 000 футов (или 5,5 км).

Служба BRI имеет следующие характеристики:

- два канала носителя со скоростями 64 Кбит/с;
- один дельта-канал со скоростью передачи 16 Кбит/с;
- полоса пропускания 48 Кбит/с для передачи информации о типах фреймов и синхронизации;
- Общая скорость 192 Кбит/с.

При обсуждении полосы пропускания интерфейса BRI ISDN важно точно определить, какая из характеристик BRI имеется в виду. Если речь идет о полосе пропускания, доступной для передачи данных пользователя, то BRI ISDN предоставляет полосу пропускания 128 Кбит/с (два В-канала со скоростями 64 Кбит/с). Если же обсуждается общая полоса пропускания обоих В-каналов и D-канала, то полоса пропускания BRI ISDN составляет 144 Кбит/с.

Хотя обычно этого не делается, можно говорить об общей полосе пропускания BRI ISDN, включая информацию о типе фреймов и синхронизацию, которая равна 192 Кбит/с.

Служба PRI ISDN предоставляется по выделенным линиям T1 и E1 между оборудованием пользователя (*Customer Premises Equipment — CPE*) и коммутатором ISDN. Коммутатор ISDN обычно является коммутатором Class 5 Telco, расположенным в центральном офисе. Этот коммутатор также обрабатывает голосовые вызовы.

Линия T1 также называется цифровой службой DS1, которая состоит из 24 каналов DS0, каждый из которых имеет скорость 64 Кбит/с, как показано в табл. 14.1. В-канал BRI также рассматривается как нулевой уровень цифровой службы и обозначается DS0.

Реализация PRI-интерфейса по линии T1 включает в себя:

- 23 канала носителя со скоростями 64 Кбит/с;
- один D-канал 64 Кбит/с, данные которого передаются в тайм-слоте 24.
- 8 Кбит/с информации о фреймах и синхронизации;
- общая скорость передачи 1,544 Мбит/с.

Передача данных по линии E1 обеспечивает следующие характеристики:

- 30 каналов носителя со скоростями 64 Кбит/с;
- Один D-канал 64 Кбит/с, данные которого передаются в тайм-слоте 16.
- 64 Кбит/с информации о фреймах и синхронизации;
- Общая скорость передачи 2,048 Мбит/с.

Таблица 14.1. Уровни цифрового сигнала

Уровень цифрового сигнала	Скорость передачи	T-обозначение	Количество каналов или служб DS0*
DS0	64 Кбит/с	—	1
DS1	1,544 Мбит/с	T1	24
DS2	6,312 Мбит/с	T2	96
DS3	44,736 Мбит/с	T3	672
DS4	274,176 Мбит/с	T4	4032

*DS0 = цифровая служба нулевого уровня (*digital service zero 0*)

Стандарты ISDN и методы доступа

Работа над стандартами для технологии ISDN началась в конце 60-х годов XX в. Полный набор рекомендаций по ISDN был опубликован в 1984 году и с тех пор постоянно обновлялся сектором стандартизации международного союза телекоммуникаций (*International Telecommunication Union Telecommunication Standardization Sector — ITU-T*), ранее известным как консультативный комитет по международной телеграфии и телефонии (*Consultative Committee for International Telegraph and Telephone — CCITT*). Стандарты ISDN представляют собой набор протоколов, которые охватывают различные аспекты цифровой телефонии и передачи данных. Союз ITU-T группирует и упорядочивает протоколы ISDN в соответствии с описанными ниже общими тематическими областями.

- **Е протоколы** — эти протоколы предлагают стандарты телефонной сети для ISDN. Например, протокол E.164 описывает международную адресацию для ISDN.
- **I протоколы** — описывают концепции, терминологию и общие методы. Серия I.100 включает в себя общие концепции ISDN и описывает структуру других рекомендаций I-серии. Серия I.200 описывает различные аспекты служб ISDN. Серия I.300 описывает аспекты работы сети. Серия I.400 описывает интерфейс UNI.
- **Q протоколы** — описывают коммутацию и сигнализацию в сетях ISDN. Термин “сигнализация” в данном контексте означает процесс установки вызова ISDN.

Стандарты ISDN определяют два главных типа каналов, каждый из которых имеет свою скорость передачи. Канал носителя (В-канал) представляет собой “чисто” цифровой маршрут со скоростью передачи 64 Кбит/с. Термин “чистый” означает, что этот канал может быть использован для передачи любых типов цифровых данных, таких, например, как оцифрованные голосовые данные, в дуплексном режиме. Второй канал называется дельта-каналом (D-канал) и может иметь скорость передачи 16 или 64 Кбит/с. D-канал имеет скорость 16 Кбит/с для интерфейса BRI и 64 Кбит/с для интерфейса PRI. Различные типы доступа в технологии ISDN показаны на рис. 14.6. D-канал используется для передачи управляющей информации для В-канала. Следует помнить о том, что при создании соединения TCP происходит обмен информацией, называемый установкой вызова. Эта информация передается по тому же маршруту, который, вероятно, будет использоваться для передачи данных. При этом для передачи управляющей информации и данных используется один и тот же маршрут. Такой метод называется внутрислосной сигнализацией. В ISDN для передачи управляющей информации используется отдельный D-канал. Такой подход называется внеполосной сигнализацией.

В технологии ISDN определены два стандартных метода доступа: BRI и PRI. Отдельный интерфейс BRI или PRI обеспечивает мультиплексированный пучок В- и D-каналов.

Интерфейс BRI использует два канала носителя (В) со скоростью 64 Кбит/с и один дельта-канал (D) со скоростью 16 Кбит/с. По В-каналам передаются данные пользователя, а по D-каналу — информация сигнализации и управляющая информация. Интерфейс BRI может работать со многими маршрутизаторами Cisco. Поскольку интерфейс BRI использует два В-канала и один D-канал, его иногда обозначают *2B+D*.

Канал	Пропускная способность	Чаще всего используется для
В	64 Кбит/с	Передачи данных в сетях с коммутацией каналов (протоколы HDLC, PPP)
D	16/64 Кбит/с	Передачи информации сигнализации (LAPD)

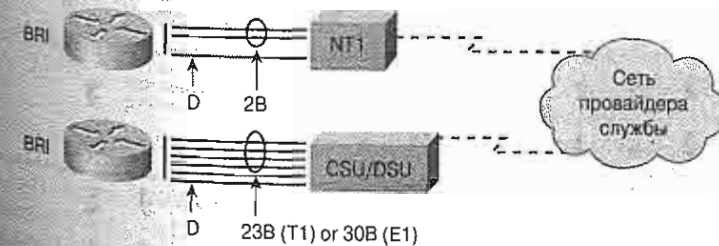


Рис. 14.6. Варианты доступа в технологии ISDN

В-каналы могут использоваться для передачи оцифрованных голосовых данных. В этом случае для кодировки голосовых данных используются специальные методы. В-каналы могут также использоваться для передачи обычных цифровых данных с относительно высокой скоростью. В этом режиме информация передается в виде фреймов, формат которых определяется протоколами 2-го уровня: HDLC или PPP.

Протокол PPP значительно более надежен чем HDLC поскольку он обеспечивает прекрасный механизм для аутентификации и согласования совместимого канала и конфигурации протокола. Узкополосный ISDN рассматривается как соединение с коммутацией каналов. В-канал является базовым модулем коммутации каналов. По D-каналу передаются сообщения сигнализации для управления вызовами по В-каналам, такие как сообщения об установке канала и его отключении. При передаче данных по D-каналу используется протокол LAPD. LAPD представляет собой протокол канального уровня, основанный на протоколе HDLC. В Северной Америке и Японии интерфейс PRI обеспечивает 23 В-канала со скоростью 64 Кбит/с и один D-канал со скоростью 64 Кбит/с.

В Европе и в большинстве других стран мира интерфейс PRI обеспечивает 30 В-каналов и один D-канал, т.е. он обеспечивает такой же уровень службы как и линия E1. Для соединений T1/E1 интерфейс PRI использует DSU/CSU.

3-уровневая модель ISDN и протоколы

ISDN использует набор стандартов ITU-T, охватывающих физический, канальный и сетевой уровни эталонной модели OSI, как показано в табл. 14.2.

- Спецификации физического уровня интерфейсов BRI и PRI ISDN определены в документах ITU-T I.430 и I.431, соответственно.
- Спецификации канального уровня ISDN основаны на протоколе LAPD и формально описаны в документах ITU-T Q.920, ITU-T Q.921, ITU-T Q.922 и ITU-T Q.923.
- Сетевой уровень ISDN определен в стандартах ITU-T Q.930 (также известном как I.450) и ITU-T Q.931 (также известном как I.451) и включает в себя соединения пользователей между собой, соединения с коммутацией каналов и соединения с коммутацией пакетов.

Таблица 14.2. Протоколы ISDN

Уровень эталонной модели OSI	D-канал	В-канал
3	Q.931 — Сетевой уровень ISDN между терминалом и коммутатором	IP
2	Q.921 — Процедура доступа к D-каналу (Link Access Procedure on the channel — LAPD)	PPP HDLC
1	I.430/I.431 — интерфейсы ISDN физического уровня: I.430 для базового интерфейса; I.431 для первичного интерфейса;	

Служба BRI обеспечивается через медный кабель локального ответвления, традиционно используемого для телефонных служб. PRI этом имеется лишь один физический маршрут, однако три информационных маршрута (2B+D). Информация от этих трех каналов мультиплексируется в один физический канал.

Форматы фреймов физического (1-го) уровня ISDN различаются в зависимости от того, является ли фрейм исходящим (от терминала в сеть — формат фрейма TE) или входящим (от сети терминалу — формат фрейма NT), как показано на рис. 14.7. Каждый фрейм содержит 16 битов от канала B1, 16 битов от канала B2, 4 бита от D-канала и 12 битов служебной нагрузки, которые вместе определяют размер фрейма, равный 48 битам. Каждую секунду передаются 4000 таких фреймов, соответственно, каналы B1 и B2 имеют пропускную способность $16 \cdot 4000 = 64$ Кбит/с, а канал D имеет пропускную способность $4 \cdot 4000 = 16$ Кбит/с.

Биты служебной нагрузки фрейма физического уровня ISDN выполняют описанные ниже функции.

- Бит описания фрейма — обеспечивает синхронизацию.
- Бит распределения нагрузки — регулирует среднее битовое значение.
- Отклик на предыдущие биты D-канала — используется для разрешения конфликта в тех случаях, когда несколько терминалов на пассивной шине конкурируют за право доступа к каналу.
- Бит активизации — активизирует устройства.
- Вакантный бит — в настоящее время не используется.
- 8 добавленных битов счетчиков битов в каналах.

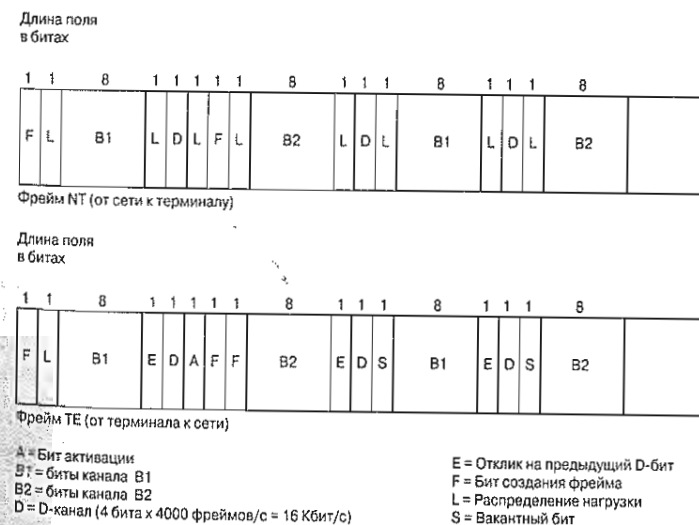


Рис. 14.7. Формат фрейма физического уровня ISDN

Отметим, что физическая скорость передачи в битах для BRI-интерфейса составляет $4000 \times 48 = 192$ Кбит/с. Эффективная скорость передачи равна $4000 \times 36 = 144$ Кбит/с = 64 Кбит + 64 Кбит + 16 Кбит (2B+D).

Протоколом 2-го уровня сигнализации ISDN является LAPD. Этот протокол аналогичен протоколу HDLC и используется в D-канале для того, чтобы потоки управляющей информации и информации сигнализации отправлялись и получались соответствующим образом.

Поля флага и управления идентичны аналогичным полям протокола HDLC, как показано на рис. 14.8. Поле адреса протокола LAPD имеет длину 2 байта. Первый байт поля адреса содержит идентификатор точки доступа к службе (service access point identifier — SAPI), который идентифицирует портал, в котором службы протокола LAPD предоставляются 3-му уровню. Бит команды/ответа (command/response — C/R) указывает на то, является ли фрейм командой или ответом на нее. Второй байт содержит идентификатор конечной точки терминала (Terminal Endpoint Identifier — TEI). Каждому устройству терминального оборудования в помещениях пользователя требуется уникальный идентификатор. Этот идентификатор TEI может быть назначен статически PRI установке (0–63), либо динамически назначен коммутатором, когда это оборудование станет впервые участвовать в вызове. Если в поле TEI содержится только единицы, то это указывает на то, что фрейм является широковещательным.

Идентификаторы TEI и SAPI вместе образуют адрес 2-го уровня. Идентификатор SAPI представляет собой 6-битовое число, которое используется для идентификации различных типов данных и управления ими для одного и того же индивидуального устройства, подсоединенного к сети ISDN. Отметим, что некоторые сообщения ISDN предназначены для установки и прекращения вызова, в то время как другие используются для передачи реальных данных. Таким образом идентификатор TEI представляет конкретное устройство ISDN, а идентификатор SAPI — конкретный процесс, происходящий на этом устройстве. Например, значение SAPI, равное 0, используется для идентификации процедур управления вызовом, в то время как значение SAPI, равное 63 идентифицирует функцию управления на 2-м уровне.

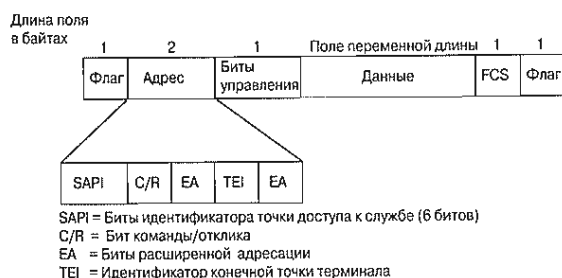


Рис. 14.8. Канальный уровень ISDN

Подобно тому, как фрейм Ethernet II содержит адрес управления доступом к среде передачи (Media Access Control — MAC) и информацию о типе протокола, фрейм LAPD содержит значения идентификаторов TEI и SAPI.

Установка вызова ISDN

Для того, чтобы установить соединение одного маршрутизатора с другим через сеть ISDN, необходимо выполнить несколько сеансов обменов данными. Для установки вызова ISDN между маршрутизатором и коммутатором ISDN используется

D-канал, а в сети провайдера службы между коммутаторами используется сигнализация сигнальной системы 7 (Signaling System 7 — SS7).

D-канал между маршрутизатором и коммутатором ISDN всегда находится в активном состоянии. Протокол Q.921 описывает процессы канального уровня протокола LAPD, которые функционируют как процессы 2-го уровня в эталонной модели OSI (Open System Interconnection — OSI). D-канал используется для функций управления вызовом, таких как установка вызова, сигнализация и прекращение вызова. Эти функции реализованы в протоколе Q.931. Протокол Q.931 определяет функции эталонной модели OSI на 3-м уровне. Стандарт Q.931 рекомендует использовать соединение сетевого уровня между терминальной конечной точкой и локальным коммутатором ISDN, однако эта рекомендация не носит обязательного характера. Поскольку некоторые коммутаторы ISDN были разработаны до того, как протокол Q.931 был стандартизован, некоторые провайдеры служб ISDN и некоторые типы коммутаторов могут использовать (и действительно используют) различные реализации протокола Q.931. Поскольку типы коммутаторов не стандартизованы, маршрутизаторы в своих конфигурациях должны иметь команды, указывающие тип коммутатора ISDN, к которому они подсоединены.

Вызов ISDN может быть установлен несколькими способами. В начале вызова вызывающая сторона делает запрос на установку вызова, как показано на рис. 14.9. До того, как произойдет реальное соединение и обработка вызова, происходит обмен сообщениями, такими, например, как сообщение обработки. Это необязательное сообщение указывает как происходит обработка вызова.

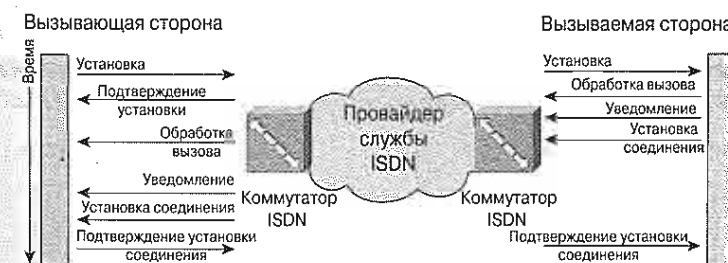


Рис. 14.9. Установка вызова ISDN по протоколу Q.931

Это же относится и к сообщению предупреждения, которое типично для телефонных сообщений, но не является обязательным. При передаче данных такие сообщения используются довольно редко. В большинстве случаев при вызовах для передачи данных пользователь видит сообщения о соединении.

Разные коммутаторы ISDN используют для установки и прекращения вызова различные процедуры. В зависимости от типа коммутатора могут выполняться все или только некоторые из этапов, показанных на рис. 14.9. Однако обмен такими сообщениями, как сообщения об установке, соединении и подтверждении соединения имеет место всегда.

Ниже описана последовательность событий, происходящих при установке вызова через интерфейс BRI или интерфейс PRI.

- Для отправки вызываемого номера локальному коммутатору ISDN используется D-канал.

- Локальный коммутатор использует протокол сигнализации SS7 для установки маршрута и передачи вызываемого номера удаленному коммутатору ISDN.
- Удаленный коммутатор ISDN посылает сигнал получателю по D-каналу.
- После того, как удаленный маршрутизатор сообщает, что он готов принять вызов, удаленный коммутатор ISDN использует сигнализацию SS7 для отправки сообщения "call-connect" локальному коммутатору.
- По одному из В-каналов осуществляется сквозное соединение, в то время как другой В-канал остается доступным для нового обмена сообщениями или для передачи данных. Оба В-канала могут использоваться одновременно.

Как и при установке вызова, запрос на прекращение вызова не является сквозной функцией, а обрабатывается коммутатором ISDN. Процесс освобождения каналов основан на обмене тремя сообщениями:

- Отсоединить (Disconnect)
- Освободить (Release)
- Полностью освободить (Release complete)

Сообщение "Освободить" передается по сети максимально быстро, насколько это возможно. На рис. 14.10 предполагается, что сообщение об освобождении генерируется вызываемой стороной. Этот процесс инициируется сообщением об отсоединении, передаваемым по D-каналу между вызывающей и вызываемой сторонами.

После получения этого сообщения пункт обмена немедленно начинает освобождение маршрута коммутатора, который поддерживает В-канал. Сообщение об освобождении одновременно посылается также и следующему пункту обмена. Таким образом сообщение проходит по всей сети через промежуточные пункты обмена к конечному пункту.

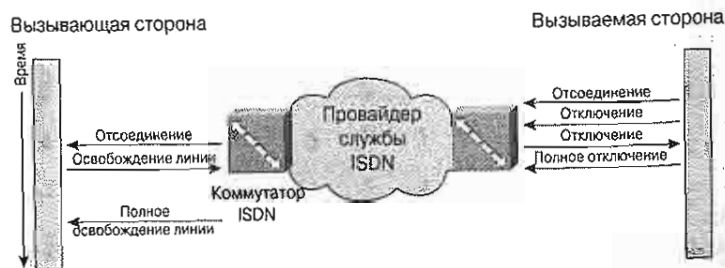


Рис. 14.10. Прекращение вызова ISDN по протоколу Q.931

По мере того как вовлеченные в этот процесс пункты обмена отключают вызов, сообщение об освобождении в конечном итоге поступает на оконечный пункт. Такая передача вызывает следующие действия:

- вызывающей стороне поступает сообщение об отсоединении;
- запускается таймер для того, чтобы обеспечить прием сообщения об освобождении;
- происходит отсоединение коммутируемого маршрута;
- когда сообщение об освобождении канала получено от предшествующего пункта обмена, ему посылается сообщение о полном освобождении.

Функции ISDN и контрольные точки

Стандарты ISDN определяют функцию как устройство или элемент аппаратного обеспечения, который предоставляет пользователю возможность доступа к службам при или BRI. Производители могут создавать аппаратное обеспечение, которое поддерживает одну или более функций. Спецификации ISDN определяют четыре *контрольные точки* (reference points), которые соединяют одно устройство ISDN с другим. Каждое устройство в сети ISDN выполняет свою конкретную задачу для облегчения создания сквозного соединения.

Для того, чтобы соединить между собой устройства, выполняющие конкретные специфические функции, необходимо четко определить интерфейс между этими двумя устройствами. Эти интерфейсы называются контрольными точками и показаны на рис. 14.11. контрольная точка определяет тип соединения между двумя функциями.

Контрольными точками, оказывающими влияние на соединение ISDN со стороны пользователя, являются следующие.

- **Контрольная точка R** — относится к соединению между несовместимым с ISDN устройством (TE2) и терминальным адаптером, таким, например, как последовательный интерфейс RS-232.
- **Контрольная точка S** — относится к точкам подсоединения коммутирующего устройства пользователя (NT2) и позволяет осуществлять вызовы между различными типами устройств CPE.
- **Контрольная точка T** — электрически идентична S-интерфейсу; относится к выходному соединению устройства NT2 с сетью ISDN или устройством NT1.
- **Контрольная точка U** — относится к соединению между устройством NT1 и сетью ISDN, принадлежащей телефонной компании.

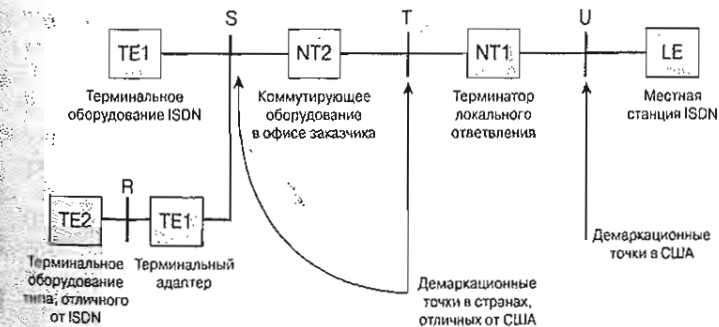


Рис. 14.11. Контрольные точки сети ISDN

Поскольку контрольные точки S и T электрически идентичны, некоторые интерфейсы обозначаются как интерфейсы S/T. Хотя эти контрольные точки выполняют различные функции, порт в электрическом аспекте остается одним и тем же и может быть использован для любой из этих функций.

Обилие аббревиатур и акронимов ISDN может вызвать у читателя некоторое замешательство. Для правильной установки сети ISDN и ее тестирования необходимо знать, как реально выглядят все ее компоненты и контрольные точки. Как показано

на рис. 14.12, соединение состоит из стенной розетки со стандартным двухпроводным кабелем к устройству NT1, далее от устройства NT1 проходит четырехпроводный кабель к ISDN-телефону, маршрутизатору Cisco или факсимильному аппарату ISDN. Интерфейс S/T реализуется с использованием восьмипроводного штекера, который позволяет подавать питание на устройства NT и TE.

Поскольку все эти штекеры внешне идентичны (как RJ-11, RJ-45 и т.д.), при их подсоединении следует соблюдать осторожность. Контрольная точка S/T представляет собой четырехпроводный интерфейс (TX и RX). Он принадлежит к типу “точка-точка” или является многоточечным (пассивная шина). При этом используется спецификация ITU I.430. Интерфейс S/T определяет интерфейс между устройством TE1 или терминальным адаптером (*Terminal Adapter* — TA) и устройством NT.

U-интерфейс определяет двухпроводный интерфейс между устройством NT и средой сети ISDN. R-интерфейс определяет интерфейс между адаптером TA и подсоединенным устройством, не являющимся устройством ISDN (TE2). Комбинация устройств NT1 и NT2 иногда обозначается как NTU.

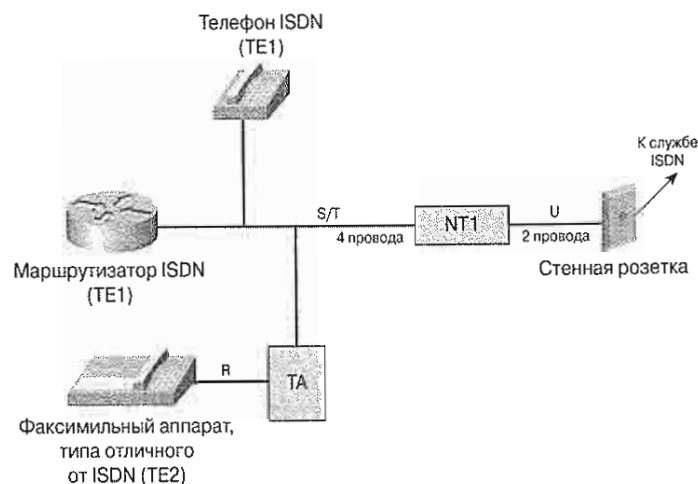


Рис. 14.12. Физические контрольные точки интерфейса BRI ISDN

К обычному S-интерфейсу ISDN могут быть подключены через одну и ту же шину (S-шина) несколько конечных устройств с различными возможностями. Если коммутатор может осуществлять связь с несколькими устройствами, то его обычно называют “многоточечным” (“multipoint.”). К сожалению, это создает определенные сложности как при установке устройства ISDN, так и при обработке вызова. Эти сложности вызывают необходимость в использовании идентификаторов профиля службы (Service Profile Identifier — SPID) и идентификаторов конечных точек (Endpoint Identifier — EID).

При выборе оборудования ISDN важно знать тип контрольной точки, который определяет тип интерфейса ISDN, который требуется пользователю. В США для подсоединения к провайдеру, как правило, требуется U-интерфейс. Это означает, что если приобретается маршрутизатор ISDN с интерфейсом S/T, то потребуется приобрести дополнительное оборудование (устройство NT1) для подсоединения к сети провайдера.

ра. Кроме того, при ошибочном подключении маршрутизатора с U-интерфейсом к устройству NT1 возможно серьезное повреждение устройств.

Таким образом, знание типа контрольных точек ISDN является принципиально важным для правильного выбора и подключения устройств ISDN.

Определение ISDN-интерфейса на маршрутизаторе

В США от пользователя требуется, чтобы он обеспечил устройство NT1. В Европе и многих других странах телефонные компании обеспечивают функцию NT1 и предоставляют пользователю интерфейс S/T. В этих конфигурациях от пользователя не требуется предоставлять отдельное устройство NT1 или интегрированную функцию NT1 в терминальном устройстве. Соответствующим образом должно заказываться другое оборудование, такое как модули и интерфейсы ISDN для маршрутизатора.

Для правильного выбора маршрутизатора Cisco с соответствующим интерфейсом ISDN необходимо выполнить следующие действия.

Этап 1. Определить, поддерживает ли маршрутизатор интерфейс BRI ISDN.

Этап 2. Определить поставщика устройства NT1. Этим устройством NT1 заканчивается локальное ответвление от центрального офиса (CO) провайдера службы ISDN. В США устройство NT1 относится к оборудованию пользователя CPE; это означает, что ответственность за его установку возлагается на пользователя. В Европе устройство NT1 обычно предоставляется провайдером службы.

Этап 3. Если устройство NT1 входит в состав оборудования CPE, то следует удостовериться в том, что маршрутизатор имеет U-интерфейс. Если у маршрутизатора S/T-интерфейс, то для подсоединения к сети провайдера ISDN потребуется устройство NT1.

Если маршрутизатор имеет гнездо с меткой “BRI”, то он уже имеет функции ISDN. Если маршрутизатор имеет встроенный интерфейс ISDN, то он является устройством TE1. Если маршрутизатор имеет U-интерфейс, то он также имеет и встроенное устройство NT1.

Если у маршрутизатора нет гнезда с меткой “BRI” и он является маршрутизатором с фиксированной конфигурацией (не является модульным), то для связи ISDN потребуется использовать его существующий последовательный интерфейс. При использовании добавляемого внешнего ISDN-интерфейса, такого как последовательный интерфейс, для обеспечения BRI-соединения потребуется подсоединение внешнего адаптера TA к последовательному интерфейсу. Если маршрутизатор является модульным, то, возможно, удастся установить плату ISDN-интерфейса при условии, что имеется доступный слот. Отметим, что маршрутизатор с U-интерфейсом ни в коем случае нельзя подключать к устройству NT1. Это, вероятнее всего, приведет к повреждению интерфейса.

Типы коммутаторов ISDN

На маршрутизаторах должен быть сконфигурирован тип коммутатора ISDN, с которым маршрутизатор будет обмениваться данными. Возможные типы коммутатора ISDN различаются в зависимости от региона страны, в котором используется комму-

татор. Причиной этого являются различные возможные реализации протокола Q.931, который используется в качестве протокола сигнализации D-канала в коммутаторах, изготавливаемых различными производителями.

Услуги, предоставляемые провайдерами, значительно различаются в зависимости от страны и конкретного региона. Так же как и модемы, различные типы коммутаторов имеют некоторые отличия в работе и предъявляют различные требования к установке вызова. Вследствие этого перед подключением маршрутизатора к некоторой службе ISDN необходимо знать тип коммутатора, установленного на телефонной станции. Эта информация указывается при конфигурировании маршрутизатора для того, чтобы он мог разместить вызовы сетевого уровня ISDN и пересылать данные.

В табл. 14.3 перечислены страны и типы коммутаторов ISDN, используемых в этих странах.

Таблица 14.3. Типы коммутаторов ISDN в различных странах мира

Страна	Тип коммутатора
США и Канада	5ESS и 4ESS компании AT&T; DMS-100 компании Northern Telecom
Франция	VN2, VN3
Япония	NTT
Великобритания	Net3 и Net5
Другие страны Европы	Net3

В дополнение к типу коммутатора, который используется провайдером службы ISDN, в некоторых случаях необходимо также узнать какие идентификаторы SPID назначены телекоммуникационной компанией (Telco). Идентификатор SPID представляет собой номер, который назначается оператором ISDN для идентификации конфигурации линии службы BRI. Идентификаторы SPID позволяют нескольким устройствам ISDN, таким как оборудование для передачи голосовых и обычных данных, совместно использовать локальное ответвление. В частности, идентификаторы SPID требуются для коммутаторов национальной сети ISDN-01 и для коммутаторов SMS-100.

Идентификаторы SPID используются только в Северной Америке и в Японии. Идентификатор SPID предоставляется оператором ISDN для идентификации линии службы ISDN. Во многих случаях при конфигурировании маршрутизатора требуется ввести идентификаторы SPID.

Каждый идентификатор SPID указывает на информацию об установке линии и о конфигурации. Идентификатор SPID представляет собой последовательность символов, которые обычно напоминают телефонные номера. Идентификаторы SPID идентифицируют все B-каналы на коммутаторе центрального офиса (CO). После того, как все эти каналы идентифицированы, коммутатор подсоединяет доступные службы к данному соединению. Следует помнить о том, что технология ISDN обычно используется для соединений удаленного доступа. Идентификаторы SPID обрабатываются при первоначальном подсоединении маршрутизатора к коммутатору ISDN. Если идентификаторы SPID являются необходимыми, но сконфигурированы неправильно, то инициализация не происходит и службы ISDN использоваться не могут.

Конфигурирование ISDN

ISDN определяет характер данных и управляющей информации, которая передается между ISDN-оборудованием пользователя CPE и коммутатором оператора. Провайдеры служб ISDN используют для своих служб ISDN различные типы коммутаторов. Каждый тип коммутатора функционирует несколько особым образом и имеет свои специфические требования к установке вызова. Оборудование CPE ISDN должно быть сконфигурировано с учетом типа коммутатора в центральном офисе CO, с которым будет осуществляться связь. Для того, чтобы стала возможной установка вызовов, передача и прием данных, эта информация должна быть сконфигурирована на маршрутизаторе пользователя. В настоящем разделе основное внимание будет уделено конфигурированию ISDN.

Имеется два типа доступа к службам ISDN: через интерфейсы BRI и PRI. Вопросы конфигурирования для интерфейсов BRI и PRI будут рассмотрены отдельно. В настоящем разделе рассматриваются команды, используемые для проверки правильности конфигурации. В нем рассматриваются следующие темы:

- конфигурирование BRI ISDN;
- конфигурирование PRI ISDN;
- тестирование конфигурации ISDN;
- устранение ошибок в конфигурации ISDN.

Для подготовки маршрутизатора к работе в среде ISDN необходимо задать на нем глобальные параметры и параметры отдельных интерфейсов. В настоящем разделе основное внимание уделяется конфигурированию интерфейса BRI на маршрутизаторах доступа.

В режиме глобального конфигурирования необходимо указать тип коммутатора провайдера служб ISDN. Существует около 10 возможных типов коммутаторов, в зависимости от страны, в которой устанавливается соединение, из которых необходимо выбрать соответствующий данной конкретной ситуации.

Задачи конфигурирования адресации ISDN включают в себя назначение IP-адреса, группы набора (для DDR) и ввод директив профиля службы ISDN (номера SPID). Необходимо также включить команду **dialer map**, которая связывает статическое преобразование адреса получателя с IP-адресом, именем узла и номером набора ISDN.

Конфигурирование интерфейса BRI ISDN

Для указания типа коммутатора провайдера ISDN в конфигурацию маршрутизатора можно ввести команду **isdn switch-type switch-type**. Ввод команды **isdn switch-type** в режиме глобального конфигурирования задает тип коммутатора ISDN одинаковым для всех интерфейсов ISDN. После ввода этой команды в режиме глобального конфигурирования могут быть отдельно сконфигурированы индивидуальные интерфейсы для указания иных типов коммутаторов.

В табл. 14.4 приведены типы коммутаторов ISDN.

Таблица 14.4. Типы коммутаторов BRI ISDN

Тип коммутатора	Описание
basic-5ess	Коммутаторы базовой скорости компании AT&T (США)
basic-dms 100	NT DMS-100 (Северная Америка)
basic-ni	Национальная сеть ISDN (Северная Америка)
basic-1tr6	ISDN-коммутаторы 1TR6 производства Германии
basic-nwnet3	ISDN-коммутаторы Net3 производства Норвегии
basic-nznet3	ISDN-коммутаторы Net3 производства Новой Зеландии
basic-ts013	ISDN-коммутаторы TS013 и TS014 производства Австралии
basic-net3	ISDN-коммутаторы NET3 в Великобритании и других странах Европы
ntt	ISDN-коммутатор NTT (Япония)

Разные провайдеры ISDN используют различные типы коммутаторов. Фактически некоторые провайдеры используют один тип коммутатора (входящего в состав аппаратного обеспечения) для имитации другого типа коммутатора в программном обеспечении. Соответствующую информацию о типе коммутатора можно получить у провайдера службы ISDN. Если на маршрутизаторе не задан правильный тип коммутатора, то он не сможет осуществлять связь с коммутатором ISDN по протоколу Q.931 на 3-м уровне. Иными словами, невозможно будет создать вызов ISDN или принять такой вызов.

Для задания типа коммутатора используется команда **isdn switch-type**. Однако требуется принять решение о том, в каком режиме ввести эту команду: в режиме глобального конфигурирования или в режиме конфигурирования интерфейса.

При вводе команды **isdn switch-type** в глобальном режиме все ISDN-интерфейсы маршрутизатора будут сконфигурированы для одного и того же типа коммутатора.

```
Router(config)#isdn switch-type type
```

При вводе команды **isdn switch-type** в режиме конфигурирования интерфейса данный тип коммутатора будет установлен только для данного интерфейса.

```
Router(config-if)#isdn switch-type type
```

Следует отметить, что действие команды в режиме конфигурирования интерфейса отменяет для данного интерфейса действие команды глобального режима. Обычно тип коммутатора задается в глобальном режиме и помощью команды **isdn switch-type**. Однако в некоторых случаях может потребоваться задание двух различных типов коммутаторов ISDN. Это необходимо в тех случаях, когда один и тот же маршрутизатор подсоединяется как к BRI-интерфейсу, так и к PRI-интерфейсу. По этой причине начиная с версии IOS Cisco 11.3(T) действие этой команды расширено на режим конфигурирования интерфейса. Команда **interface bri interface-number** назначает ISDN-интерфейс на маршрутизаторе, который аппаратно поддерживает ISDN (устройство TE1). Соответственно, для того, чтобы сконфигурировать на первом интерфейсе ISDN тип коммутатора базовой скорости AT&T, следует ввести команды, приведенные в примере 14.1.

Пример 14.1. Команда **interface bri**

```
RTA(config)#interface bri 0
RTA(config-if)#isdn switch-type basic-5ess
```

Если маршрутизатор аппаратно не поддерживает ISDN (т.е. является устройством TE2) то для него требуется внешний терминальный адаптер ISDN. На таком маршрутизаторе следует использовать команду **interface serial interface-number**. После того, как служба ISDN установлена, провайдер службы сообщает информацию о типе коммутатора и идентификаторы SPID. Эти идентификаторы используются для определения служб, доступных индивидуальным клиентам службы ISDN. В зависимости от типа коммутатора эти идентификаторы SPID могут быть добавлены в конфигурацию. Коммутаторы национальной сети ISDN-1 и коммутаторы DMS-100 требуют конфигурирования идентификаторов SPID, в то время как для коммутаторов типа 5ESS компании AT&T этого не требуется. Идентификаторы SPID должны быть заданы при использовании имитатора Adtran ISDN. Этот имитатор представляет собой устройство, которое может быть использовано в лабораторных условиях и при тестировании для имитации соединения ISDN без необходимости реального получения учетной записи у провайдера. Формат идентификаторов SPID может различаться в зависимости от типа коммутатора ISDN и требований конкретного провайдера. Для задания идентификаторов SPID, требуемых сетью ISDN при иницировании вызова с локальным пунктом обмена ISDN, следует использовать команды режима конфигурирования интерфейса **isdn spid1** и **isdn spid2**. В табл. 14.5 описаны эти две команды.

Таблица 14.5. Параметры команд **isdn spid1** и **isdn spid2**

Параметры команд	Описание
spid-number	Номер, задающий службу к которой происходит подсоединение. Это значение назначается провайдером службы ISDN
ldn	(Необязательный) Номер локального набора. Этот номер должен соответствовать информации вызываемой стороны, поступающей от коммутатора ISDN для использования обоих В-каналов на большинстве коммутаторов

Аргумент **switch-type** указывает тип коммутатора провайдера службы ISDN. Для отключения коммутатора на интерфейсе ISDN следует ввести команду **isdn switch-type none**. В примере 14.2 показано конфигурирование BRI-интерфейсов ISDN в режиме глобального конфигурирования.

Пример 14.2. Конфигурирование BRI-интерфейса в национальной сети ISDN

```
Router(config)#isdn switch-type basic-ni
```

Для задания идентификаторов SPID следует использовать команду **isdn spid#** в режиме конфигурирования интерфейса для определения номеров SPID, назначенных для В-каналов.

```
Router(config-if)# isdn spid1 spid-number [ldn]
Router(config-if)#isdn spid2 spid-number [ldn]
```

Необязательный параметр *ldn* определяет локальный номер каталога набора. Для большинства коммутаторов этот номер должен соответствовать информации вызываемой стороны, поступающей от коммутатора ISDN. Идентификаторы SPID задаются в режиме конфигурирования интерфейса.

Для входа в режим конфигурирования интерфейса необходимо ввести в режиме глобального конфигурирования команду **interface bri**.

```
Router(config)#interface bri slot/port
```

Аргумент *slot/port* описывает номер слота адаптера порта/номер порта интерфейса. Эти номера назначаются при изготовлении во время установки или при их добавлении к системе. Их можно вывести на экран с помощью команды **show interfaces**.

Для того, чтобы задать идентификаторы SPID для обоих В-каналов на интерфейсе BRI 0/0, следует использовать синтаксис команд, показанный в примере 14.3.

Пример 14.3. Задание на идентификаторов SPID на интерфейсе BRI

```
Router(config)#interface bri0/0
Router(config-if)#isdn spid1 51055540000001 5554000
Router(config-if)#isdn spid2 51055540010001 5554001
```



Лабораторная работа: конфигурирование BRI-интерфейса ISDN

В этой лабораторной работе требуется сконфигурировать маршрутизатор ISDN для его подсоединения к коммутатору ISDN. Для имитации среды коммутатор/ISDN используется имитатор ISDN Adtran Atlas550.

Конфигурирование PRI-интерфейса ISDN

Интерфейс PRI реализуется по выделенной линии T1 или E1. Ниже описаны основные задачи конфигурирования PRI-интерфейса.

- Этап 1.** Задать тип коммутатора ISDN. Необходимо задать правильный тип коммутатора PRI, с которым маршрутизатор будет осуществлять интерфейс в центральном офисе (CO) провайдера.
- Этап 2.** Выбрать контроллер. Необходимо указать контроллер T1/E1, тип фреймов и кодировку в линии для устройства провайдера.
- Этап 3.** Установить порт интерфейса, который будет функционировать в качестве интерфейса PRI. Задать тайм-слот группы PRI для линии T1/E1 и указать используемую скорость.

Поскольку маршрутизатор подсоединяется к интерфейсу PRI с использованием линии T1/E1, как такового интерфейса PRI нет. Вместо этого физический интерфейс маршрутизатора, который подсоединен к выделенной линии, называется контроллером T1 (или контроллером E1, если используется линия E1). Этот контроллер должен быть правильно сконфигурирован для осуществления интерфейса с сетью оператора связи. D-канал и В-каналы интерфейса PRI ISDN конфигурируются отдельно от контроллера с использованием команды **interface serial**.

Для указания коммутатора ISDN, к которому подсоединяется интерфейс PRI, следует использовать команду **isdn switch-type**. Как и для BRI-интерфейса, эта команда может быть введена в глобальном режиме или в режиме конфигурирования интерфейса. В табл. 14. Приведены возможные типы коммутаторов, которые могут быть использованы при конфигурировании PRI-интерфейса.

Таблица 14.6. Типы коммутаторов PRI ISDN

Тип коммутатора	Описание
primary-5ess	Коммутаторы базовой скорости компании AT&T (США)
primary-dms100	Коммутаторы DMS-100 компании Northern Telecom (Северная Америка)
primary-ni	Национальная сеть ISDN (Северная Америка)
primary-net5	Тип коммутатора для Net5 в Великобритании, других странах Европы и в Австралии
primary-ntt	Коммутатор ISDN NTT (Япония)

Конфигурирование контроллера T1 или E1 включает в себя четыре этапа описанные ниже.

- Этап 1.** В режиме глобального конфигурирования указать контроллер и порт/слот маршрутизатора, в котором находится карта PRI-интерфейса:

```
Router(config)#controller {t1 | e1} { slot/port}
```

- Этап 2.** Задать тип фрейма, кодировку линии и тип синхронизации, указанные провайдером службы. Для указания типа фрейма, используемого провайдером службы PRI, используется команда **framing**. Для линии T1 используется синтаксис команды:

```
Router(config-controller)#framing {sf | esf}
```

Для линий E1 следует использовать команду **framing** со следующими опциями:

```
Router(config-controller)#framing {crc4 | no-crc4} [australia]
```

Для задания метода сигнализации физического уровня в цифровых устройствах провайдера используется команда **linecode**:

```
Router(config-controller)#linecode {ami | b8zs | hdb3}
```

В Северной Америке для устройств оператора линии T1 используется метод сигнализации B8ZS. Он позволяет использовать полностью 64 Кбит/с для каждого канала ISDN. В Европе обычно используется кодировка hdb3.

- Этап 3.** Задать интерфейс для функционирования PRI и количество фиксированных тайм-слотов, выделенных на цифровом оборудовании провайдера:

```
Router(config-controller)#pri-group [timeslots range]
```

Для линии T1 диапазон используемых тайм-слотов составляет 1-24; для линии E1, он равен 1-31.

- Этап 4.** Указать интерфейс для работы D-канала PRI-интерфейса. Этим интерфейсом является интерфейс маршрутизатора к линиям T1/E1.

```
Router(config)#interface serial { slot/port: / unit:} {23 | 15}
```


Для оборудования линий E1 or T1 нумерация каналов начинается с единицы (1-31 для E1 и 1-24 для T1). Нумерация последовательных интерфейсов на маршрутизаторах Cisco начинается с нуля. Соответственно, 16-й канал, т.е. канал сигнализации линии E1, является 15-м подынтерфейсом последовательного порта. Канал 24, канал сигнализации линии T1, становится последовательным подынтерфейсом 23. Следовательно, команда **interface serial 0/0:23** относится к D-каналу PRI-интерфейса линии T1.

Подынтерфейсы, которые обычно используются в протоколе Frame Relay, обозначаются точкой. Например, обозначение S0/0.16 указывает на подынтерфейс. Не следует путать каналы линий T1 или E1 с подынтерфейсами. В обозначениях каналов используется не точка, а двоеточие, например:

- S0/0.23 относится к подынтерфейсу;
- S0/0:23 относится к каналу.

После того, как маршрутизация DDR (или пользователь) создает сквозной маршрут по сети ISDN, для передачи данных требуется какой-либо метод инкапсуляции дейтаграмм. Возможными типами инкапсуляции для ISDN являются:

- протокол PPP;
- протокол HDLC;
- протокол Frame Relay;
- сбалансированный протокол доступа к каналу (*Link Access Protocol, Balanced — LAPB*);
- фирменный протокол Combinet (*Combinet Proprietary Protocol — CPP*).

Протокол LAPB также может быть использован для доставки дейтаграмм по D-каналу. Как отмечалось ранее в настоящей главе, наиболее вероятным является использование в качестве протокола 2-го уровня протокола PPP. Для задания типа инкапсуляции на интерфейсе ISDN используется команда **encapsulation**:

```
Router(config-if)#encapsulation [ppp | labp | hdlc | x25 | cpp]
```

Если конфигурируется инкапсуляция протокола PPP, то при получении вызовов более чем из одного источника удаленного доступа необходимо использовать протокол аутентификации по паролю (*Password Authentication Protocol — PAP*) или протокол аутентификации с предварительным согласованием вызова (*Challenge Handshake Authentication Protocol — CHAP*). В примере 14.4 показано типовое конфигурирование PPP-инкапсуляции BRI с использованием протокола CHAP.

Пример 14.4. Пример инкапсуляции BRI

```
Router(config)#interface bri 0
Router(config-if)#encapsulation ppp
Router(config-if)#ppp authentication chap
```

Тестирование конфигурации ISDN

Команда **show** используется для проверки того, что конфигурация ISDN функционирует соответствующим образом:

```
Router#show isdn status
Router#show interfaces bri0/0
Router#show isdn active
```

Для подтверждения операций интерфейса BRI следует использовать команду **show isdn status** для выяснения статуса BRI-интерфейсов. Эта команда может использоваться после конфигурирования BRI ISDN для проверки того, что TEI (маршрутизатор) корректно осуществляет связь с коммутатором ISDN. Вывода в примере 14.5 показывает, что TEI были успешно обсуждены и 3-й уровень ISDN (сквозной) готов принимать вызовы или осуществлять их.

Пример 14.5. Команда show isdn status

```
Cork#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
dsl 0, interface ISDN Switchtype = basic-ni
Layer 1 Status:
ACTIVE
Layer 2 Status:
TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
TEI = 65, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
Spid Status:
TEI 64, ces = 1, state = 5(init)
spid1 configured, no LDN, spid1 sent, spid1 valid
Endpoint ID Info: epsf = 0, usid = 70, tid = 1
TEI 65, ces = 2, state = 5(init)
spid2 configured, no LDN, spid2 sent, spid2 valid
Endpoint ID Info: epsf = 0, usid = 70, tid = 2
Layer 3 Status:
0 Active Layer 3 Call(s)
Activated dsl 0 CCBs = 0
The Free Channel Mask: 0x80000003
Total Allocated ISDN CCBs = 0
```

PRI конфигурировании BRI ISDN требуется вводить команды как в глобальном режиме, так и в режиме конфигурирования интерфейса. Для конфигурирования типа коммутатора ISDN следует войти в режим глобального конфигурирования и выполнить команду **isdn switch-type switch-type**, как показано в примере 14.6.

Пример 14.6. Частичное конфигурирование ISDN

```
Router(config)# isdn switch-type basic-ni
!
<Output Omitted>
!
interface BRI0/0
isdn switch-type basic-ni
isdn spid1 51055540000001 5554000
isdn spid2 51055540010001 5554001
```

Следует удостовериться в том, что состояние 1-го уровня является активным (ACTIVE), а для 2-го уровня появляется сообщение о состоянии MULTIPLE_FRAME_ESTABLISHED. Эта команда также отображает количество активных вызовов.

Команда **show isdn active** отображает информацию о текущем вызове, включая вызываемый номер, время активности вызова до отсоединения, рекомендация загрузки (advice of charge — АОС), загрузка модулей во время вызова, и выбор момента предоставления информации АОС — во время вызова или в конце всех вызовов.

Команда **show dialer** отображает информацию об интерфейсе номеронабирателя. Эта информация включает в себя состояние вызова, значение таймера длительности удаленного вызова, причин вызова и подсоединенное удаленное устройство.

Команда **show interfaces bri0/0** отображает статистику для BRI-интерфейса, сконфигурированного на маршрутизаторе. Для вывода информации о конкретном канале в конце команды следует ввести его номер. В приводимом ниже выводе по команде **show interfaces bri0/0:1** показано, что В-канал использует инкапсуляцию протокола PPP, параметры LCP были согласованы и открыты и работают два протокола управления сетью (Network Control Protocol): IP-протокол управления (Control Protocol — IPCP) и протокол управления CDP (CDP Control Protocol — CDPCCP).

В примере 14.7 приведен вывод по этой команде на BRI-интерфейсе.

Пример 14.7. Команда show interfaces bri0/0

```
BranchF#show interface bri0/0: 1 2
BRI0:1 is up, line protocol is up
Hardware is BRI
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input 00:00:01, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/1/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
82 packets input, 2844 bytes, 0 no buffer
Received 82 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
82 packets output, 2838 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
5 carrier transitions
(output omitted)
```

Устранение ошибок в конфигурации ISDN

Ниже приводятся команды, используемые для отладки конфигурации ISDN и устранения в ней ошибок.

- **debug isdn q921** — отображает сообщения канального (2-го) уровня в D-канале между маршрутизатором и коммутатором ISDN. Эту команду отладки следует использовать в том случае, если команда **show isdn status** не показывает информации о 1-м и 2-м уровнях.

- **debug isdn q931** — отображает обмен сообщениями об установке вызова и его прекращении для соединения в сети ISDN (3-й уровень).
- **debug ppp authentication** — отображает сообщения аутентификации протокола PPP, включая обмен пакетами CHAP и обмены протокола PAP.
- **debug ppp negotiation** — отображает информацию о передаче данных протокола PPP и об обменах при обсуждении компонент протокола PPP, включая протокол управления каналом (link control protocol — LCP), аутентификацию и протокол управления сетью (Network Control Protocol). В случае успешного обсуждения протокола PPP устанавливается активный статус протокола LCP, выполняется аутентификация, а затем обсуждаются параметры протокола управления сетью.
- **debug ppp error** — отображает ошибки протокола и статистику ошибок, связанных с обсуждением соединения PPP и его функционированием.

Маршрутизация DDR

Под маршрутизацией DDR понимается набор функций Cisco IOS, который позволяет двум или более маршрутизаторам установить динамическое соединение по простой сети удаленного доступа. Маршрутизация DDR используется для установки периодических соединений с небольшим объемом передачи данных через сеть ISDN или PSTN. Она также позволяет при необходимости осуществлять обмен сообщениями об обновлении маршрутов, хотя чаще всего применяется статическая маршрутизация.

Традиционно для связи двух узлов используются выделенные линии распределенных сетей WAN, которые финансово эффективны лишь в том случае, если соединение используется в течение значительного времени дня. Маршрутизация DDR удовлетворяет потребность в периодических соединениях по сети с использованием службы коммутации каналов. Гибкость DDR проявляется в том, что она позволяет осуществлять соединения с несколькими конечными точками и использует WAN-соединения только при необходимости, что сокращает расходы, связанные с сетью WAN.

При использовании DDR маршрутизатор подсоединяется к сети в том случае, когда имеются данные для передачи и отсоединяется от сети после завершения передачи этих данных (рис. 14.13).

Маршрутизация DDR обычно используется в следующих ситуациях:

- когда телеработникам в течение рабочего дня требуется периодически подключаться к корпоративной сети предприятия;
- когда удаленным офисам периодически требуется отправлять небольшие объемы данных — такие как коммерческие транзакции или запросы о состоянии депозитов, главному компьютеру в центральном офисе;
- в тех случаях, когда пользователи используют автоматическую систему заказов;
- при периодическом получении электронной почты от Internet-провайдера по расписанию.

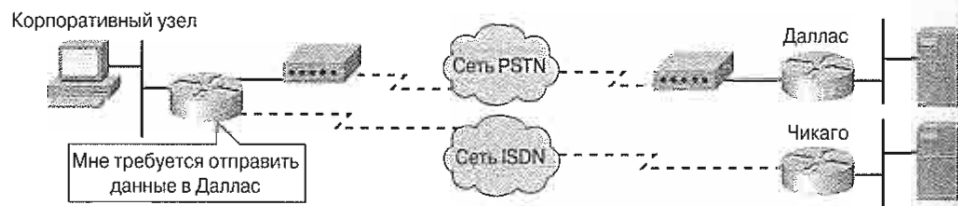


Рис. 14.13. Маршрутизация DDR

Функционирование маршрутизации DDR

Работа маршрутизации DDR начинается при получении требуемых данных на интерфейсе, на котором она сконфигурирована. Если эти данные “представляют интерес”, то инициируется вызов. Такие “вызывающие интерес” данные могут определяться как IP-данные определенного протокола, пакеты от источника с заданным адресом или пунктом назначения или другими критериями.

Задание критериев, согласно которым данные определяются как “представляющие интерес”, осуществляется сетевым администратором. Вызов прекращается после того как представляющие интерес данные переданы и истек интервал холостого хода.

Ключевым фактором эффективного функционирования маршрутизации DDR является определение данных, представляющих интерес. Имеется несколько способов определения таких представляющих интерес данных с использованием списков номеронабирателя или списков доступа. Даже данные, которые не являются представляющими интерес, могут быть пересланы если соединение с пунктом их назначения является активным.

Реализация маршрутизации DDR на маршрутизаторах Cisco включает в себя несколько этапов, описанных ниже.

Этап 1. Маршрутизатор получает данные, просматривает свою таблицу маршрутизации для выяснения того, имеется ли там маршрут к пункту назначения и определяет выходной интерфейс.

Этап 2. Если на выходном интерфейсе сконфигурирована маршрутизация DDR, то маршрутизатор проверяет, являются ли данные “представляющими интерес”. Сетевой администратор должен заранее определить какие данные относятся к этому типу.

Этап 3. Маршрутизатор анализирует информацию номеронабирателя, которая необходима для осуществления вызова с использованием преобразования адресов и получения доступа к маршрутизатору следующего перехода.

Этап 4. После этого маршрутизатор проверяет, используется ли в данный момент это преобразование адресов. Если данный интерфейс в настоящее время подсоединен к требуемому удаленному получателю, то передача данных считается разрешенной. После установки соединения любой поток данных к этому получателю считается разрешенным, однако только данные представляющие интерес переустанавливают таймер холостого хода. Если в настоящий момент интерфейс не подсоединен к требуемому удаленному получателю, то маршрутизатор посылает информацию об установке вызова через BRI-интерфейс с использованием D-канала. После актив-

зации данного канала маршрутизатор передает как данные, представляющие интерес, так и данные, которые таковыми не являются. Последний тип данных может включать в себя обычные данные и сообщения об обновлениях маршрутизации.

Этап 5. Таймер холостого хода начинает работать, если в течение заданного для него интервала не поступают данные, представляющие интерес, и отключает вызов согласно заданной для него конфигурации. Это процесс показан на рис. 14.14.



Рис. 14.14. Общий характер функционирования маршрутизации DDR

Унаследованная DDR

Термин “унаследованная DDR” используется для определения базовых конфигураций DDR, в которых отдельный комплект параметров набора применяется к одному интерфейсу. Если на интерфейсе требуется использовать несколько конфигураций набора, то следует использовать профили набора.

Для того, чтобы сконфигурировать унаследованную DDR, необходимо выполнить следующие действия.

Этап 1. Определить статические маршруты.

Этап 2. Задать критерии для данных, представляющих интерес.

Этап 3. Сконфигурировать информацию номеронабирателя.

Задание статических маршрутов для DDR

Для того, чтобы стала возможной пересылка данных, маршрутизатор должен знать, какой маршрут следует использовать к данному пункту назначения. При использовании протокола динамической маршрутизации интерфейс DDR набирает номер удаленного узла для каждого обновления маршрутизации или сообщения приветствия, если эти пакеты определены как представляющие интерес. Для предотвращения частой или постоянной активизации канала DDR, что является необходимым для поддержки протокола динамической маршрутизации, необходимые маршруты следует сконфигурировать статическим образом. Для задания статического маршрута используется следующая команда:

```
Router(config)#ip route net-prefix mask { address | interface } [ distance ] [permanent]
```

На рис. 14.15 показан центральный маршрутизатор (Central router), определяющий статический маршрут к локальной сети LAN (10.40.0.0) домашнего маршрутизатора


```

!
no ip classless
ip route 10.10.0.0 255.255.0.0 10.1.0.2
ip route 10.20.0.0 255.255.0.0 10.1.0.2
!
dialer-list 1 protocol ip permit

```

Необходимо связать список номеронабирателя, определяющий для данного DDR-интерфейса данные, представляющие интерес, с интерфейсом DDR. Это можно сделать с помощью команды **dialer-group group-number**, как показано в примере 14.10.

Пример 14.10: Команда dialer-group group-number

```

Home(config-if)#dialer-group 1
Home#show running-config
hostname Home
!
isdn switch-type basic-5ess
!
username central password cisco
interface BRI0
ip address 10.1.0.1 255.255.255.0
encapsulation ppp
dialer idle-timeout 180
dialer map ip 10.1.0.2 name Central 5552000
dialer-group 1
no fair-queue
ppp authentication chap
!
router rip
network 10.0.0.0
!
no ip classless
ip route 10.10.0.0 255.255.0.0 10.1.0.2
ip route 10.20.0.0 255.255.0.0 10.1.0.2
!
!
dialer-list 1 protocol ip permit

```

В этой команде параметр **group-number** задает номер группы номеронабирателя, к которой принадлежит данный интерфейс. Номер группы может быть целым числом в диапазоне от 1 до 10. Этот номер должен соответствовать параметру **group-number** списка номеронабирателя. Каждый интерфейс может иметь только одну группу номеронабирателя, однако один и тот же список номеронабирателя может быть назначен нескольким интерфейсам (с помощью команды **dialer-group**).

Для удаленного DDR-интерфейса должна быть указана корректная информация набора. Это можно сделать с помощью команды **dialer map**, как показано на рис. 14.16.

Команда **dialer map** преобразует удаленный протокольный адрес в телефонный номер. Эта команда необходима для вызова к нескольким узлам:

```

Router(config-if)#dialer map protocol next-hop-address[name hostname]
[ speed 56 | 64 ] [ broadcast ] dial-string

```

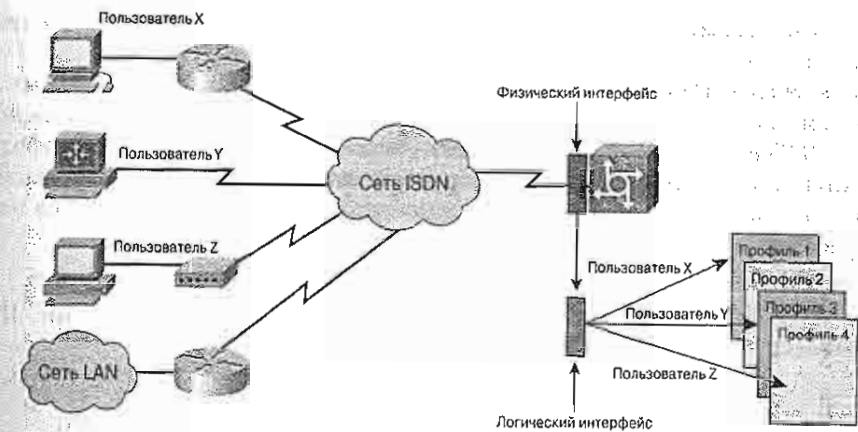


Рис. 14.16. Преобразование номера

Если вызывается только один узел, то следует использовать команду безусловного набора строки вызова, при этом набирается один телефонный номер независимо от пункта назначения для данных; этот этап уникален для унаследованной DDR. Хотя эта информация требуется всегда, этапы конфигурирования информации получателя в случае использования профилей номеронабирателя отличаются от тех, которые выполняются для унаследованной DDR.

Для задания количества секунд холостого хода перед отключением вызова используется команда **dialer idle-timeout seconds**. Параметр **seconds** указывает количество секунд до отсоединения вызова после отправки последнего пакета, представляющего интерес. По умолчанию это значение равно 120.

Лабораторная работа: конфигурирование унаследованной DDR

В этой лабораторной работе требуется сконфигурировать маршрутизатор ISDN для осуществления вызова унаследованной DDR к другому маршрутизатору с функциями ISDN. Для имитации среды коммутатор/ISDN используется эмулятор ISDN Adtran Atlas550. Канал активизируется только при получении данных протокола HTTP.

Профили набора

С унаследованной DDR связан ряд ограничений, поскольку конфигурация применяется непосредственно к интерфейсу. Это означает, что существует взаимно однозначное соответствие между двумя интерфейсами DDR на разных концах канала. Если IP-адрес применяется непосредственно к интерфейсу, то лишь те интерфейсы, которые сконфигурированы в данной конкретной подсети, могут установить соединение DDR с этим интерфейсом.

Профили набора удаляют конфигурацию с интерфейса, который принимает вызовы или осуществляет их и связывает конфигурацию с интерфейсом для каждого конкретного вызова. Это позволяет физическим интерфейсам динамически устанавливать свои характеристики в зависимости от требований входного или выходного вызова. Профили набора могут определять тип инкапсуляции и списки управ-

ления доступом, задавать минимальное или максимальное количество вызовов, также включать и отключать некоторые функции.

Профили набора помогают в проектировании и реализации более сложных и масштабируемых объединенных сетей с коммутацией каналов путем реализации новой модели DDR на маршрутизаторах доступа Cisco и на серверах доступа. профили набора отделяют логическую составляющую DDR, сетевой уровень, инкапсуляцию и параметры набора от физического интерфейса, который осуществляет вызов или принимает вызов.

Используя профили набора можно решить следующие задачи:

- сконфигурировать В-каналы на интерфейсе ISDN с различными IP-подсетями;
- использовать различные типы инкапсуляции на В-каналах интерфейса ISDN;
- установить различные параметры DDR на В-каналах интерфейса ISDN;
- устранить нерациональное использование В-каналов ISDN, предоставив BRI-интерфейсам ISDN возможность принадлежать к нескольким пулам набора.

Профиль набора состоит из следующих элементов.

- **Интерфейс набора номера (Dialer interface)** — логическое устройство, использующее профиль набора для каждого конкретного получателя.
- **Пул номеров набора (Dialer pool)** — каждый интерфейс набора относится к некоторому пулу набора, представляющему собой группу из одного или более физических интерфейсов, связанных с профилем набора.
- **Физические интерфейсы (Physical interfaces)** — интерфейсы в пуле набора конфигурируются для требуемых параметров инкапсуляции и для идентификации пулов набора, к которым принадлежит данный интерфейс. Тип инкапсуляции, аутентификация протокола PPP и многоканальный PPP конфигурируются на физическом интерфейсе.

Представляющий интерес пакет пересылается на удаленный IP-адрес DDR. Маршрутизатор просматривает сконфигурированные интерфейсы набора в поисках такого, который находится в той же подсети, в какой и удаленный IP-адрес DDR. Если такой существует, то маршрутизатор ищет в пуле набора неиспользуемый физический интерфейс DDR. После этого к интерфейсу применяется конфигурация из профиля набора и маршрутизатор пытается создать соединение DDR. После окончания соединения интерфейс возвращается в пул набора для осуществления следующего вызова.

Конфигурирование профилей набора

На маршрутизаторе могут быть сконфигурированы несколько интерфейсов набора. Каждый интерфейс набора связан с полной конфигурацией вызова к какому-либо получателю. При вводе команды **interface dialer** создается интерфейс набора и происходит переход в режим конфигурирования интерфейса. Для того, чтобы сконфигурировать интерфейс набора номера, необходимо выполнить следующие действия.

Этап 1. Сконфигурировать один или более интерфейсов набора с помощью базовых команд DDR и задать такие параметры как IP-адрес, тип инкапсуляции и аутентификацию, интервал таймера простоя и группу набора для данных, представляющих интерес.

Этап 2. Сконфигурировать строку набора номера и имя удаленного номеронабирателя для указания имени удаленного маршрутизатора и телефонного номера, который требуется к нему набирать. Пул набора связывает этот логический интерфейс с пулом физических интерфейсов.

Этап 3. Сконфигурировать физические интерфейсы и включить их в пул набора с помощью команды **dialer pool-member**. С помощью этой команды интерфейс может быть включен в несколько пулов набора для указания нескольких номеров пула набора. Если в пуле имеется более одного физического интерфейса, то следует использовать опцию приоритетности команды **dialer pool-member** для установки приоритета интерфейса в пуле набора. Этот приоритет используется только для исходящих вызовов.

С пулами набора можно использовать комбинацию синхронных, последовательных интерфейсов, интерфейсов BRI и PRI ISDN.

Тестирование конфигурации DDR

По команде **show dialer interface** отображается информация в том же формате, в каком отображается статистика унаследованной DDR для входящих и исходящих вызовов. Появление сообщения “Состояние набора: канальный уровень активизирован” (“Dialer state is data link layer up”) означает, что номеронабиратель функционирует нормально, а интерфейс, связанный с профилем Dialer1, свидетельствует о том, что интерфейс bri0 связан с профилем набора Dialer1, как это показано в выводе по этой команде в примере 14.11.

Пример 14.11. Команда show dialer interface

```
Router# show dialer interface bri 0
BRI0 - dialer type = ISDN
Dial String Successes Failures Last called Last status
0 incoming call(s) have been screened.
BRI0: B-Channel 1
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Dial reason: ip (s=10.1.1.8, d=10.1.1.1)
Interface bound to profile Dialer0
Time until disconnect 102 secs
Current call connected 00:00:19
Connected to 5773872 (wolfman)
BRI0: B-Channel 2
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is idle
```

По команде **show isdn active** отображается информация о текущих активных вызовах ISDN (образец вывода показан в примере 14.12.). В этом выводе вызов ISDN направлен удаленному маршрутизатору с именем Seattle.

Пример 14.12. Команда show isdn active

```
Phoenix#show isdn active
```

```
-----
ISDN ACTIVE CALLS
-----
```

```
History table has a maximum of 100 entries.
History table data is retained for a maximum of 15 Minutes.
-----
```

```
Call Calling Called Remote Seconds Seconds Seconds Charges
Type Number Number Name Used Left Idle Units/Currency
-----
```

```
Out 5551000 Seattle 87 41 78 0
-----
```

Команда **show isdn status** отображает информацию о трех уровнях BRI-интерфейса. В этом выводе 1-й уровень ISDN является активным, 2-й уровень установлен с действующими идентификаторами SPID1 и SPID2, а на 3-м уровне имеется одно активное соединение.

Для обнаружения проблем с конфигурацией DDR используется группа команд **debug**.



Лабораторная работа: конфигурирование профилей набора

В этой лабораторной работе требуется сконфигурировать на маршрутизаторах профили набора. Это позволяет одновременно осуществлять DDR-вызов с двух удаленных маршрутизаторов на центральный BRI-маршрутизатор ISDN. Для имитации среды коммутатор/ISDN используется эмулятор Adtran Atlas550 ISDN.

Резюме

В настоящей главе были рассмотрены приведенные ниже основные положения, связанные с технологией ISDN и маршрутизацией DDR.

- Технология ISDN предоставляет возможность интегрированной передачи голосовых и обычных данных по общедоступной телефонной сети.
- Компоненты ISDN включают в себя терминалы, терминальные адаптеры, NT-устройства и коммутаторы ISDN.
- Контрольные точки ISDN (R, S, T и U) определяют логические интерфейсы между функциональными группами, такими как адаптеры TAs и устройства NT1.
- Набор стандартов ITU-T описывает технологию ISDN и ее связь с физическим, канальным и сетевым уровнем эталонной модели OSI.
- Двумя наиболее часто используемыми видами инкапсуляции для ISDN являются протоколы PPP и HDLC.

- Технология ISDN имеет много применений, включая удаленный доступ, удаленные узлы и соединения SOHO.
- Имеются две службы ISDN: интерфейсы BRI и PRI.
- Интерфейс BRI ISDN обеспечивает общую полосу пропускания 144 Кбит/с по трем отдельным каналам и доступную для пользователя полосу пропускания 128 Кбит/с.
- Конфигурирование службы BRI включает в себя конфигурирование BRI-интерфейса, типа коммутатора ISDN и идентификаторов SPID.
- Маршрутизация DDR устанавливает соединения с коммутацией каналов при необходимости и освобождает их после передачи данных.

В дополнение к материалу, изложенному в настоящей главе, рекомендуется ознакомиться с относящимися к ней лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

2B+D. В контексте службы BRI ISDN — два В-канала и один D-канал.

В-канал, канал-носитель (Bearer Channel — B channel). В ISDN-сетях дуплексный канал с пропускной способностью 64-Кбит/, используемый для передачи пользовательских данных.

D-канал, дополнительный канал, дельта-канал, канал управления скоростью передачи (Delta Channel — D channel). Дуплексный ISDN-канал с пропускной способностью 16-Кбит/с (для BRI) или 64-Кбит/с (для PRI).

Q 931. Протокол, который описывает сетевой уровень между оконечной точкой и локальным ISDN-коммутатором. Не накладывает ограничений на непосредственные соединения оконечных точек. Разные ISDN-провайдеры могут использовать различные реализации этого протокола.

Идентификатор профиля службы (Service Profile Identifier — SPID). Число, используемое некоторыми провайдерами услуг для определения служб, к которым подключено абонентское ISDN-устройство. SPID используется ISDN-устройством во время доступа к коммутатору, который инициализирует соединение с провайдером услуг.

Интерфейс базовой скорости (Basic Rate Interface — BRI). ISDN-интерфейс, состоящий из двух В-каналов и одного D-канала для канально-коммутируемой передачи голоса, видео и других данных.

Интерфейс первичной скорости (основного уровня) (Primary Rate Interface — PRI). ISDN-интерфейс для основного доступа. Состоит из одного D-канала (64 Кбит/с) и двенадцати трех (для T1) или 30 (для E1) В-каналов для голоса или данных.

Интерфейс типа "пользователь-сеть" (User-Network Interface — UNI). Спецификация, определяющая стандарты взаимодействия для интерфейса между устройствами (маршрутизаторами или коммутаторами), расположенными в частной сети, и коммутаторами общедоступных сетей. Также используется для описания сходных соединений в сетях Frame Relay.

Оборудование заказчика (Customer Premises Equipment — CPE). Оконечное оборудование, такое как терминалы, телефоны и модемы, поддерживаемые телефонной

компаниями, установленные на территории клиента этой компании и подключенное к ее сети.

Процедура доступа к D-каналу (Link Access Procedure — LAPD). В сетях ISDN протокол канального уровня для D-канала. LAPD получен из LAPB и разработан, в основном, для удовлетворения требований сигнализации базового доступа ISDN. Определяется в соответствии с рекомендациями ITU-T (International Telecommunications Union, Международный телекоммуникационный союз) Q.920 и Q.921.

Сбалансированный протокол доступа к каналу связи (Link Access Procedure, Balanced — LAPB). Протокол канального уровня в наборе протоколов X.25. LAPB — бит-ориентированный протокол, являющийся частью протокола HDLC.

Сетевая нагрузка 1-го типа (Network Termination Type 1 — NT1). Устройство, соединяющее четырех проводного абонента и стандартное двухпроводное устройство местной линии.

Сетевая нагрузка 2-го типа (Network Termination Type 2 — NT2). Устройство, направляющее поток данных между разными абонентскими устройствами и NT1. NT2 является интеллектуальным устройством, которое осуществляет коммутацию и концентрацию.

Контрольная точка (Reference Point). Спецификация, которая определяет соединения между специфическими устройствами в зависимости от их функций в непосредственном соединении.

Терминальное оборудование 1-го типа (Terminal Equipment Type 1 — TE1). Устройство, совместимое с ISDN-сетью. TE1 подключается к сетевой нагрузке 1-го, либо 2-го типа.

Терминальное оборудование 2-го типа (Terminal Equipment Type 2 — TE2). Устройство, не совместимое с ISDN-сетью и требующее использования терминального адаптера.

Терминальный адаптер (Terminal Adapter — TA). Устройство, используемое для подсоединения основных интерфейсов ISDN к существующим интерфейсам, таким как EIA/TIA-232. Как правило, представляет собой ISDN-модем.

Цифровая сеть интегрированных служб (Integrated Services Digital Network — ISDN). Коммуникационный протокол, предложенный телефонными компаниями, который позволяет передавать информацию по телефонным сетям, в том числе голосовые данные, а также данные, полученные из других источников.

Контрольные вопросы

1. По какому каналу ISDN передаются данные?
 - A. По каналу носителя со скоростью 16 Кбит/с
 - B. По дельта-каналу со скоростью 16 Кбит/с
 - C. По каналу носителя со скоростью 64 Кбит/с
 - D. По дельта-каналу со скоростью 64 Кбит/с
2. Какой канал используется в ISDN для внеполосной сигнализации?
 - A. Канал передачи данных
 - B. Канал носителя
 - C. Локальное ответвление
 - D. Дельта-канал

3. Каким является первое динамически назначаемое значение TEI?
 - A. 64
 - B. 127
 - C. 0
 - D. 1
4. Какой механизм используется для передачи управляющей информации вызова между двумя коммутаторами ISDN?
 - A. D-канал
 - B. SS7
 - C. B-канал
 - D. Протокол Q.921
5. Для чего в первую очередь используется D-канал при обработке вызова ISDN?
 - A. Для передачи данных
 - B. Для передачи голосовых данных
 - C. Для передачи видеоданных
 - D. Для сигнализации вызовов
6. Какой из приведенных ниже интерфейсов требуется в Северной Америке в качестве сервера удаленного доступа, использующего BRI ISDN?
 - A. Интерфейс E1 PRI ISDN
 - B. U-интерфейс BRI ISDN
 - C. Интерфейс T1 PRI ISDN
 - D. Интерфейс S/T BRI ISDN
7. О чем свидетельствует наличие на маршрутизаторе U-интерфейса?
 - A. Он имеет встроенное устройство TA
 - B. Он имеет встроенное устройство TE1
 - C. Он имеет встроенное устройство NT1
 - D. Он имеет встроенное устройство BRI
8. Какой из приведенных ниже типов коммутаторов используется в BRI-соединениях в Европе?
 - A. Net3
 - B. Net5
 - C. Northern Telecom DMS-100
 - D. VN3
9. Кто из приведенных ниже предоставляет идентификаторы SPID?
 - A. Изготовитель маршрутизатора
 - B. Коммутатор ISDN
 - C. Оператор ISDN
 - D. Сетевой администратор

10. Для чего используется DDR?
- A. Для регулярных соединений по сети Frame Relay с небольшим объемом передаваемых данных
 - B. Для регулярных соединений по сети ISDN с небольшим объемом передаваемых данных
 - C. Для постоянных соединений по сети ISDN с небольшим объемом передаваемых данных
 - D. Для соединений по сети ISDN с большим объемом передачи
11. Какое из приведенных ниже утверждений относительно DDR неверно? (Выбрать четыре)
- A. DDR подсоединяет маршрутизатор к сети удаленного доступа
 - B. DDR создает постоянные соединения между двумя узлами.
 - C. DDR позволяет маршрутизатору осуществлять соединение только с одной конечной точкой.
 - D. DDR сокращает расходы на сеть WAN при небольшом объеме передачи.
 - E. DDR целесообразно применять в случае наличия постоянного WWW-сервера.
 - F. DDR используется только с ISDN.
12. Каково главное ограничение унаследованной DDR (Legacy DDR)?
- A. Не поддерживается аутентификация PPP
 - B. Требуется использовать преобразования номеров
 - C. Конфигурация применяется непосредственно к физическому интерфейсу.
 - D. Применение Legacy DDR ограничено IP-приложениями



В этой главе...

- Описаны службы, стандарты и компоненты протокола Frame Relay
- Рассмотрены функции интерфейса локального управления (Local Management Interface — LMI)
- Описаны подынтерфейсы протокола Frame Relay
- Описано базовое конфигурирование протокола Frame Relay

Протокол Frame Relay

Ранее были описаны две технологии распределенных сетей: протокол “точка-точка” (Point-to-Point Protocol — PPP) и цифровая сеть интегрированных служб (Integrated Services Digital Network — ISDN), которые используются с целью установки связи для пользователей, которым требуется получить доступ к другим географически удаленным сетевым устройствам. В настоящей главе рассматривается другой тип технологии распределенных сетей, *Frame Relay*, который также используется в этих целях.

В ней описываются службы, стандарты, компоненты и функционирование протокола Frame Relay. Кроме того, в этой главе описано конфигурирование служб протокола Frame Relay и команды, используемые для тестирования и поддержки установленных соединений.

Рекомендуется выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Обзор протокола Frame Relay

Протокол Frame Relay представляет собой стандарт Консультативного комитета по международной телефонии и телеграфии (Consultative Committee for International Telegraph and Telephone, CCITT, в настоящее время — отдел стандартизации при международном телекоммуникационном союзе, ITU-T) и Американского национального института стандартов (American National Standards Institute, ANSI), описывающий процесс передачи данных по *общедоступным сетям данных (public data network — PDN)*. Эта сетевая технология канального уровня была создана для обеспечения высокопроизводительной и эффективной связи в сетях всего мира. Протокол Frame Relay предоставляет возможность пересылать информацию по сети WAN, разделяя ее на отдельные пакеты. Каждый пакет проходит через ряд коммутаторов сети Frame Relay и доставляется получателю. Протокол Frame Relay действует на физическом и канальном уровнях эталонной модели OSI, но для коррекции ошибок использует протоколы верхних уровней, такие как TCP.

Протокол Frame Relay первоначально планировалось использовать на интерфейсах ISDN. В настоящее время этот протокол является стандартным промышленным коммутируемым протоколом канального уровня, используемым для работы с различными виртуальными каналами с использованием инкапсуляции протокола управления каналом высокого уровня (High-Level Data Link Control — HDLC) для

обмена данными между соединенными устройствами. Протокол Frame Relay использует виртуальные каналы для установки соединений через ориентированную на соединение службу.

Сеть, обеспечивающей интерфейс протокола Frame Relay, может быть как общедоступная сеть одного из национальных операторов связи или сеть, обслуживающая отдельное предприятие, оборудование которой принадлежит частному владельцу. Протокол Frame Relay обеспечивает пакетно-коммутируемый обмен данными, который происходит по интерфейсу между устройствами пользователя (такими как маршрутизаторы, мосты и хосты) и сетевым оборудованием (таким как узлы коммутации Frame Relay). Как было сказано ранее, устройства пользователя часто называются оборудованием терминала данных (data terminal equipment, DTE), а сетевое оборудование, взаимодействующее с DTE, называется оконечным оборудованием канала данных (data circuit-terminating equipment — DCE) (рис. 15.1).

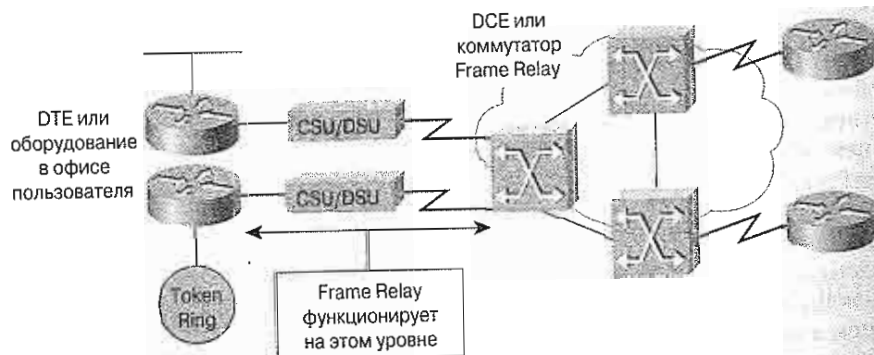


Рис. 15.1. Устройства пользователя

Терминология протокола Frame Relay

Соединение между двумя устройствами DTE в сети Frame Relay называется логическим соединением или виртуальным каналом VC. Виртуальные каналы могут устанавливаться динамически, путем отправки сигнальных сообщений в сеть. В этом случае они называются коммутируемыми виртуальными каналами (Switched Virtual Circuit — SVC), однако такой способ не является типичным. Обычно используются постоянные виртуальные каналы (Permanent Virtual Circuit — PVC), которые конфигурируются до начала работы сети. Информация о коммутации для виртуальных каналов хранится в памяти коммутатора.

Поскольку этот протокол изначально предназначался для работы на высококачественных цифровых линиях, он не имеет механизмов исправления ошибок при передаче. Как и в технологии локальных сетей (Local-Area Network — LAN) Ethernet, если во фрейме обнаруживается ошибка, то он отбрасывается без уведомления.

Устройство с интерфейсом Frame Relay, также называемое сборщиком/разборщиком (assembler/disassembler) Frame Relay или маршрутизатор, подсоединенный к сети Frame Relay, могут иметь несколько виртуальных каналов, связывающих их с различными конечными точками. Это делает технологию Frame Relay финансово эффективной заменой сеточной топологии выделенных линий, поскольку каждой конечной точке требуется лишь один короткий отрезок выделенной линии и интерфейс Frame Relay. Дополни-

тельная экономия достигается за счет того, что пропускная способность выделенной линии определяется средней потребностью в полосе пропускания для виртуальных каналов, а не максимальной полосой пропускания.

Различные виртуальные каналы на одной физической линии доступа можно отделить от друга, поскольку каждый из них имеет свой идентификатор канального соединения (Data-Link Connection Identifier — DLCI). Идентификаторы DLCI записываются в поле адреса каждого фрейма. Они имеют лишь локальное значение и могут быть различными на разных концах одного и того же VC-канала.

Ниже объясняются некоторые термины, используемые в настоящей главе при обсуждении протокола Frame Relay (рис. 15.2.).

- **Скорость локального доступа (local access rate) (скорость порта)** — скорость установки соединения локального ответвления со средой протокола Frame Relay. Она характеризует скорость поступления данных в сеть и получения данных из нее.
- **Идентификатор канального соединения (data-link connection identifier — DLCI)**. Как показано на Рис. 15.2, DLCI представляет собой номер, идентифицирующий логический канал между устройствами источника и получателя. Коммутатор протокола Frame Relay назначает DLCI каждой паре маршрутизаторов для создания постоянных виртуальных каналов.
- **Интерфейс локального управления (local management interface — LMI)** — стандарт сигналов, передаваемых между офисным оборудованием пользователя (CPE) и коммутатором протокола Frame Relay, ответственным за установку связи и поддержку состояния этих устройств. Интерфейсы локального управления могут поддерживать:
 - механизм анализа активности, проверяющий наличие передачи данных по линии;
 - механизм многоадресной передачи (multicast), предоставляющий сетевому серверу свои локальные DLCI;
 - групповую адресацию, предлагая несколько DLCI в качестве адресов для многоадресной передачи (передачи в несколько пунктов назначения);
 - изменение сферы действия DLCI путем придания своим локальным DLCI (используемым только локальным коммутатором) глобального состояния (вся сеть на базе протокола Frame Relay);
 - статусного механизма, придающего выходной статус идентификаторам локального управления, известным только данному коммутатору. Существует несколько типов LMI и поэтому маршрутизаторы должны быть проинформированы об используемом типе LMI. Поддерживаются три типа LMI: cisco, ansi и q933a.

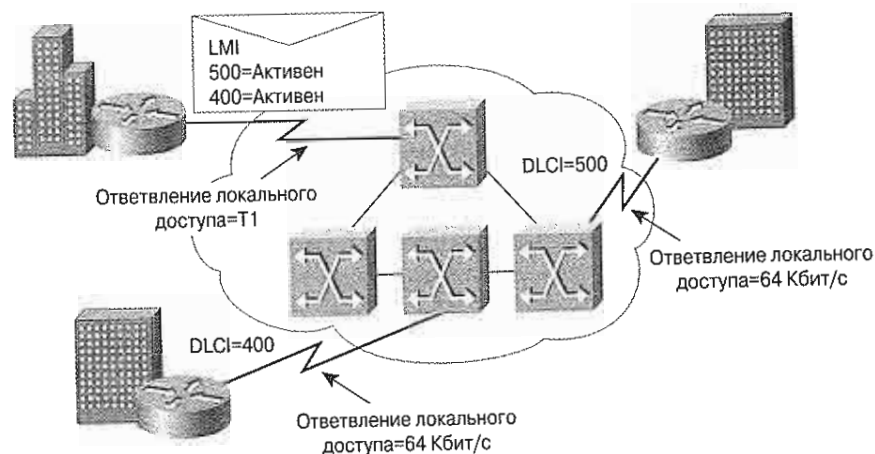


Рис. 15.2. Значение DLCI идентифицирует логическое соединение, которое мультиплексируется в физический канал

- **Согласованная скорость передачи информации (committed information rate, CIR)** представляет собой гарантируемую провайдером услуг скорость передачи в бит/с.
- **Согласованный объем** — максимальное количество битов, которое коммутатор должен передать за установленный интервал времени с согласованной скоростью.
- **Избыточный объем** — максимальное количество превышающих CIR битов, которое коммутатор протокола Frame Relay пытается передать. Это количество зависит от возможностей службы, заложенных производителем оборудования, но обычно ограничено скоростью порта локального отведения.
- **Прямое явное уведомление о перегрузке (Forward Explicit Congestion Notification — FECN).** В случае, когда коммутатор протокола Frame Relay обнаруживает в сети затор, он посылает пакет FECN устройству получателя, информируя его о заторе.
- **Обратное явное уведомление о перегрузке (Backward Explicit Congestion Notification — BECN).** Как показано на рис. 15.3, когда коммутатор протокола Frame Relay обнаруживает в сети затор, он посылает BECN-пакет маршрутизатору сети отправителя с инструкцией уменьшить скорость передачи пакетов. Если маршрутизатор получает такой пакет в текущем временном интервале, то он уменьшает скорость передачи на 25%.
- **Индикатор разрешения на отбрасывание пакетов (discard eligibility indicator — DE).** Когда маршрутизатор обнаруживает в сети затор, коммутатор Frame Relay первыми отбрасывает пакеты с установленным DE-битом. Бит DE устанавливается на пакетах избыточного потока данных (т.е. превышающего согласованную скорость передачи).

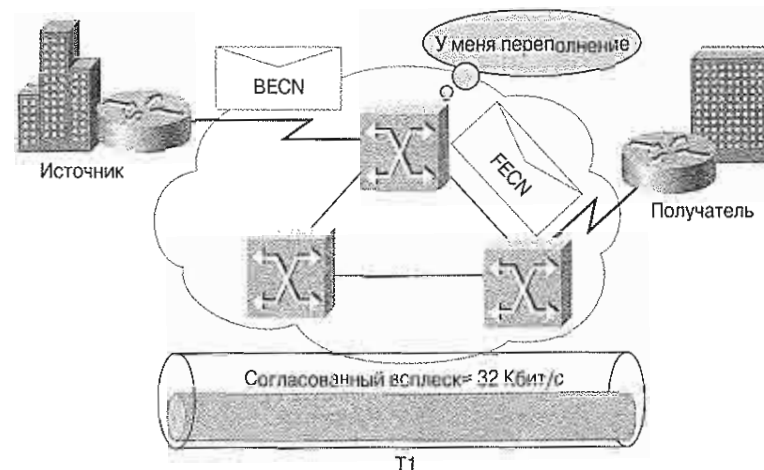


Рис. 15.3. Коммутатор протокола Frame Relay посылает BECN-пакеты маршрутизатору отправителя с целью снижения или ликвидации перегрузки в сети

Функционирование протокола Frame Relay

Протокол Frame Relay может быть использован в качестве интерфейса к службе, предоставляемой поставщиком услуг, или к сети, оборудование которой принадлежит частному владельцу. Для создания общедоступной службы на основе протокола Frame Relay коммутирующее оборудование этого протокола размещается на площадке (в центральном офисе, телефонной станции) поставщика услуг. В этом случае пользователи получают экономические преимущества за счет использования регулируемой потоком данных скорости передачи, и им не приходится тратить время и усилия на администрирование и поддержку службы и оборудования сети.

Для сетей, использующих протокол Frame Relay, не существует стандарта на оборудование, осуществляющее внутренние коммуникации. Поэтому поддержка интерфейсов протокола Frame Relay не требует обязательного использования этого протокола между сетевыми устройствами. Таким образом, как показано на рис. 15.4, могут быть использованы традиционная коммутация каналов, пакетная коммутация или комбинированный подход, объединяющий обе эти технологии.

Линии, соединяющие устройства пользователя с сетевым оборудованием, могут работать со скоростями, выбираемыми из широкого диапазона. Типичными являются скорости от 56 Кбит/с до 2 Мбит/с, хотя протокол Frame Relay может поддерживать как более высокие, так и более низкие скорости.

В качестве интерфейса между оборудованием пользователя и сетевым оборудованием (рис. 15.5), протокол Frame Relay предоставляет средства мультиплексирования при обмене данными (называемые *виртуальными каналами*, *virtual circuits*) через совместно используемую физическую среду (medium) путем назначения DLCI каждой паре устройств DCE.

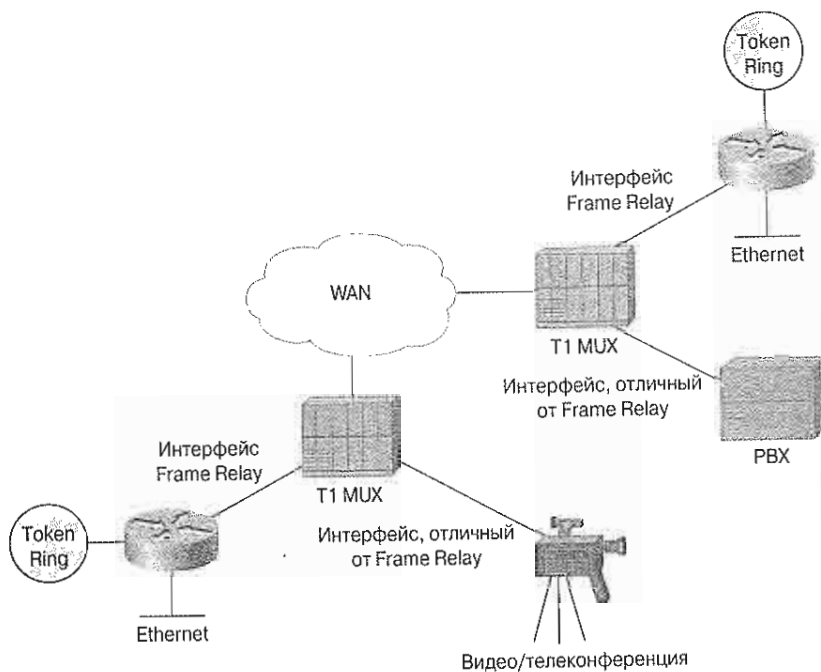


Рис. 15.4. Протокол Frame Relay может использоваться в качестве интерфейса к сети за счет соединения между собой таких устройств, как коммутаторы этого протокола и маршрутизаторы

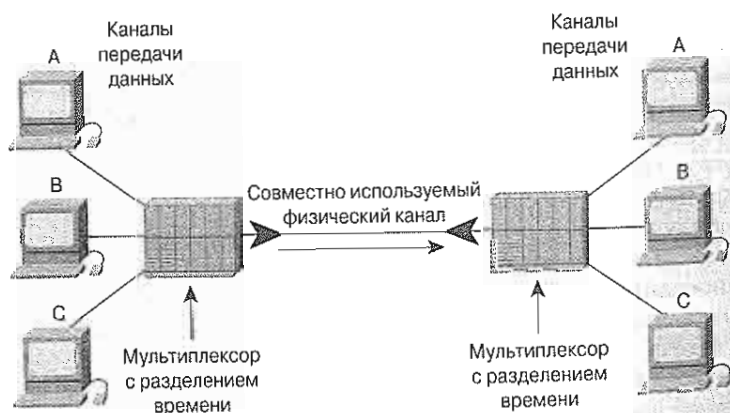


Рис. 15.5. Одно физическое соединение обеспечивает непосредственную связь со всеми устройствами сети

Мультиплексирование, осуществляемое в соответствии с протоколом Frame Relay, предоставляет более гибкий и эффективный способ использования доступной полосы пропускания. Этот протокол позволяет пользователям совместно использовать одну полосу пропускания, сокращая их финансовые расходы. Например, представим себе, что имеется распределенная сеть, использующая протокол Frame Relay. Этот протокол можно представить как группу дорог, владельцем которых являются телефонные компании,

они же занимаются их ремонтом и поддержкой. Можно арендовать дорогу (полосу) исключительно для своей компании (выделенную) или, заплатив меньше, арендовать полосу на совместно используемой дороге. Конечно, протокол Frame Relay может быть полностью реализован и в частных сетях, однако там он редко используется.

Стандарты протокола Frame Relay оговаривают параметры адресации *постоянных виртуальных каналов* (*permanent virtual circuit, PVC*), которые в сети протокола Frame Relay конфигурируются и управляются администратором. Постоянные виртуальные каналы характеризуются своими идентификаторами DLCI (рис. 15.6). DLCI протокола Frame Relay имеют локальный характер. Это означает, что их значения в распределенной сети протокола Frame Relay не являются уникальными и могут совпадать. Два устройства DTE, соединенные одним виртуальным каналом, могут использовать различные DLCI для обращения к одному и тому же соединению, как показано на рис. 15.6.

В ситуации, когда протокол Frame Relay предоставляет средства мультиплексирования логического обмена данными, коммутирующее оборудование провайдера службы сначала создает таблицу, задающую значение DLCI выходным портам. При получении фрейма коммутирующее устройство анализирует идентификатор соединения и доставляет фрейм на соответствующий выходной порт. В конечном итоге еще до отправки первого фрейма устанавливается полный путь к пункту назначения.

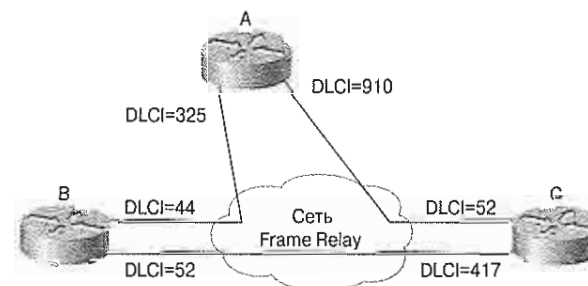


Рис. 15.6. Два конечных устройства на разных концах соединения могут использовать различные номера DLCI для обращения к одному и тому же соединению

Формат фрейма протокола Frame Relay

Формат фрейма протокола Frame Relay показан на рис. 15.7. Поля флагов указывают на начало и конец фрейма. За первым полем флага следуют два байта адресной информации: 10 битов из этих двух байтов представляют собой текущий ID канала (т.е. DLCI).

Ниже описаны поля фрейма.

- Флаг — указывает на начало и конец фрейма.
- Адрес — указывает длину адресного поля. Хотя в настоящее время адреса протокола Frame Relay имеют длину 2 байта, адресные биты позволяют в будущем увеличить длину адреса. Восьмой бит каждого байта адресного поля используется для указания адреса. Адрес содержит следующую информацию.
 - Значение DLCI — отображает значение DLCI и состоит из 10 битов адресного поля.
 - Контроль перегрузки — последние 3 бита адресного поля, управляющие механизмами уведомления о перегрузке в сети. Такими механизмами являются FECN, BECN и DE (биты допустимости отбрасывания).

- Данные — поле переменной длины, содержащее инкапсулированные данные протоколов верхних уровней.
- FCS — последовательность проверки фрейма (frame check sequence, FCS), используемая для обеспечения целостности передаваемых данных.

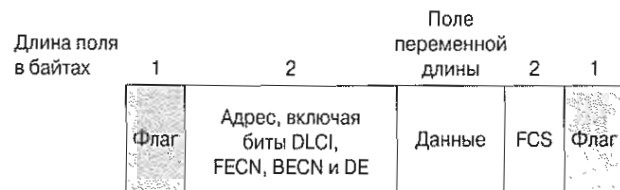


Рис. 15.7. Поля флагов задают начало и конец фрейма

Адресация протокола Frame Relay

На рис. 15.8 изображены два воображаемых PVC, один между Атлантой и Лос-Анджелесом, другой — между Сан-Хосе и Питтсбургом. Для ссылки на свой PVC с Атлантой Лос-Анджелес использует DLCI 22, в то время как Атланта использует для этой же цели DLCI 82. Аналогичным образом, Сан-Хосе использует DLCI 12 для ссылки на свой PVC с Питтсбургом. Сеть использует свои внутренние механизмы для того, чтобы эти два локальных идентификатора PVC имели разные значения.

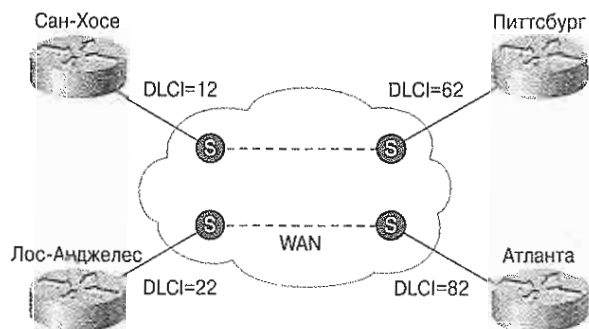


Рис. 15.8. Пример использования DLCI в сети протокола Frame Relay

Реализация протокола Frame Relay в маршрутизаторах Cisco — LMI

В истории протокола Frame Relay важное значение имеет 1990 год, когда компании Cisco Systems, StrataCom, Northern Telecom и Digital Equipment Corporation создали группу с целью концентрации средств и усилий на развитии технологии протокола Frame Relay и на ускорении внедрения взаимосвязанных программных продуктов этого протокола. Эта группа создала спецификацию, соответствующую базисной версии протокола, но дополнила ее новыми возможностями для сложных сред совместного использования. Эти усовершенствования стали называть *интерфейсом локального управления (Local Management Interface, LMI)*.

Функционирование LMI

Главными целями применения LMI являются:

- определение оперативного состояния различных PVC, известных маршрутизатору;
- передача пакетов об активности устройств, с целью удостовериться в том, что PVC продолжает функционировать, а не отключился в связи с простоем (рис. 15.9);
- информирование маршрутизатора о доступных PVC;
- три типа LMI могут быть активизированы следующими командами маршрутизатора: **ansi**, **cisco** и **q933a**.

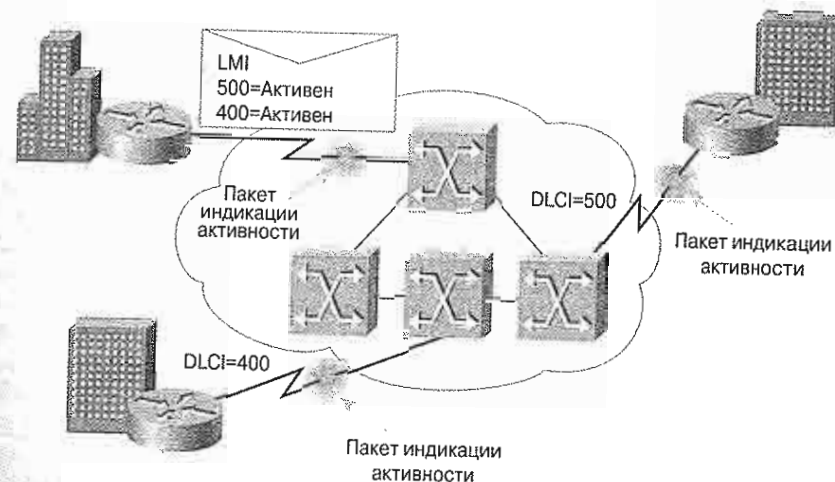


Рис. 15.9. LMI обеспечивают управление соединениями в сети

Дополнительные возможности интерфейса локального управления (LMI)

В дополнение к основным функциям протокола Frame Relay по передаче данных LMI-спецификация этого протокола включает в себя дополнительные возможности, которые облегчают поддержку больших и сложных сетей совместного использования. Некоторые из этих дополнительных возможностей называются *общими (common)* и могут быть использованы любым устройством, удовлетворяющим требованиям спецификации. Другие функции LMI рассматриваются как *необязательные (optional)*. Приведем полный список дополнительных возможностей, предоставляемых LMI.

- Сообщения о состоянии виртуального канала — они обеспечивают связь и синхронизацию между сетевыми устройствами и устройствами пользователя, периодически сообщая о появлении новых PVC и удалении существовавших, а также информируя о работе сети в целом. Эти сообщения избавляют от ненужной рассылки данных по уже несуществующим каналам.
- Рассылка данных одновременно нескольким получателям (многоадресная рассылка, multicast). Такая рассылка позволяет отправить один фрейм, а сеть обеспечивает его доставку сразу нескольким адресатам. Она является эффек-

тивным средством передачи сообщений протокола маршрутизации и протоколов преобразования адресов, которые обычно требуется рассылать одновременно в несколько пунктов назначения.

- Глобальная адресация (необязательная) придает локальному идентификатору соединения глобальный характер, после чего он может быть использован для идентификации конкретного интерфейса во всей сети протокола Frame Relay. Глобальная адресация делает сеть протокола Frame Relay в вопросе адресации похожей на локальную сеть; протоколы преобразования адресов работают в этих двух типах сетей одинаково.
- Простой контроль потока (необязательный) — предоставляет механизм управления потоком типа XON/XOFF, который применяется ко всему интерфейсу. Предназначен для устройств, верхние уровни которых не могут использовать биты уведомления о переполнении и требуют определенного уровня контроля потока данных.

Формат LMI-фрейма

Спецификация протокола Frame Relay также включает в себя процедуры рассылки LMI. Сообщения LMI рассылаются во фреймах, отличающихся друг от друга индивидуальными LMI-идентификаторами (DLCI), определенными в спецификации консорциума как DLCI=1023. Формат фрейма протокола Frame Relay показан на рис. 15.10.

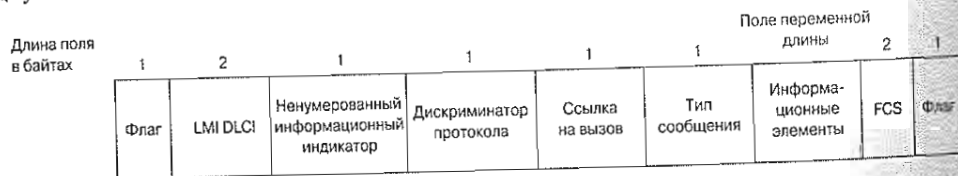


Рис. 15.10. В LMI-фреймах базовый протокольный заголовок такой же, как и у обычного фрейма протокола Frame Relay

После поля флага и поля LMI фрейм содержит 4 обязательных байта. Первый из этих обязательных байтов (*индикатор ненумерованной информации, unnumbered information indicator*) имеет такой же формат, как и LARV-индикатор фрейма *ненумерованной информации (unnumbered information, UI)*, в котором последний (poll/final) бит установлен в ноль. Следующий байт, называемый *дискриминатором протокола (protocol discriminator)*, содержит значение, определяющее LMI. Третий обязательный байт (*ссылка на вызов, call reference*) всегда заполнен нулями.

Последний обязательный байт представляет собой поле *типа сообщения (message type)*. Определены два типа сообщений: сообщения запросов о состоянии и сообщения о текущем состоянии. Сообщения о текущем состоянии являются ответами на сообщения-запросы. *Сообщения об активности (keepalive)* (сообщения, посылаемые в оба конца соединения для подтверждения того, что обе стороны продолжают рассматривать соединение как активное) и сообщения о состоянии PVC представляют собой примеры таких сообщений. Они являются типичными для LMI, и, как правило, присутствуют в любой реализации сети, соответствующей спецификации протокола Frame Relay.

Вместе взятые, запросы о состоянии и ответы на них (сообщения о состоянии) позволяют проверить целостность логического и физического каналов. Эта информация имеет критически важное значение для маршрутизации, поскольку протоколы маршрутизации принимают решения, основанные на предположении о целостности сети.

Далее следует поле информационного элемента (information element, IE), содержащее переменное количество байтов. За полем типа сообщения находится некоторое количество IE. Каждый информационный элемент состоит из однобайтного *идентификатора IE*, поля длины IE и одного или более байтов, содержащих конкретные данные.

Глобальная адресация

Кроме общих возможностей LMI имеется несколько необязательных, которые, однако, оказываются исключительно полезными при совместном использовании среды. Первой такой возможностью является опция *глобальной адресации (global addressing)*. При ее использовании значения, вводимые в DLCI-поле фрейма становятся глобально значимыми адресами индивидуальных устройств конечного пользователя (например, маршрутизаторов). Пример такой адресации приведен на рис. 15.8.

Как уже отмечалось ранее, базовая (нерасширенная) спецификация протокола Frame Relay поддерживает только такие значения поля DLCI, которые имеют локальный характер. В этом случае отсутствуют адреса, идентифицирующие сетевые интерфейсы или узлы, подсоединенные к этим интерфейсам. Ввиду отсутствия таких адресов они не могут быть найдены обычными методами обнаружения и преобразования адресов. Это означает, что при обычной адресации протокола Frame Relay необходимо создавать карты статической разметки, которые будут указывать маршрутизаторам, какие DLCI следует использовать для нахождения удаленных устройств и ассоциированных с ними адресов.

Следует обратить внимание на то, что каждый интерфейс на рис. 15.8 имеет собственный идентификатор. Предположим, что Питтсбург должен отправить фрейм в Сан-Хосе. Идентификатором Сан-Хосе является 22, поэтому Питтсбург помещает значение 22 в поле DLCI и посылает фрейм в сеть протокола Frame Relay. В точке выхода сеть меняет содержимое поля DLCI на 62 для указания на узел, являющийся источником фрейма. Каждому интерфейсу маршрутизатора в качестве идентификатора узла присвоено уникальное значение, поэтому отдельные устройства без труда различаются. Это позволяет выполнять маршрутизацию в сложных средах. В больших разветвленных средах глобальная адресация предоставляет значительные преимущества. В результате сеть протокола Frame Relay выглядит для периферийного маршрутизатора как обычная локальная сеть.

Многоадресная передача

Еще одной ценной особенностью LMI является одновременная передача одного и того же пакета данных нескольким пользователям. Группы многоадресной рассылки задаются последовательностью из четырех зарезервированных значений DLCI (от 1019 до 1022). Фреймы, отправленные устройством, использующим один из этих четырех DLCI, дублируются сетью и рассылаются по всем выходным точкам, указанным в наборе. В многоадресном расширении определены также сообщения LMI, которые уведомляют устройства пользователя о добавлении, удалении и наличии многоадресных групп. В сетях, использующих динамическую маршрутизацию, многие маршрутизаторы должны обмениваться между собой информацией о маршрутах. Сообщения о состоянии сети могут эффективно рассылаться путем использования многоадресных идентификаторов DLCI. Это также позволяет рассылать сообщения отдельным группам пользователей.

Инверсный протокол ARP

Механизм инверсного протокола ARP позволяет маршрутизатору автоматически строить карту отображения протокола Frame Relay, как показано на рис. 15.11. Маршрутизатор узнает используемые DLCI от коммутатора при первоначальном обмене LMI. После этого маршрутизатор посылает запрос инверсного ARP каждому DLCI для каждого протокола, сконфигурированного и поддерживаемого этим интерфейсом. Возвращаемая инверсным ARP информация используется для построения карты отображения протокола Frame Relay.

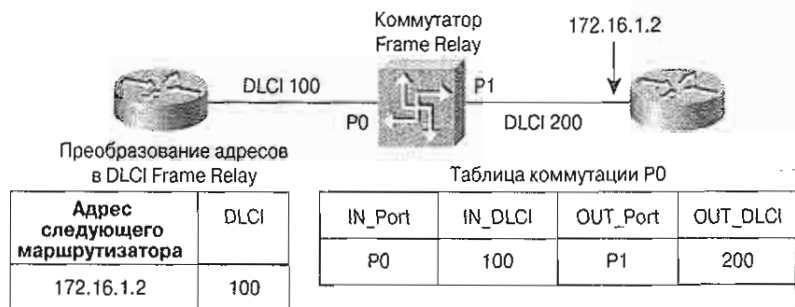


Рис. 15.11. Маршрутизатор узнает используемые DLCI от коммутатора протокола Frame Relay и посылает запрос инверсного ARP каждому DLCI

Отображение в протоколе Frame Relay

Адрес маршрутизатора следующего перехода, найденный в таблице маршрутизации, должен быть преобразован в DLCI протокола Frame Relay, как показано на рис. 15.12. Это преобразование осуществляется через структуру данных, называемую картой отображения протокола Frame Relay (Frame Relay map). После этого таблица маршрутизации используется для определения адреса следующего перехода или DLCI для выходного потока данных. Эта структура данных может быть статически сконфигурирована на маршрутизаторе или автоматически установлена путем использования возможностей инверсного протокола ARP.

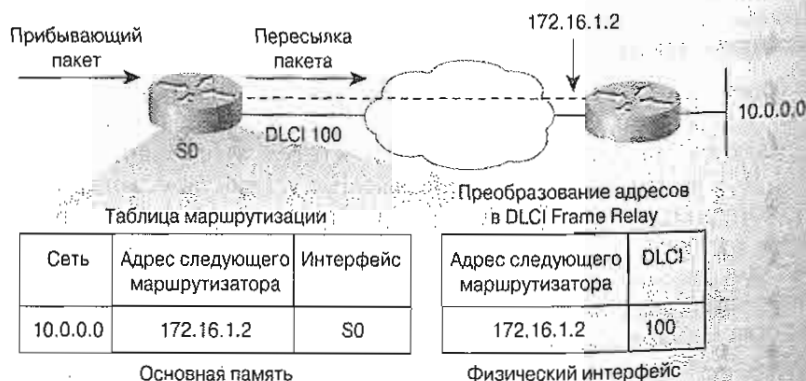


Рис. 15.12. Ответы на запросы инверсного ARP заносятся в таблицу отображения ("адрес-DLCI") маршрутизатора или сервера доступа

Таблицы коммутации протокола Frame Relay

Таблица коммутации протокола Frame Relay состоит из четырех элементов: два — для входного порта и входного DLCI и два — для выходного порта и выходного DLCI, как показано на рис. 15.13. Таким образом, при прохождении каждого коммутатора значение DLCI может быть отображено заново. Поскольку ссылка на порт может измениться, значения DLCI остаются постоянными.

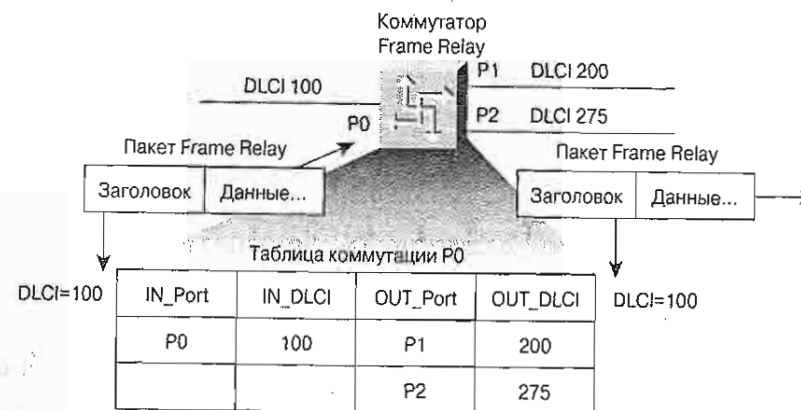


Рис. 15.13. Маршрутизаторы используют инверсный протокол ARP для нахождения удаленных IP-адресов и создания карты отображения локальных DLCI и ассоциированных с ними IP-адресов

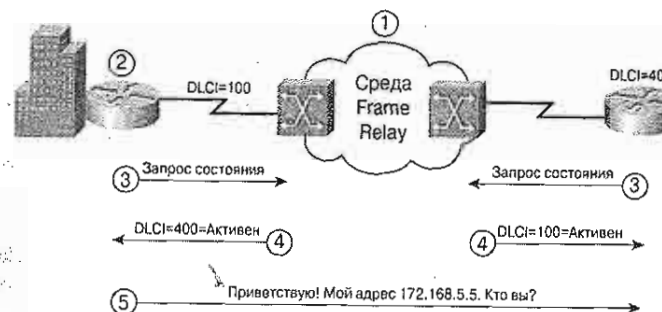


Рис. 15.14. Если инверсный ARP не работает или удаленный маршрутизатор не поддерживает этот протокол, то необходимо сконфигурировать маршруты (т.е. DLCI и IP-адреса) удаленных маршрутизаторов

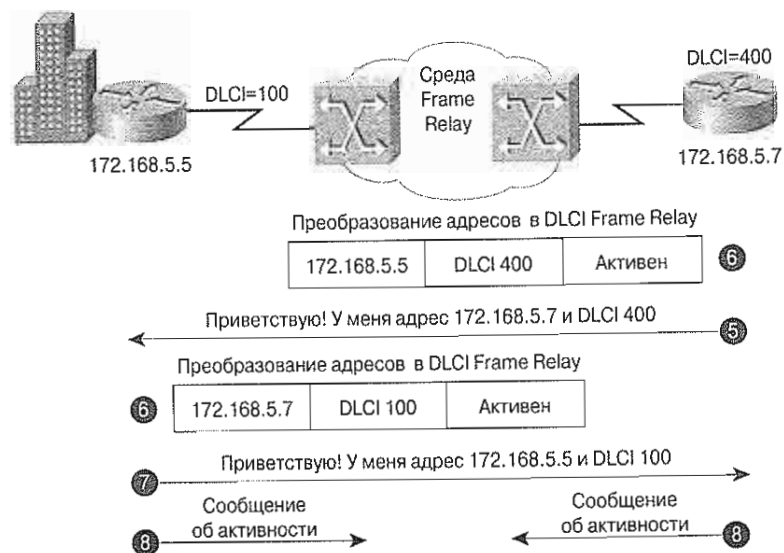


Рис. 15.15. Маршрутизатор изменяет состояние каждого DLCI, основываясь на ответе коммутатора протокола Frame Relay

Развертывание службы протокола Frame Relay

После изучения основ и терминологии протокола Frame Relay обратитесь к рис. 13.14 и 13.15, а также прочитайте приведенные ниже инструкции, которые помогут вам развернуть службу протокола Frame Relay.

- Этап 1.** Следует заказать службу протокола Frame Relay у провайдера или создать собственную среду действия этого протокола.
- Этап 2.** Подсоединить каждый маршрутизатор, непосредственно или посредством CSU/DSU (модуль канальной службы/модуль цифровой службы) к коммутатору протокола Frame Relay.
- Этап 3.** Когда маршрутизатор CPE начинает функционировать, он посылает сообщение-запрос о состоянии коммутатору протокола Frame Relay. Это сообщение уведомляет коммутатор о состоянии этого маршрутизатора и запрашивает у коммутатора информацию о состоянии связи других удаленных маршрутизаторов.
- Этап 4.** После получения коммутатором этого запроса он отвечает сообщением о состоянии, содержащим DLCI всех удаленных маршрутизаторов, которым данный локальный маршрутизатор может посылать данные.
- Этап 5.** Каждый маршрутизатор рассылает каждому DLCI пакет запроса инверсного ARP, представляя себя и предлагая каждому удаленному маршрутизатору сделать то же, сообщив свой адрес сетевого уровня.
- Этап 6.** Для каждого DLCI, о котором маршрутизатор получает сообщение инверсного ARP, создается элемент в таблице отображения протокола Frame Relay, содержащий локальный DLCI и адрес сетевого уровня удаленного маршрутизатора, а также информацию о состоянии канала связи. Отметим, что этот

DLCI является локально сконфигурированным, а не тем, который используется удаленным маршрутизатором. В таблице отображения протокола Frame Relay могут быть зафиксированы три вида состояния канала связи.

- **Активное состояние** — указывает на то, что канал активен и маршрутизаторы могут обмениваться данными.
- **Неактивное состояние** — указывает на то, что локальная связь с коммутатором протокола Frame Relay существует, а связь удаленного маршрутизатора с этим коммутатором отсутствует.
- **Отключенное состояние** — указывает на то, что от коммутатора не поступило LMI или отсутствует служба между маршрутизатором CPE и коммутатором протокола Frame Relay.

Этап 7. Каждые 60 секунд маршрутизаторы обмениваются сообщениями инверсного протокола ARP.

Этап 8. Каждые 10 секунд (этот интервал устанавливается в параметрах конфигурации) маршрутизатор CPE посылает коммутатору Frame Relay сообщение об активности. Цель рассылки таких сообщений состоит в проверке работоспособности этого коммутатора.

Подынтерфейсы протокола Frame Relay

Для того, чтобы привести в действие механизм рассылки полных сообщений об изменениях маршрутизации в сети протокола Frame Relay необходимо сконфигурировать на маршрутизаторе логически назначаемые интерфейсы, называемые подынтерфейсами (субинтерфейсами). Подынтерфейсы являются логическими разделами одного физического интерфейса. В конфигурации, использующей подынтерфейсы, каждый постоянный виртуальный канал может быть сконфигурирован как соединение «точка-точка». Это позволяет подынтерфейсу функционировать аналогично выделенной линии, как показано на рис. 15.16.

Прежние реализации протокола Frame Relay требовали, чтобы маршрутизатор (т.е. устройство DTE) имел последовательный интерфейс в распределенной сети для каждого PVC, как показано на рис. 15.17.

Логическое разделение одного физического последовательного интерфейса распределенной сети на несколько виртуальных подынтерфейсов позволяет существенно уменьшить общую стоимость сети протокола Frame Relay, как показано на рис. 15.18.

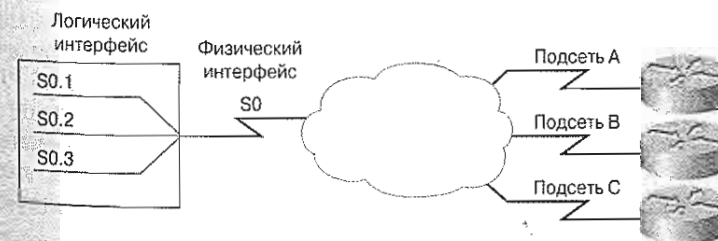


Рис. 15.16. Сообщения об изменениях маршрутной информации могут рассылаться через подынтерфейсы так, как если бы они исходили от различных физических интерфейсов

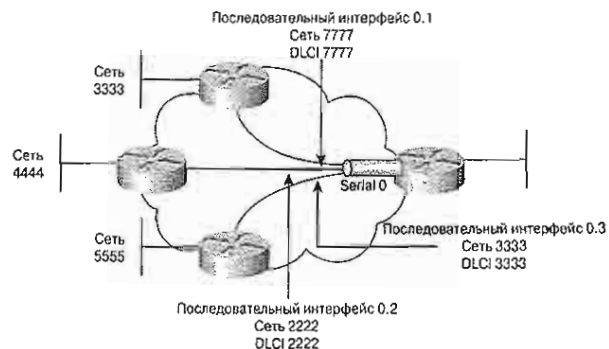


Рис. 15.17. Увеличение количества интерфейсов центрального маршрутизатора эффективно, но значительно увеличивает стоимость сети

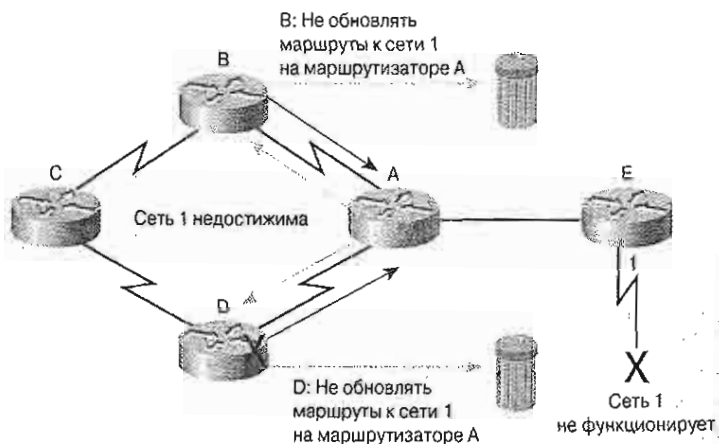


Рис. 15.18. Каждый подынтерфейс рассматривается как отдельная сеть и имеет уникальный номер DLCI

Среды с расщеплением горизонта

В средах маршрутизации с расщеплением горизонта маршруты, найденные на одном подынтерфейсе, могут быть сообщены другому подынтерфейсу. Вследствие этого маршрутизация с расщеплением горизонта уменьшает количество петель маршрутизации, не позволяя сообщениям об изменениях в сети, полученных на одном физическом интерфейсе, передаваться через тот же самый физический интерфейс (рис. 15.19). Благодаря этому в ситуации когда удаленный маршрутизатор посылает сообщение об изменении на центральный маршрутизатор, который соединяет несколько виртуальных каналов (PVC) в один физический интерфейс, последний не может передавать этот маршрут другим удаленным маршрутизаторам через тот же физический интерфейс (рис. 15.20).

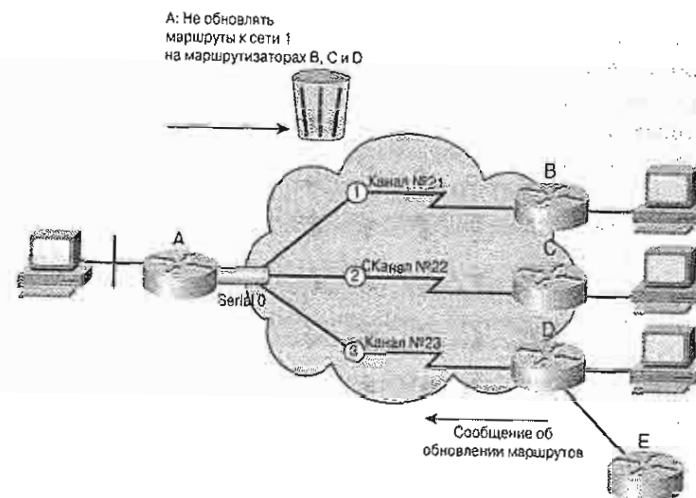
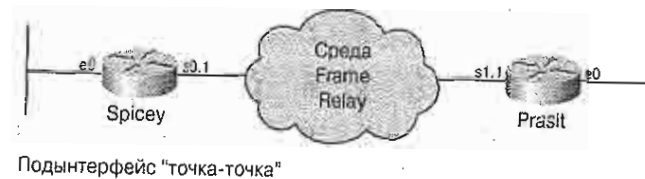
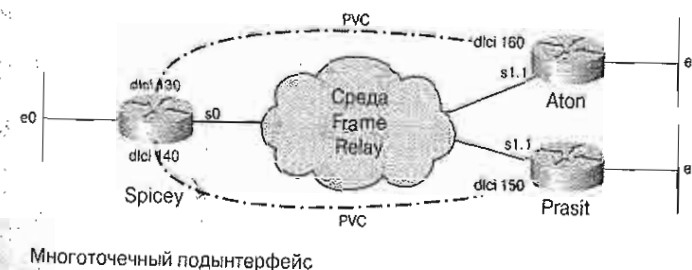


Рис. 15.19. В ситуации, когда используется расщепление горизонта, маршрутизатор, который получил маршрутную информацию через некоторый интерфейс, не посылает вновь информацию об этом маршруте на этот интерфейс



Подынтерфейс "точка-точка"



Многоточечный подынтерфейс

Рис. 15.20. При использовании расщепления горизонта сообщения об изменениях, полученные на центральном маршрутизаторе, не могут передаваться другим маршрутизаторам через тот же самый физический интерфейс

Разрешение проблем достижимости посредством использования подынтерфейсов

Подынтерфейс может быть сконфигурирован для обеспечения поддержки соединений перечисленных ниже типов.

- **Соединение типа “точка-точка”.** При этом отдельный подынтерфейс используется для установки соединения PVC с другим физическим интерфейсом или подынтерфейсом на удаленном маршрутизаторе. В этом случае подынтерфейсы оказываются в одной подсети и каждый из них имеет отдельный DLCI. Каждое соединение типа “точка-точка” является отдельной подсетью. В такой ситуации проблемы широковещательной передачи отсутствуют, поскольку маршрутизаторы непосредственно соединены друг с другом и функционируют как выделенная линия.
- **Многоточечное соединение.** Один подынтерфейс используется для установки нескольких PVC-соединений с несколькими физическими интерфейсами или подынтерфейсами удаленных маршрутизаторов. В этом случае все участвующие интерфейсы будут находиться в одной и той же подсети и каждый интерфейс будет иметь собственный локальный DLCI. Поскольку подынтерфейс в такой среде действует как обычная сеть протокола Frame Relay, сообщения об изменениях подвергаются расщеплению горизонта.

Базовая конфигурация протокола Frame Relay

В базовом варианте предполагается, что настройка параметров протокола Frame Relay устанавливается на одном или нескольких физических интерфейсах (рис. 15.21), а LMI и инверсный ARP поддерживаются удаленным маршрутизатором (маршрутизаторами). В такой среде LMI сообщает маршрутизатору о доступных DLCI. Инверсный ARP включен по умолчанию, поэтому данные о нем не появляются при выводе информации о конфигурации сети. Для установки базовой конфигурации протокола Frame Relay необходимо выполнить следующие действия:

Этап 1. Выбрать интерфейс и перейти в режим установки конфигурации:

```
Router(config)# interface serial 0
```

Этап 2. Сконфигурировать адрес сетевого уровня, например, IP-адрес:

```
Router(config-if)# ip address 192.168.38.40 255.255.255.0
```

Этап 3. Выбрать тип инкапсуляции для потока данных, передаваемого от одного конца сети к другому:

```
Router(config)# encapsulation frame relay [ cisco | ietf ]
```

где:

- **cisco** — значение, принимаемое по умолчанию, которое используется при соединении с другим маршрутизатором Cisco;
- **ietf** — используется для подсоединения всех отличных от Cisco маршрутизаторов.

Этап 4. Если используется версия ОС Cisco 11.1 или более ранняя, то необходимо указать тип LMI, используемый коммутатором протокола Frame Relay:

```
Router(config-if)# frame-relay lmi-type { ansi | cisco  
| q9331 }
```

где значение **cisco** принимается по умолчанию.

При использовании версии 11.2 или более поздней тип LMI распознается автоматически, поэтому при установке конфигурации его задавать не требуется.

Этап 5. Задать ширину полосы пропускания данного канала в Кбит/с:

```
Router(config-if)# bandwidth полоса
```

Эта команда воздействует на процесс маршрутизации таких протоколов, как IGRP, поскольку она определяет метрику канала.

Этап 6. Если инверсный протокол ARP был на маршрутизаторе отключен, то его следует снова включить (он является включенным по умолчанию):

```
Router(config-if)# frame-relay inverse-arp [протокол]  
[dlci]
```

где

- **протокол** — название одного из поддерживаемых протоколов, таких как IP, IPX, Apple Talk, DECNet, VINES или XNS
- **dlci** — DLCI локального интерфейса, с которым предполагается обмениваться сообщениями инверсного ARP

После знакомства с основными этапами конфигурации протокола Frame Relay воспользуемся ими для конфигурирования этого протокола на последовательном интерфейсе маршрутизатора Cisco 1600.

Конфигурирование последовательного интерфейса для подключения по протоколу Frame Relay

Для установки на последовательном интерфейсе типа инкапсуляции пакетов, используемого протоколом Frame Relay, необходимо выполнить следующие действия.

Этап 1. Войти в режим установки конфигурации последовательного интерфейса:

```
1600(config)# interface serial 0
```

Этап 2. Установить на этом интерфейсе метод инкапсуляции протокола Frame Relay:

```
1600(config-if)# encapsulation frame-relay
```

Этап 3. Разрешить изменение конфигурации этого интерфейса:

```
1600(config-if)# no shutdown
```

Проверка работоспособности протокола Frame Relay на последовательном интерфейсе

Для проверки правильности установленной на данный момент конфигурации можно удостовериться, что тестируемый PVC является активным для канала протокола Frame Relay. Для этого выполните следующие действия.

Этап 1. Ввести команду **encapsulation frame-relay** и подождать 60 секунд.

Этап 2. В привилегированном EXEC-режиме ввести команду **show frame-relay pvc**

Этап 3. Проверить, что в выводе упомянутой выше команды имеется сообщение (в примере выделенное жирным шрифтом) **PVC STATUS=ACTIVE**:


```
1600# show frame relay pvc
PVC Statistics for interface Serial0 (Frame Relay DTE)
DLCI=17, DLCI USAGE=LOCAL, PVC STATUS =ACTIVE, INTERFACE
=Serial0.1
input pkts 45 output pkts 52 in bytes 7764
out bytes 9958 dropped pkts 0 in FECN pkts 0
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
in DE pkts 0 out DE pkts 0
pvc create time 00:30:59, last time pvc status changed
00:19:21
```

Этап 4. Рекомендуется запомнить номер, указанный в сообщении DLCI=... (в данном примере этот номер равен 17). Он будет использован при завершении конфигурирования интерфейса протокола Frame Relay.

Этап 5. Если после ввода команды ничего не произойдет, то следует выполнить команду **show interfaces serial 0** для выяснения активности данного последовательного интерфейса. Пример такой команды приведен в следующем разделе. Первая строка вывода должна выглядеть следующим образом:

```
Serial0 is up, line protocol is up
```

Если первой строкой вывода является `Serial0 is up, line protocol is down`, то необходимо проверить на коммутаторе протокола Frame Relay правильность установки типа LMI. Это можно выяснить из строки вывода `LMI type is CISCO`, содержащейся в том же тексте вывода.

Этап 6. Для продолжения установки конфигурации следует вновь перейти в глобальный режим.

Тестирование протокола Frame Relay

После установки конфигурации протокола Frame Relay можно убедиться в том, что все соединения активны, выполнив одну из команд **show** (табл. 15.1).

Таблица 15.1. Команда show

Команда	Описание
show interfaces serial	Отображает информацию о DLCI, используемых при групповой передаче, о DLCI, используемых на последовательных интерфейсах, сконфигурированных под протокол Frame Relay, а также о DLCI интерфейса локального управления (LMI), используемого для LMI
show frame-relay pvc	Отображает состояние каждого сконфигурированного соединения и статистику потока данных. Эта команда также полезна для того, чтобы узнать количество BECN- и FECN-пакетов, полученных маршрутизатором
show frame-relay map	Отображает адрес сетевого уровня и ассоциированный с ним DLCI для каждого удаленного устройства, с которым соединен локальный маршрутизатор
show frame-relay lmi	Отображает статистику потока данных LMI. Например, выводится количество сообщений о состоянии, которыми обменивались локальный маршрутизатор и коммутатор протокола Frame Relay

Проверка работоспособности канала

Для проверки работоспособности канала следует выполнить перечисленные ниже действия.

Этап 1. В привилегированном командном режиме (EXEC) необходимо ввести команду **show interface serial 0**

В результате ее выполнения будет получена следующая информация:

```
1600# show interface serial 0
Serial0 is up, line protocol is up
Hardware is QUICC Serial
MTU 1500 bytes, BW 1544 Kbit,
    DLY 2000 usec, rely 255/255, load 1/255
Encapsulation FRAME-RELAY
    loopback not set, keepalive set (10 sec)
LMI enq sent 163, LMI stat recvd 136,
    LMI upd recvd 0, DTE LMI up
LMI enq recvd 39, LMI stat sent 0, LMI upd sent 0
LMI DLCI 1023 LMI type is CISCO frame relay DTE
Broadcast queue 0/64, broadcasts sent/dropped 27/0,
    interface broadcast 28
Last input 00:00:01, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops);
    Total output drops: 0
Queuing strategy: weighted fair
Output queue: 0/64/0 (size/threshold/drops)
Conversations 0/1 (active/max active)
Reserved Conversations 0/0 (allocated/max allocated)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1813 packets input, 109641 bytes, 0 no buffer
Received 1576 broadcasts, 0 runts, 0 giants
13 input errors, 0 CRC, 13 frame, 0 overrun,
    0 ignored, 0 abort
1848 packets output, 117260, 0 underruns
0 output errors, 0 collisions, 32 interface resets
0 output buffer failures, 0 output buffers swapped out
29 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

Этап 2. Следует удостовериться, что в вышеприведенном выводе имеются следующие (выделенные) строки:

- `Serial0 is up, line protocol is up` — означает, что соединение протокола Frame Relay является активным;
- `LMI enq sent 163, LMI stat recvd 136` — означает, что соединение отправляет и получает данные. Количество принятых и переданных данных, естественно, будет отличаться от приведенного в данном примере;
- `LMI type is CISCO` — означает, что тип LMI для данного маршрутизатора сконфигурирован правильно.

Этап 3. Если последнее сообщение при выводе отсутствует, то следует удостовериться в том, что:

- установка LMI провайдером службы протокола Frame Relay соответствует данному каналу;
- происходит рассылка сообщений об активности и маршрутизатор получает сообщения об изменениях LMI.

Этап 4. Для того, чтобы продолжить установку конфигурации, следует вновь войти в глобальный режим

Проверка наличия карты отображения

Для того, чтобы убедиться в наличии таблицы отображения протокола Frame Relay, необходимо выполнить следующие действия.

Этап 1. Находясь в привилегированном командном режиме (EXEC), ввести команду **show frame-relay map**. Проверить, что сообщение `status defined, active` (в примере выделено) появляется для каждого последовательного интерфейса.

```
1600# show frame-relay map
Serial0.1 (up): point-to-point dlci, dlci 17(0x11,0x410),
broadcast, status defined, active
```

Этап 2. Если такое сообщение не появляется, то необходимо:

- удостовериться в том, что маршрутизатор центрального сайта подключен и сконфигурирован;
- проверить вместе с провайдером протокола Frame Relay, что канал функционирует правильно.

Этап 3. Для того, чтобы продолжить конфигурирование, следует вновь перейти в глобальный режим установки конфигурации

Проверка связи с маршрутизатором центрального сайта

Для того, чтобы убедиться в наличии связи с маршрутизатором центрального сайта, необходимо выполнить следующие действия.

Этап 1. Находясь в привилегированном режиме (EXEC), ввести команду **ping**, после которой должен быть указан IP-адрес маршрутизатора центрального сайта.

Этап 2. Обратите внимание на строку `Success rate...` (в примере она выделена).

```
1600# ping 192.168.38.40
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.38.40,
  timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5),
  round-trip min/avg/max = 32/32/32 ms
1600#
```

Если доля успешного обмена равна 10% или больше, то этот этап тестирования можно считать успешно выполненным.

Этап 3. Для продолжения установки конфигурации следует вновь перейти в глобальный режим.



Лабораторная работа: конфигурирование протокола Frame Relay

В этой лабораторной работе требуется сконфигурировать маршрутизатор, чтобы он мог без проблем устанавливать соединение с локальным коммутатором Frame Relay.

Для имитации среды Frame Relay используется имитатор Adtran Atlas550.



Лабораторная работа: конфигурирование PVC протокола Frame Relay

В этой лабораторной работе требуется сконфигурировать два маршрутизатора так, чтобы они взаимодействовали по PVC протокола Frame Relay. При отсутствии коммутатора Frame Relay и LMI сделайте это вручную.

Конфигурирование подынтерфейсов

Для установки конфигурации подынтерфейсов на одном физическом интерфейсе, как показано на рис. 15.21, необходимо выполнить следующие действия.

Этап 1. Выбрать интерфейс, на котором будут созданы подынтерфейсы и войти в режим установки конфигурации.

Этап 2. Удалить все адреса сетевого уровня, назначенные данному физическому интерфейсу. Если физический интерфейс имеет адрес, то локальные интерфейсы не будут получать фреймы.

Этап 3. Сконфигурировать инкапсуляцию протокола Frame Relay, как это было описано выше в разделе “Базовая конфигурация протокола Frame Relay”.

Этап 4. Выбрать подынтерфейс, который требуется сконфигурировать:

```
Router(config-if)# interface serial номер.номер-
подынтерфейса { multipoint | point-to-point }
где:
```

■ **номер.номер-подынтерфейса** — представляет собой номер подынтерфейса, лежащий в диапазоне от 1 до 4 294 967 293. Номер интерфейса, предшествующий точке, должен соответствовать номеру интерфейса, которому принадлежит подынтерфейс.

■ **multipoint** — используется, если требуется, чтобы маршрутизатор направлял далее принимаемые им широковещательные сообщения и сообщения об изменениях маршрутной информации. Это значение следует выбрать если используется IP-маршрутизация и желательно объединить все маршрутизаторы в одну и ту же подсеть (рис. 15.22).

■ **point-to-point** — используется в том случае, когда не требуется, чтобы маршрутизатор направлял далее принимаемые им широковещательные сообщения и сообщения об изменениях маршрутов в сети, а также в случае, когда требуется чтобы каждая пара маршрутизаторов, образующая соединение “точка-точка” имела собственную подсеть (рис. 15.23).

Выбор одного из двух значений: **point-to-point** или **multipoint** является обязательным; значения по умолчанию не предусмотрено.

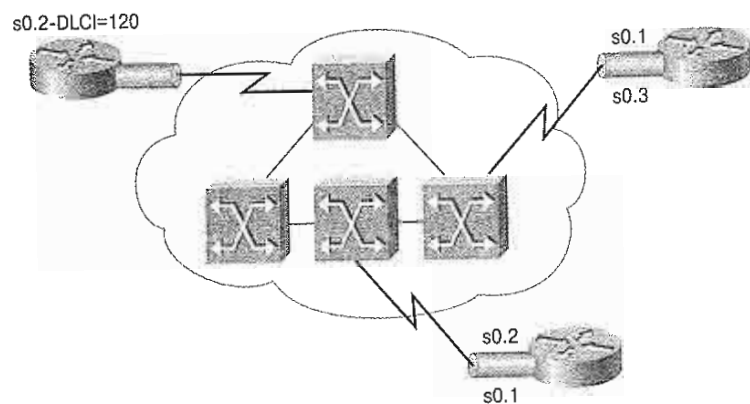


Рис. 15.21. Подынтерфейсы типа "точка-точка"

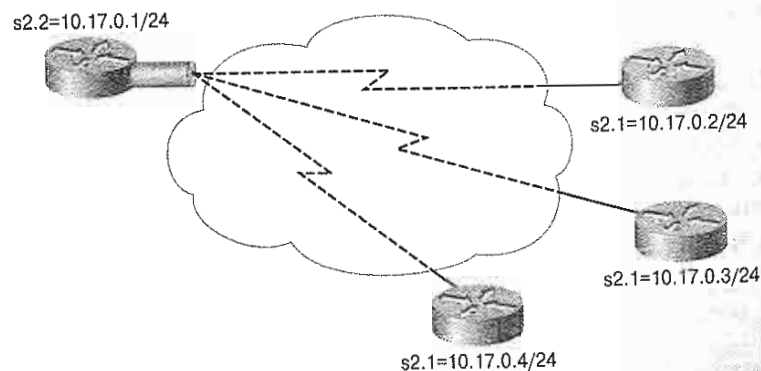


Рис. 15.22. Многоточечная конфигурация

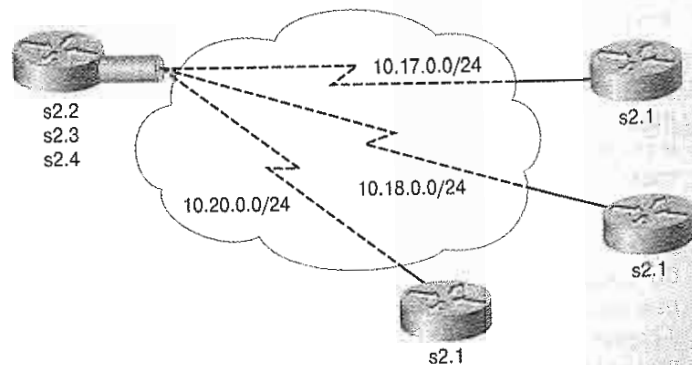


Рис. 15.23. Конфигурация подынтерфейсов

Этап 5. Сконфигурировать на подынтерфейсе адрес сетевого уровня. Если подынтерфейс имеет тип **point-to-point** и используется протокол IP, то можно использовать команду **ip unnumbered**:

Router(config-if)# **ip unnumbered** интерфейс

Если требуется использовать эту команду, то желательно, чтобы рассматриваемый интерфейс был интерфейсом обратной петли. Это связано с тем, что канал протокола Frame Relay не будет работать, если в данной команде указан интерфейс, работающий со сбоями, а интерфейсы обратной петли обладают весьма высокой надежностью.

Этап 6. Если была установлена конфигурация **multipoint** или **point-to-point**, то необходимо изменить локальный DLCI для подынтерфейса, для того, чтобы его можно было отличить от физического интерфейса:

Router(config-if)# **frame-relay interface-dlci** номер-dlci

где:

- номер-dlci — определяет локальный номер DLCI, связанный в настоящий момент с данным подынтерфейсом. Это единственный способ связать определяемый LMI постоянный виртуальный канал с подынтерфейсом, поскольку LMI не знает о существовании подынтерфейсов.

Эту команду необходимо выполнить для всех подынтерфейсов типа **point-to-point**. Она также необходима для всех многоточечных подынтерфейсов, для которых включен инверсный протокол ARP. Однако она не требуется для многоточечных подынтерфейсов, на которых установлена статическая разметка маршрутов.

Эта команда не используется для физических интерфейсов.

Лабораторная работа: конфигурирование подынтерфейсов протокола Frame Relay

В этой лабораторной работе требуется сконфигурировать три маршрутизатора в полносвязной сети Frame-Relay. Для имитации среды Frame Relay используется имитатор Adtran Atlas550.

ПРИМЕЧАНИЕ

Если подынтерфейс определен как **point-to-point**, его нельзя переназначить на **multipoint** с тем же номером без предварительной перезагрузки маршрутизатора. Однако такой перезагрузки можно избежать, задав этому подынтерфейсу другой номер.

Необязательные команды конфигурирования

При необходимости на маршрутизаторе можно указать дополнительные параметры соединения посредством использования следующей команды:

router(config-if)# **frame-relay map** протокол протокольный-адрес dlci [broadcast] [ietf | cisco | payload-compress | packet-by-packet]

В табл. 15.2 описаны различные параметры этой команды.

Таблица 15.2. Синтаксис команды frame-relay map

Параметр	Описание
протокол	Задаёт тип поддерживаемого протокола, способ использования моста или управления логическим каналом
протокольный-адрес dlci	Определяет адрес интерфейса сетевого уровня маршрутизатора Определяет локальный DLCI, используемый для соединения с удалённым протокольным адресом
broadcast	(Необязательный параметр) Направляет широковещательные сообщения на этот адрес в случае, когда не включен режим групповой рассылки. Используется в случае, когда требуется, чтобы маршрутизатор направлял дальше сообщения об изменении маршрутной информации
ietf cisco	(Необязательный параметр) Выбирает тип инкапсуляции протокола Frame Relay. Если удалённый маршрутизатор является маршрутизатором Cisco, то следует использовать значение cisco, в противном случае — значение ietf
payload-compress и packet-by-packet	(Необязательный параметр) Задаёт использование режима сжатия пакетов при загрузке методом Стеккера (Stacker)

Обычно инверсный протокол ARP используется при запросе протокольного адреса следующего перехода для некоторого соединения. Ответы на эти запросы помещаются в таблицу отображения (т.е. составляется карта отображения протокола Frame Relay, как показано на рис. 15.24). После этого карта используется для маршрутизации выходного потока данных. Если удалённый маршрутизатор не поддерживает инверсный ARP, то при установке протокола OSPF поверх протокола Frame Relay или в случае когда желательно контролировать широковещательные сообщения при маршрутизации, необходимо определить таблицу отображения статически. Элементы такой таблицы называют *статическими картами (static map)*.

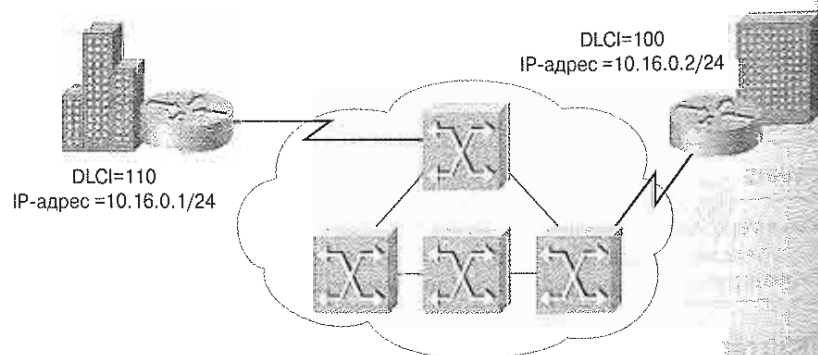


Рис. 15.24. Ответы на запросы инверсного ARP об адресе следующего перехода заносятся в таблицу отображения инверсного протокола ARP

При использовании протокола Frame Relay можно увеличить или уменьшить интервал отправки сообщений об активности, т.е. период времени, по истечении которого интерфейс маршрутизатора посылает сообщение об активности коммутатору протокола Frame Relay. По умолчанию он равен 10 секундам, а изменить его можно выполнив команду:

```
router(config-if)# keepalive число
```

Параметр число задаёт значение интервала в секундах. Обычно это значение устанавливается на 2–3 секунды меньше, чем установленное на коммутаторе протокола Frame Relay. Это делается для обеспечения синхронизации работы этих устройств.

Если в сети не используется LMI или осуществляется взаимное тестирование маршрутизаторов, то каждому из локальных интерфейсов следует назначить DLCI посредством следующей команды:

```
router(config-if)# frame-relay local-dlci число
```

Здесь параметр число представляет собой DLCI используемого локального интерфейса.

Резюме

В этой главе были рассмотрены следующие вопросы.

- Технология распределенных сетей, использующая протокол Frame Relay, представляет собой гибкий метод установки связи между локальными сетями через каналы распределенных сетей.
- Протокол Frame Relay обеспечивает возможность пакетно-коммутируемой передачи данных через интерфейс между устройствами пользователя (такими, как маршрутизаторы, мосты и хосты) и сетевым оборудованием (таким, как коммутирующие узлы).
- Для установки соединения через каналы распределенных сетей протокол Frame Relay использует виртуальные каналы.
- Главными целями применения LMI являются:
 - определение оперативного состояния различных PVC, известных маршрутизатору;
 - передача пакетов об активности устройств, с целью удостовериться в том, что PVC продолжает функционировать, а не отключился в связи с бездействием;
 - информирование маршрутизатора о доступных PVC;
 - возможность автоматического построения карты отображения протокола Frame Relay с использованием механизма инверсного ARP;
 - преобразование определенного по таблице маршрутизации адреса следующего перехода в DLCI протокола Frame Relay.
- Протокол Frame Relay может разделить один физический интерфейс распределенной сети на несколько подынтерфейсов.
- В среде маршрутизации с расщеплением горизонта маршруты, полученные с одного интерфейса могут быть сообщены другому интерфейсу.

Глоссарий

Идентификатор канального соединения (data-link connection identifier — DLCI). Значение, которое определяет PVC или SVC в сети Frame Relay. В базовой спецификации Frame Relay DLCI-идентификаторы являются локальными (для указания одного и того же соединения подключенные устройства могут использовать разные

значения), а в расширенной спецификации LMI — глобальными (указывают на отдельные оконечные устройства).

Интерфейс локального управления (Local management interface — LMI). Набор усовершенствований основной спецификации Frame Relay. Он включает в себя:

- механизм многоадресной передачи (multicast), предоставляющий сетевому серверу свои локальные и многоадресные DLCI;
- механизм глобальной адресации, который назначает DLCI-интерфейсам глобальное, а не локальное значение в сетях Frame Relay
- механизм извещений об активности, который проверяет состояние канала передачи данных;
- механизм определения состояния, который предоставляет отчет о текущем состоянии известных коммутатору DLCI-интерфейсов. В терминологии ANSI LMI называется LMT.

Обратное явное уведомление о перегрузке (Backward explicit congestion notification — BECN). Бит, устанавливаемый во фреймах протокола Frame Relay, которые передаются в направлении, обратном тому, в котором передаются кадры, столкнувшиеся с перегруженным маршрутом. DTE-устройства, получающие фреймы с установленным BECN-битом могут потребовать, чтобы протоколы высшего уровня предприняли соответствующие действия по управлению потоком данных.

Открытая сеть передачи данных (Public data network — PDN). Принадлежащие государству (как в Европе) или частным концернам (как в США) сети, обеспечивающие общедоступную компьютерную связь, обычно платную. PDN позволяют небольшим организациям создавать распределенные сети без затрат на прокладку каналов связи на дальние расстояния.

Постоянный виртуальный канал (соединение) (Permanent virtual circuit — PVC). Постоянно действующий виртуальный канал. Если виртуальный канал должен существовать постоянно, то использование PVC уменьшают загрузку полосы пропускания, необходимую на установку и разрыв соединения.

Протокол Frame Relay. Стандартный промышленный протокол передачи данных с коммутацией каналов, который управляет несколькими виртуальными каналами между подключенными устройствами с помощью HDLC-инкапсуляции. Он более эффективен, чем X.25, и обычно рассматривается как его замена.

Прямое явное уведомление о перегрузке (Forward Explicit Congestion Notification — FECN). Бит, устанавливаемый во фреймах протокола Frame Relay для уведомления DTE-устройств, получающих фреймы, о перегрузке участка сети между источником и получателем. DTE-устройства, получающие фреймы с установленным FECN-битом могут потребовать, чтобы протоколы высшего уровня предприняли соответствующие действия по управлению потоком данных.

Скорость локального доступа (скорость порта) (Local access rate). Скорость установки соединения (локального ответвления) со средой протокола Frame Relay. Она характеризует скорость поступления данных в сеть и получения данных из нее.

Физическая передающая среда (Physical media, media). Употребляется как в единственном (medium), так и во множественном числе (media). Типичными сетевыми передающими средами являются: витая пара, коаксиальный или волоконно-оптический кабель, электромагнитные волны (для СВЧ, лазерной и инфракрасной передачи данных).

Контрольные вопросы

Для проверки понимания тем и понятий, описанных в настоящей главе, рекомендуется ответить на предлагаемые ниже обзорные вопросы. Ответы на них приведены в приложении А.

1. Каким образом протокол Frame Relay обрабатывает несколько потоков обмена данными по одному физическому соединению?
 - А. Они передаются в дуплексном режиме;
 - В. Он мультиплексирует каналы;
 - С. Он конвертирует их в ячейки АТМ;
 - Д. Этот протокол допускает передачу нескольких потоков данных одновременно.
2. Какие из перечисленных ниже протоколов используются протоколом Frame Relay для коррекции ошибок?
 - А. Протоколы физического и канального уровней.
 - В. Протоколы верхнего уровня.
 - С. Протоколы нижнего уровня.
 - Д. Протокол Frame Relay не выполняет коррекции ошибок.
3. Что из перечисленного ниже позволяет протоколу Frame Relay сделать свои DLCI глобальными?
 - А. Он передает их в широковещательном режиме.
 - В. Он высылает несколько сообщений отдельным получателям.
 - С. Он рассылает сообщения сразу нескольким получателям.
 - Д. DLCI не могут стать глобальными.
4. Какая из перечисленных ниже скоростей является той скоростью, на которой коммутатор протокола Frame Relay будет передавать данные?
 - А. Согласованная скорость передачи информации (CIR).
 - В. Скорость передачи данных.
 - С. Скорость синхронизации.
 - Д. Скорость в бодах (бит/сек).
5. Кто из перечисленных ниже назначает номера DLCI?
 - А. Конечный пользователь.
 - В. Корневое устройство сети.
 - С. Сервер DLCI.
 - Д. Провайдер службы.
6. В какое из перечисленных ниже полей заголовка протокола Frame Relay включается информация DLCI?
 - А. В поле флага.
 - В. В поле адреса.
 - С. В поле данных.
 - Д. В поле контрольной суммы.

7. Что из перечисленного ниже позволяет протоколу Frame Relay поддерживать PVC в активном состоянии?
 - A. Соединение типа "точка-точка".
 - B. Интерфейс сокетов Windows.
 - C. Сообщения об активности.
 - D. Переход PVC в неактивное состояние.
8. Как протокол Frame Relay использует запросы инверсного ARP?
 - A. Он конвертирует IP-адреса в MAC-адреса.
 - B. Он конвертирует MAC-адреса в IP-адреса.
 - C. Он конвертирует MAC-адреса в сетевые адреса.
 - D. Он использует таблицу отображения IP-адресов в DLCI.
9. Что из перечисленного ниже используется в протоколе Frame Relay для определения адреса следующего перехода?
 - A. Таблица ARP.
 - B. Таблица маршрутизации протокола RIP.
 - C. Таблица отображения протокола Frame Relay.
 - D. Таблица маршрутизации протокола IGRP.
10. Для какой цели из перечисленных ниже протокол Frame Relay использует расщепление горизонта?
 - A. Для увеличения числа сообщений об обновлении маршрутной информации.
 - B. Для предотвращения маршрутных петель.
 - C. Для увеличения времени конвергенции.
 - D. Протокол Frame Relay не использует расщепление горизонта.
11. На каком уровне функционирует протокол Frame Relay?
 - A. A. На 2-м уровне
 - B. B. На 3-м уровне
 - C. C. На 4-м уровне
 - D. D. На 1-м уровне
12. Какое из приведенных ниже утверждений является истинным?
 - A. Целью использования оборудования DTE является обеспечение в сети служб синхронизации и коммутации.
 - B. Предложения о стандартизации протокола Frame Relay были первоначально представлены Консультативному Комитету по международной телеграфии и телефонии (Consultative Committee for International Telegraph and Telephone — CCITT).
 - C. Прежние версии протокола Frame Relay в совокупности называют интерфейсом локального управления LMI.
 - D. Коммутируемые виртуальные каналы VC представляют собой постоянные соединения, которые используются в ситуациях, требующих лишь спорадической передачи данных между устройствами DTE по сети Frame Relay.

13. Какая из приведенных ниже команд используется (в режиме config) для входа в режим конфигурирования последовательного интерфейса для инкапсуляции пакетов протокола Frame Relay?
 - A. # **configure terminal**
 - B. # **encapsulation frame-relay**
 - C. # **frame-relay interface dlci number**
 - D. # **interface serial0**
14. Если выполняется команда **show interface serial 0** и появляется сообщение "Serial line is up, line protocol is up" ("Последовательный канал активен, протокол канала установлен"), то какова правильная интерпретация этого сообщения?
 - A. По соединению отправляются и получаются данные.
 - B. Интерфейс LMI маршрутизатора сконфигурирован правильно.
 - C. Соединение протокола Frame Relay активно.
 - D. Маршрутизатор центрального узла активизирован и подсоединен.
15. Какие действия выполняются по команде **show interfaces serial**?
 - A. Отображается информация о многоадресных идентификаторах DLCI, о DLCI, которые используются на сконфигурированных последовательных интерфейсах протокола Frame Relay и о DLCI интерфейса LMI, используемых для LMI.
 - B. Отображается состояние всех сконфигурированных соединений и статистика передачи данных. Эта команда также полезна для того, чтобы узнать количество пакетов DECN и FECN, получаемых маршрутизатором.
 - C. Отображается адрес сетевого уровня и ассоциированный идентификатор DLCI для каждого удаленного получателя, к которому подсоединен локальный маршрутизатор.
 - D. Отображается статистика передачи данных на интерфейсе LMI. В частности, отображается количество сообщений о состоянии, которыми обменивались локальный маршрутизатор и коммутатор протокола Frame Relay.
16. Что такое FECN и BECN?
 - A. Механизмы регистрации ошибок передачи
 - B. Механизмы уведомления о переполнении
 - C. Механизмы управления потоком
 - D. D. Механизмы уведомления об активности
17. Какое из приведенных ниже утверждений относящихся к VC-каналам протокола Frame Relay справедливо?
 - A. A. Эти каналы требуют установки и прекращения сеанса.
 - B. B. Эти каналы используются только в том случае, когда передача данных носит спорадический характер.
 - C. C. Эти каналы обеспечивают постоянные маршруты коммуникации в сетях Frame Relay.
 - D. D. Эти каналы обеспечивают логические двусторонние маршруты связи между сетевыми устройствами.

18. Для чего в протоколе Frame Relay используется контрольная сумма CRC?

- A. Для управления потоками в виртуальных каналах VC
- B. Для обнаружения ошибок при передаче
- C. Для управления функциями преобразования адресов
- D. Для управления операциями с битами BECN и FECN

19. Что из приведенного ниже не является расширением LMI Frame Relay?

- A. Генерируемые алгоритмом MAC-адреса
- B. Группы многоадресной рассылки
- C. Глобальная адресация
- D. Сообщения о состоянии виртуальных каналов



В этой главе...

- Описаны важнейшие аспекты функционирования рабочих станций, на которых установлены ОС Windows, UNIX или Linux
- Рассмотрены функции сетевых серверов
- Рассмотрены сетевые операционные системы (Network Operating System — NOS)

Введение в сетевое администрирование

Термин “сетевое администрирование” охватывает многие аспекты и элементы многих рабочих специальностей и обязанностей, связанных с управлением компьютерной сетью. В настоящей главе основное внимание уделяется некоторым задачам, связанным с управлением рабочими станциями и операционными системами (NOS) и предоставляется обзор некоторых популярных решений, связанных с использованием серверов, которые устанавливаются в сети для управления сетевыми ресурсами предприятия. В данной главе описываются достоинства и недостатки возможных аппаратных и программных решений, а также приводятся рекомендации в отношении того, в какой среде эти варианты дают наилучший результат. В ней также приводится информация о том, как можно использовать эталонную модель OSI (Open System Interconnection — OSI) и простой протокол управления сетью (Simple Network Management Protocol — SNMP) для облегчения управления сетью.

Рекомендуется выполнить лабораторные работы (e-Lab Activities), ознакомиться с видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске. Эти приложения дополняют материал книги и помогают лучше усвоить используемые понятия и методы.

Обзор настольных компьютеров и серверных операционных систем

Первые персональные компьютеры (personal computer — PC) создавались как отдельные настольные системы. Программное обеспечение операционной системы позволяло осуществлять доступ к файлам и системным ресурсам только одному пользователю. Этот пользователь имел физический доступ к персональному компьютеру. По мере того, как настольные компьютеры стали все больше использоваться на рабочих местах, производители программного обеспечения стали разрабатывать специализированные операционные системы NOS. При их разработке ставилась цель обеспечить безопасность, привилегии пользователей и совместное использование ресурсов многими пользователями.

Взрывной рост сети Internet побудил разработчиков сетевых операционных систем создавать современные NOS на основе связанных с сетью Internet технологий и служб, таких как “Всемирная паутина” (World Wide Web).

За последние десять лет работа в сети приобрела центральное место в работе настольных персональных компьютеров. Различие между современными операционными системами настольных компьютеров, включающих в себя сетевые функции и службы, и собственно сетевыми операционными системами NOS постепенно стерлось. В настоящее время наиболее популярные операционные системы, такие как Microsoft Windows Server 2003 и Linux, устанавливаются, как на мощных сетевых серверах так и на настольных компьютерах конечных пользователей.

Рабочие станции

Под рабочей станцией понимается клиентский компьютер, который используется для запуска приложений и подсоединен к серверу, от которого он получает данные, совместно используемые вместе с другими компьютерами. Сервером называется компьютер, на котором работает сетевая операционная система NOS. Рабочая станция использует специальное программное обеспечение, такое, например, как сетевая оболочка для выполнения следующих действий:

- перехватывать данные пользователя и команды приложения;
- определять, предназначена ли команда локальной операционной системе или NOS;
- направлять команду на локальную операционную систему или на карту сетевого интерфейса для обработки и последующей передачи в сеть;
- доставлять передаваемые по сети данные приложению, работающему на рабочей станции.

Операционные системы Windows NT, Windows 2000 и Windows XP Professional могут работать и на персональных компьютерах. Компьютерная система, на которой работает какая-либо из упомянутых выше операционных систем называется либо рабочей станцией, как показано на рис. 16.1, либо сервером (рис. 16.2). Персональным компьютером называется система, на которой работает любая из других популярных операционных систем, таких как DOS, Windows 95, Windows 98, Windows ME, или Windows XP Home.

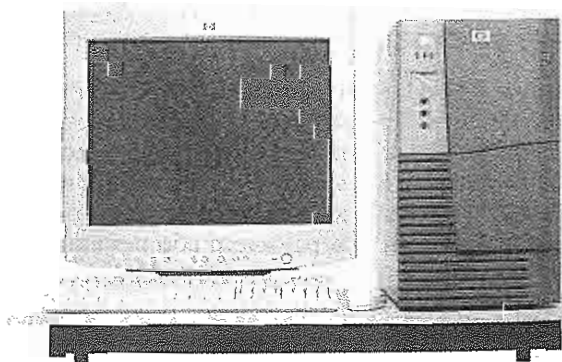


Рис. 16.1. Типичная рабочая станция

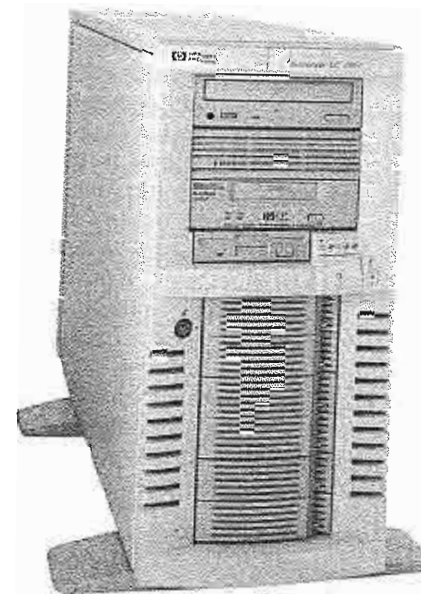


Рис. 16.2. Типичный сервер

ОС UNIX и Linux также могут использоваться в качестве операционных систем настольных компьютеров, однако чаще всего они используются на мощных компьютерах. Такие рабочие станции используются в инженерных и научных приложениях, которым требуются специальные выделенные компьютеры, обладающие высокой производительностью. Ниже приводятся некоторые конкретные приложения, которые часто работают на рабочих станциях UNIX.

- Компьютерное проектирование (Computer-aided design — CAD).
- Проектирование электронных микросхем.
- Прогнозирование погоды.
- Графические компьютерные анимации.
- Управление телекоммуникационным оборудованием.

Большинство операционных систем для настольных компьютеров обладают сетевыми функциями и поддерживают доступ к сети многих пользователей. По этой причине в настоящее время наблюдается тенденция классифицировать компьютеры и операционные системы на основе типов исполняемых приложений. Такая классификация основывается на роли или функции, выполняемой данным компьютером, такой как роль рабочей станции или сервера.

Типичная настольная система или рабочая станция обычно выполняет такие приложения как текстовый процессор, электронные таблицы или программа финансового анализа. На высокопроизводительных рабочих станциях используются такие приложения, как графическое проектирование, управление оборудованием и другие, упомянутые выше приложения.

Бездисковой рабочей станцией называется компьютер специального типа, который предназначен только для работы в сети. Как показывает само название, бездисковая рабочая станция не имеет дисководов, однако у нее есть монитор, клавиатура, оперативная память, загрузочные инструкции в постоянной памяти ROM и карта сетевого интерфейса. Программное обеспечение, требуемое для подключения к сети загружается из ПЗУ устройства (микросхемы, расположенной на плате сетевого интерфейса).

Поскольку у бездисковой рабочей станции нет дисководов, пользователь не может загрузить какие-либо данные с рабочей станции или передать данные ей. Бездисковая рабочая станция не может заразить сеть вирусом и не может быть использована для копирования данных из сети на диск. В результате этого бездисковые рабочие станции обеспечивают более высокий уровень безопасности, чем обычные рабочие станции. По этой причине такие рабочие станции часто используются в сетях с повышенными требованиями к безопасности.

Переносные компьютеры также могут функционировать в качестве рабочих станций в локальной сети LAN, подсоединяясь к сети через док-станцию, внешний адаптер LAN или через карту PCMCIA. Док-станция, показанная на рис. 16.3, представляет собой дополнительное устройство, которое превращает переносной компьютер в настольный.

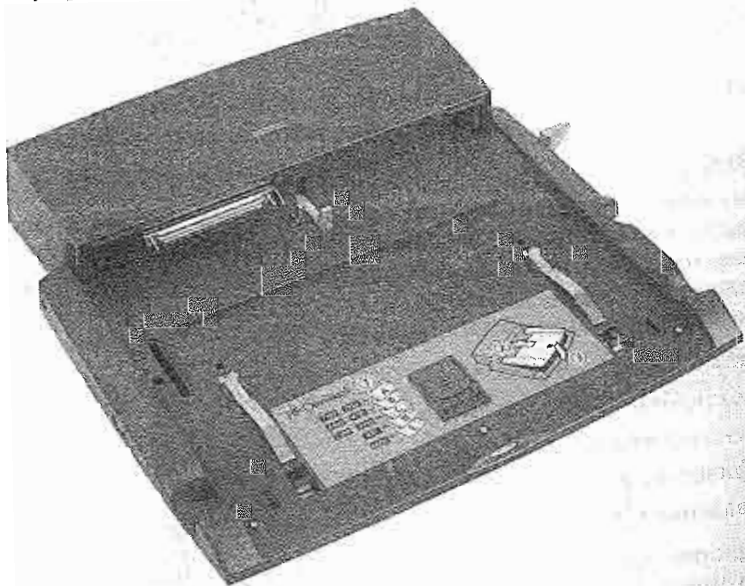


Рис. 16.3. Док-станция

Серверы

В среде операционной системы NOS многие клиентские системы получают доступ к одному или более серверам и совместно используют их ресурсы. Клиентские настольные системы имеют свою собственную оперативную память и периферийные устройства, такие как клавиатура, монитор и дисководы. На серверных компьютерных системах должны быть установлены программы для поддержки многих конкурирующих между собой за доступ пользователей и многих выполняемых заданий в тех случаях когда клиенты запрашивают у сервера удаленные ресурсы. Операционные системы

NOS имеют дополнительные средства управления сетью и другие функции, предназначенные для одновременной поддержки доступа нескольких пользователей. За исключением самых малых сетей операционные системы NOS устанавливаются на мощных серверах. Серверы обычно имеют высокоскоростные винчестеры большой емкости, большой объем оперативной памяти RAM, высокоскоростные карты сетевых интерфейсов и, в некоторых случаях, несколько центральных процессоров (central processing unit — CPU). Такие серверы обычно конфигурируются для использования семейства протоколов Internet (Transmission Control Protocol/Internet Protocol — TCP/IP) и предлагают одну или более служб TCP/IP.

Серверы, на которых функционирует операционная система NOS, также используются для аутентификации пользователей и предоставляют клиентам доступ к совместно используемым ресурсам, как показано на рис. 16.4. Эти серверы предназначены для одновременной обработки запросов от многих клиентов. Перед тем как клиент получит доступ к ресурсам сервера, ему требуется пройти идентификацию и авторизацию на право использования ресурсов. Для этого каждому клиенту назначается учетная запись и пароль. Учетная запись и пароль впоследствии проверяются службой аутентификации, которая выступает в качестве охраны доступа к сети. За счет централизации учетных записей пользователей, повышения уровня безопасности и управления доступом к сети на основе серверов упрощается работа сетевого администратора.

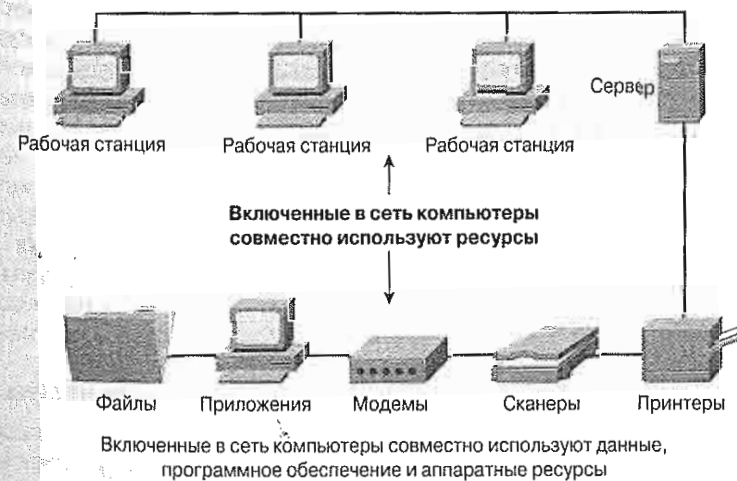


Рис. 16.4. Совместное использование ресурсов

В качестве серверов обычно используются крупные системы с дополнительной памятью для поддержки многих заданий, которые одновременно являются активными и резидентными в оперативной памяти. Серверам требуется дополнительное дисковое пространство для хранения совместно используемых файлов и для выполнения функций расширенной памяти в системе. Кроме того, серверам обычно требуются дополнительные слоты на материнских платах для подсоединения совместно используемых устройств, таких как принтеры и многочисленные сетевые интерфейсы.

Другим качеством систем, способных функционировать в качестве серверов, является их вычислительная мощность. Обычно компьютеры имеют один центральный процес-

сор CPU, который выполняет инструкции, решающие конкретную задачу или поддерживающие некоторый процесс. Для того, чтобы эффективно работать и быстро отвечать на запросы клиентов, сервер NOS должен иметь мощный процессор CPU. Однопроцессорные системы могут выполнять свои функции для большинства типов серверов в том случае, если они имеют достаточное быстродействие. Для увеличения быстродействия на некоторых системах устанавливаются дополнительные процессоры. Такие системы называются мультипроцессорными. Они могут выполнять несколько заданий одновременно, выделяя каждому заданию отдельный процессор. Мультипроцессорные системы значительно увеличивают объем работ, который может выполнить сервер.

Поскольку серверы выступают в качестве центрального источника ресурсов, которые жизненно важны для работы клиентских систем, как показано на рис 16.5, они должны быть не только эффективными, но и надежными. Термин “надежный” означает, что серверные системы должны быть способны эффективно работать при высокой нагрузке. Он также означает, что эти системы способны сохранять работоспособность в случае сбоя в одном или более процессах или компонентах без полной утраты работоспособности. Это достигается за счет избыточности, которая предусматривается при проектировании серверных систем. Под избыточностью понимается включение в систему дополнительных аппаратных компонентов, которые могут принять на себя выполнение функций других компонентов в случае выхода последних из строя. Избыточность является важной характеристикой отказоустойчивых систем, которые проектируются с учетом возможных сбоев и иногда могут даже ремонтироваться без прерывания работы. Поскольку работа операционной системы NOS зависит от непрерывной работы сервера, затраты на дополнительные аппаратные компоненты оказываются финансово оправданными.

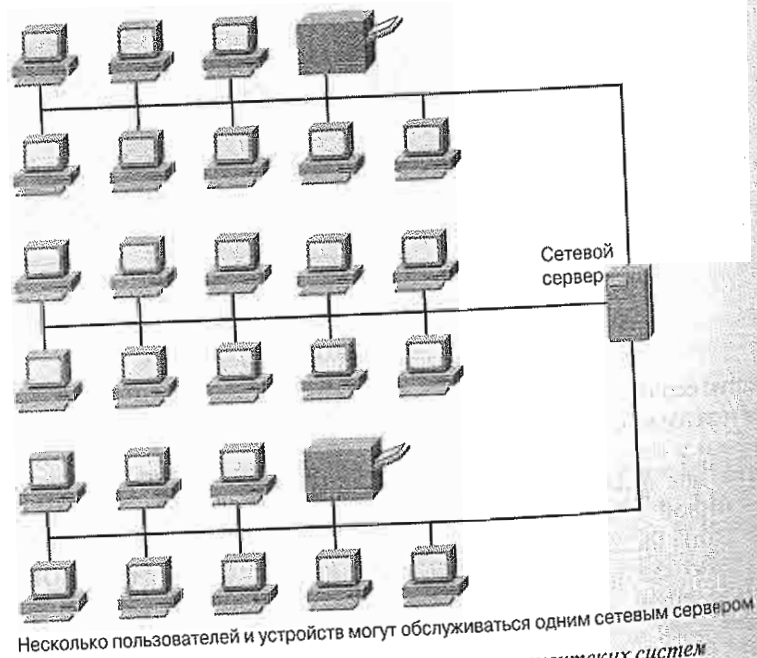


Рис. 16.5. Сервер поддерживает множество клиентских систем

Серверные приложения и функции включают в себя Web-службы, использующие протокол передачи гипертекста (Hypertext Transfer Protocol — HTTP) и службы идентификации узлов, использующие систему доменных имен (Domain Name System — DNS). Стандартные протоколы для электронной почты (e-mail), поддерживаемые серверами, включают в себя простой протокол передачи почты (Simple Mail Transfer Protocol — SMTP), почтовый протокол (Post Office Protocol — POP) и протокол доступа к сообщениям Internet (Internet Message Access Protocol — IMAP). В качестве протоколов совместного использования файлов используются сетевая файловая система Sun (Network File System — NFS) и модуль серверных сообщений (Microsoft Server Message Block — SMB).

Часто сетевые серверы также обеспечивают службы печати. Кроме того, они могут обеспечивать в сети службу протокола динамического конфигурирования хостов (Dynamic Host Configuration Protocol — DHCP), которая автоматически выделяет адреса протокола IP клиентским компьютерам. Кроме предоставления служб клиентам сети серверы могут также выполнять в сети функции базового брандмауэра. Это достигается путем использования прокси-сервера или трансляции сетевых адресов (network address translation — NAT); обе эти службы позволяют скрыть внутренние частные сетевые адреса со стороны сети Internet. Такие серверные приложения обычно не реализуются на рабочих станциях локальной сети LAN.

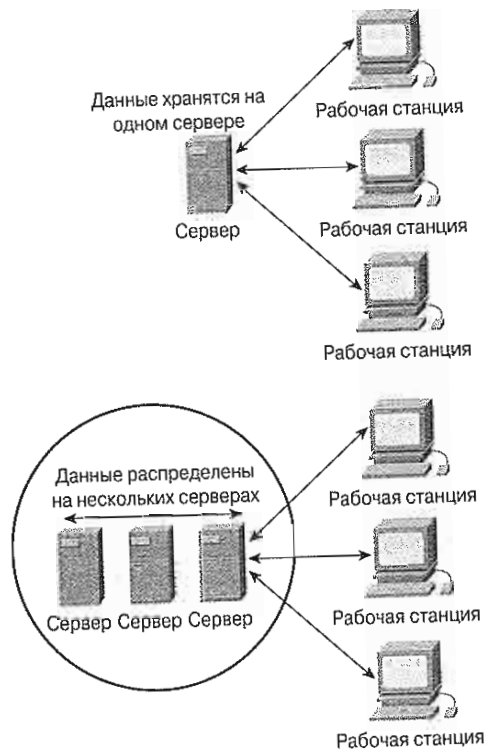
Один сервер, на котором работает NOS, эффективно работает лишь в том случае, когда он обслуживает небольшое число клиентов. Однако большинству организаций для достижения приемлемой производительности приходится использовать несколько серверов, как показано на рис. 16.6. Типичный подход к проектированию сети состоит в использовании нескольких серверов, каждый из которых отвечает за отдельную службу: за электронную почту, за совместное использование файлов, обеспечивает работу протокола FTP и т.д.

Концентрация сетевых ресурсов, таких как файлы, принтеры и приложения на серверах, как показано на рис. 16.7, также облегчает резервное копирование и поддержку генерируемых этими серверами данных. Вместо распределения этих ресурсов на отдельных компьютерах осуществляется их размещение на специализированных выделенных серверах, что облегчает доступ и резервное копирование.

Связи между клиентами и серверами

В модели “клиент-сервер” обработка данных происходит на нескольких компьютерах. Распределенная обработка позволяет осуществлять доступ к удаленным системам для совместного использования информации и сетевых ресурсов. В среде сети, построенной по модели “клиент-сервер”, клиент и сервер совместно используют данные и отвечают за их обработку. Для поддержки сетевых служб для пользователей большинство систем NOS проектируются на основе модели “клиент-сервер”. Компьютер, работающий в сети, может быть хостом, рабочей станцией, клиентом или сервером. Компьютер, на котором работает протокол TCP/IP, независимо от того, является ли он клиентом или сервером, рассматривается как компьютер-хост. Ниже приведен список основных моментов связи между клиентом и сервером.

- Локальным компьютером-хостом называется машина, на которой в настоящее время работает пользователь.
- Удаленным хостом называется система, к которой пользователь получает доступ из другой системы.
- Сервер предоставляет ресурсы одному или более клиентам через сеть.
- Клиентом называется компьютер, который использует службы одного или более серверов сети.



Данные могут быть размещены на одном сервере или распределены на нескольких серверах

Рис. 16.6. Среда сети, работающей по модели "клиент-сервер"

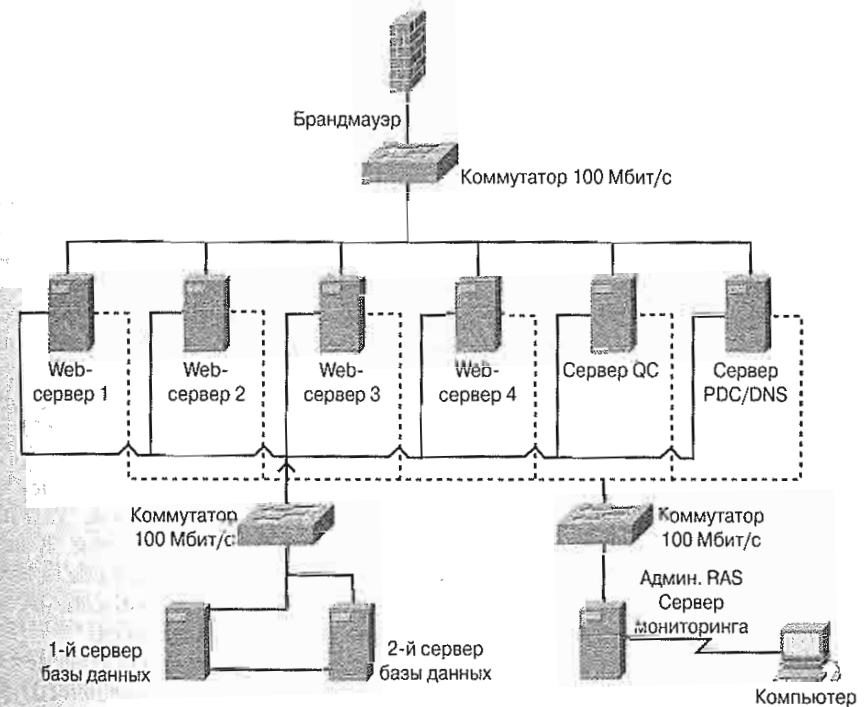


Рис. 16.7. Семейство серверов сети

Простым примером связи клиента с сервером может служить сеанс протокола FTP. Этот протокол является основным стандартным методом передачи файлов от одного компьютера другому. Для того, чтобы клиент мог передать файл серверу или получить файл от него, на сервере должен быть установлен "демон" или служба FTP. В этом случае клиент запрашивает у сервера передачу файлов. Сервер обеспечивает службы, необходимые для передачи или получения файла, как показано на рис. 16.8.

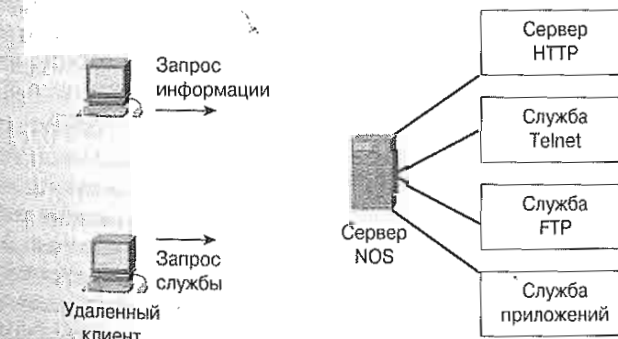


Рис. 16.8. Взаимодействие клиента и сервера

Другим наглядным примером распределенной обработки данных в среде “клиент-сервер” является сеть Internet. Клиент или компьютер переднего плана, обычно выполняет функции представления данных для пользователя, такие как форматирование данных на экране, создание форм ввода и редактирование данных. Это осуществляется с помощью браузера, такого как Netscape или Internet Explorer. Web-браузеры посылают запросы Web-серверам. Когда браузер запрашивает данные у сервера, последний отвечает и программа-браузер получает ответ от Web-сервера. После этого браузер отображает данные протокола HTTP в своем окне. Сервер, или компьютер заднего плана, обрабатывает запросы клиентов относительно Web-страниц и предоставляет службы HTTP или World Wide Web.

Другим примером связи по модели “клиент-сервер” может служить сервер базы данных и записи в ней или запрос клиента в локальной сети (local-area network — LAN). У клиента или на компьютере переднего плана может работать приложение, написанное на языке C или Java, а на сервере — программа Oracle или другое программное обеспечение управления базами данных. В этом случае клиент также может выполнять задания по форматированию и представлению данных для пользователя. Сервер при этом обеспечивает пользователю службы хранения данных, их поиска и выборки.

В типичной среде файлового сервера клиенту может потребоваться поиск в обширной области файлов базы данных для локальной обработки файлов. Этот поиск в файлах базы данных может вызвать избыточный поток данных в сети. В модели “клиент-сервер” клиент направляет запрос серверу; процессор сервера базы данных может обрабатывать порядка 100 000 записей в секунду и передавать клиенту лишь незначительный объем данных, удовлетворяющих требованиям запроса.

В качестве серверов обычно используются более мощные компьютеры, чем клиентские, и они лучше приспособлены для обработки больших объемов данных. В сети “клиент-сервер” большие базы данных хранятся на серверах и там же происходит обработка данных. Клиенту требуется лишь создать запрос серверу. При этом по сети передается лишь небольшой объем данных или результаты обработки запроса. Таким образом удовлетворяется запрос клиента и используется лишь небольшая часть полосы пропускания сети.

Распределение функций в сетях “клиент-сервер” дает существенные преимущества, однако влечет за собой также и определенные проблемы и затраты. Хотя концентрация ресурсов на серверных системах дает большую безопасность, упрощает доступ и координирует управление, вместе с тем сервер становится основной уязвимой точкой сети. Без работающего сервера вся сеть перестает функционировать. Кроме того администрирование и поддержка сервера требуют более квалифицированного персонала, что увеличивает затраты на поддержку работы сети. Сервера также требуют дополнительного аппаратного и специализированного программного обеспечения, что существенно увеличивает стоимость создания сети.

Сетевые операционные системы NOS

Операционная система компьютера является основой программного обеспечения, которая обеспечивает работу приложений и служб на рабочей станции. Аналогичным образом NOS позволяет осуществлять коммуникацию между устройствами и совместное использование ими сетевых ресурсов. Обычно NOS является операционной системой, которая работает на сервере, таком как сервер UNIX, сервер Microsoft Windows NT или сервер Windows 2003. В табл. 16.1 приведены различные операционные системы, предлагаемые этими компаниями.

Таблица 16.1. Сетевые операционные системы

Novell	UNIX	Windows	Linux
NetWare	HP-UX	NT	Red Hat
IntraNetWare	Sun Solaris	2003 Server	SCO
GroupWise	BSD	.NET Server	SuSE
	SCO		Debian
	AIX		Mandrake
			Xandros

На рабочей станции операционная система выполняет функции управления аппаратным обеспечением компьютера, средой выполнения программы и интерфейсом пользователя. Операционная система выполняет эти функции для отдельного пользователя или группы пользователей, которые обычно используют данный компьютер по очереди, а не одновременно. Администратор может создать учетные записи для нескольких пользователей, однако в каждый конкретный момент войти в систему может только один.

Вместе с тем NOS распределяет свои функции между несколькими компьютерами сети. Работа NOS зависит от локальной операционной системы, установленной на каждом компьютере. Она добавляет свои функции, которые позволяют компьютеру получать доступ к совместно используемым ресурсам сети многим пользователям на конкурентной основе.

Рабочие станции в среде операционной системы NOS функционируют как клиентские машины. Используя функции локальной операционной системы пользователь может получать доступ к локальным ресурсам данной рабочей станции. Эти ресурсы включают в себя приложения, файлы и непосредственно подсоединенные устройства, такие как принтеры. Когда рабочая станция становится клиентом в среде NOS, дополнительное специализированное программное обеспечение позволяет локальному пользователю получать доступ к удаленным ресурсам, которые не являются локальными, таким образом, как если бы эти ресурсы были частью локальной системы. Операционная система NOS расширяет возможности клиентской рабочей станции, делая доступными удаленные службы, которые становятся расширением собственной локальной операционной системы.

Хотя на рабочей станции могут иметь учетные записи несколько пользователей, в каждый конкретный момент времени активной является только одна учетная запись. Однако операционная система NOS поддерживает одновременно несколько активных учетных записей пользователей и предоставляет на конкурентной основе доступ к совместно используемым ресурсам многим клиентам. Серверы должны поддерживать работу многих пользователей и выступать в качестве хранилища ресурсов, совместно используемых многими клиентами. Серверам требуется специализированное программное обеспечение и дополнительное аппаратное обеспечение. Для получения конкурентного доступа к общим ресурсам компьютеры под управлением NOS принимают на себя специализированные роли. Клиентские системы имеют специализированное программное обеспечение, которое позволяет им запрашивать общие ресурсы, которые контролируются серверными системами, отвечающими на запросы клиентов. Система, которая может выполнять роль сервера NOS, должна быть способна поддерживать конкурентный доступ многих пользователей. Сетевой администратор создает учетную запись для каждого пользователя, которая позволяет ему присоеди-

ниться к сети и войти в нее. Учетная запись пользователя на сервере позволяет серверу аутентифицировать его и предоставить ему ресурсы, доступ к которым ему разрешен. Системы, которые обладают такой способностью, называются многопользовательскими.

Таковыми функциями обладают, в частности, операционные системы UNIX, Linux и Windows NT/Windows 2000/Windows XP.

Сервер NOS является многозадачной системой. С внутренней стороны операционная система должна быть способна выполнять несколько заданий или поддерживать несколько процессов одновременно. Серверные системы осуществляют это с помощью задающего расписание программного обеспечения, встроенного в среду выполнения заданий. Это программное обеспечение выделяет внутреннее процессорное время, память и другие элементы системы различным заданиям таким образом, чтобы они могли совместно использовать системные ресурсы. Для каждого пользователя во внутренней среде сервера выделяется отдельное задание или процесс. Эти внутренние задания создаются динамически, по мере подсоединения пользователей к системе и удаляются из нее при отсоединении пользователя.

Основными функциями, которые необходимо принять во внимание при выборе операционной системы NOS, являются производительность, средства управления и мониторинга, средства обеспечения безопасности, масштабируемость и надежность в сочетании с отказоустойчивостью. Все эти функции кратко рассматриваются в следующем разделе.

Производительность системы

Операционная система NOS должна обеспечивать высокую скорость операций чтения/записи файлов при обмене данными в сети между серверами и клиентами. Она должна быть способна поддерживать высокую производительность и при высокой нагрузке, когда многие, возможно, сотни клиентов осуществляют запросы. NOS должна отвечать на запросы клиентов на доступ к базам данных серверов, такие как запрос транзакции на извлечение записей из базы данных, которая хранится на серверной системе NOS. Устойчиво высокая производительность при большой нагрузке является важным требованием к операционной системе NOS.

Средства управления и мониторинга сети

Интерфейс управления на сервере NOS предоставляет средства для мониторинга работы сервера, администрирования клиентов, управления передачей файлов и печатью, а также хранением файлов на дисках. Он также предоставляет средства установки новых служб и их конфигурированием. Кроме того, серверы требуют регулярного мониторинга и настройки.

Безопасность в сети

Операционная система NOS должна обеспечивать защиту общих ресурсов, находящихся под ее управлением. Меры безопасности включают в себя аутентификацию пользователя перед использованием им ресурсов сети для предотвращения несанкционированного доступа. Функция обеспечения безопасности сети также выполняет шифрование данных для их защиты по время передачи между серверами и клиентами.

Масштабируемость

Под масштабируемостью сети понимается способность NOS обеспечить расширение сети без ухудшения ее производительности. Высокая производительность сети должна поддерживаться операционной системой NOS при добавлении новых пользователей и новых серверов для их поддержки.

Надежность/отказоустойчивость

Мерой надежности сети является ее способность предоставлять службы NOS при высокой нагрузке и поддерживать службы в случаях сбоя какого-либо компонента или прерывания процесса. Использование избыточных дисковых служб и балансирование нагрузки между несколькими серверами может повысить надежность и отказоустойчивость сети.

Операционные системы Windows NT, Windows 2000 Windows .NET

В настоящем разделе обсуждаются различные операционные системы NOS, предлагаемые корпорацией Microsoft.

ОС Windows NT Workstation была первой операционной системой для настольных компьютеров, предназначенной для рынка корпоративных сетей. ОС Windows NT 4 имеет интерфейс пользователя, аналогичный интерфейсу ОС Windows 95 и была предназначена для создания среды для критически важных коммерческих операций, которая была бы более устойчивой, чем операционные системы Microsoft для обычных потребителей.

Операционные системы Windows 2000

ОС Windows 2000 Professional является более поздней разработкой операционной системы Microsoft для корпоративных настольных систем. Как и программный продукт Windows 2000 Server, Windows 2000 имеет в качестве базы ядро NT и включает в себя много усовершенствованных функций. Например, Windows 2000 Professional обеспечивает высокий уровень безопасности и устойчивости для критически важных приложений. ОС Windows 2000 поддерживает технологию "plug-and-play". Она может быть установлена на жестких дисках, использующих файловую систему FAT32 и включает в себя шифрование файлов для защиты файлов на жестких дисках. Технология "plug-and-play" является полезным средством, позволяющим администратору быстро и легко добавлять в систему новые компоненты. Операционная система автоматически распознает их и устанавливает в системе соответствующие драйверы. В сущности после того как компонент "подсоединен" ("plugged") к системе, он начинает функционировать ("plays") без дополнительного конфигурирования со стороны системного администратора. До появления этой технологии при добавлении нового компонента к системе приходилось устанавливать драйверы и конфигурировать устройство вручную. В операционную систему Windows 2000 включена огромная база данных драйверов для типичных устройств, поддерживающих технологию "plug-and-play".

Среди других преимуществ Windows 2000 Professional, как операционной системы для настольных систем, следует отметить следующие.

- Эта операционная система обеспечивает лучшую поддержку мобильных пользователей с помощью усовершенствованного управления питанием (Advanced Power Management — APM) и усовершенствованного интерфейса конфигурирования и питания (Advanced Configuration and Power Interface — ACPI). Операционная система Windows NT не поддерживает интерфейс ACPI.
- ОС Windows 2000 Professional обеспечивает более высокий уровень безопасности для виртуальных частных сетей (Virtual Private Networking — VPN) с помощью туннельного протокола 2-го уровня (Layer 2 Tunneling Protocol — L2TP) и IP-протокола обеспечения безопасности (IP Security — IPSec). Прежние версии операционных систем Windows поддерживали для виртуальных частных сетей только туннельный протокол “точка-точка”.
- Функция автономных папок позволяет пользователям возможность копировать и синхронизировать документы, получаемые из сети, в локальной системе, с тем, чтобы к ним можно было получать доступ и в то время, когда компьютер не подсоединен к сети.
- Протокол печати в Internet (The Internet Printing Protocol — IPP) позволяет пользователю распечатать документ на устройство с заданным URL (uniform resource locator — URL) и управлять принтерами через интерфейс Web-браузера.
- Встроенные программы дефрагментации и другие средства и утилиты помогают пользователю поддерживать операционную систему и управлять ею. Для ОС Windows NT пользователю приходилось приобретать их отдельно.
- Эта операционная система поддерживает средства обеспечения безопасности Kerberos (разрабатываемый в настоящее время стандарт для аутентификации пользователей сети) и функции домена Windows 2000, такие как клиент активного каталога (Active Directory client).
- Она предлагает более простой и более эффективный вариант администрирования учетных записей (Account administration) чем у Windows 2000.

Административные задачи в Windows 2000 используют общую схему: консоль управления Microsoft (Microsoft Management Console — MMC). Это средство использует интегрируемые оснастки, которые представляют собой модули, содержащие средства для выполнения конкретных административных функций. Пользователи и группы создаются и управляются с помощью оснастки MMC Active Directory User and Computers. Получить доступ к ней можно с помощью последовательности команд меню: **Start**⇒**Programs**⇒**Administrative Tools**⇒**Active Directory Users and Computers**. В Windows 2000, в отличие от Windows NT 4.0, можно помещать такие объекты, как пользователи и ресурсы в контейнерные объекты, называемые организационными модулями (organizational unit — OU). Административные полномочия в отношении каждого модуля OU могут быть переданы пользователю или группе. Эта функция предоставляет более строгий контроль, чем это было возможно в ОС Windows NT 4.0.

Операционные системы Windows 2000 и 2003 Server

Операционные системы Windows 2000 и 2003 Server включают в себя: Windows 2000 Server, Windows 2000 Advanced Server и, в самое последнее время, Windows 2003 Server. Выбор наилучшей из перечисленных версий Windows Server определяется конкретными потребностями сети.

Windows 2000 Server

Операционная система Windows 2000 Server является идеальным выбором для малых и средних сетей и включает в себя много новых серверных функций. Windows 2000 Server имеет множество серверных функций, включающих в себя службы передачи файлов, печати и Web-сервера, а также серверные службы приложений. Отличием ОС Windows 2000 Server от предыдущих версий серверных операционных систем Microsoft является полный набор служб инфраструктуры, основанный на службах активного каталога (Active Directory). Служба активного каталога полностью интегрирована в ОС Windows 2000 Server и служит централизованной точкой управления пользователями, группами, службами безопасности и сетевыми ресурсами. Многие сетевые администраторы, знакомые с ОС Novell, вероятно, заметят сходство службы активного каталога Active Directory и служб каталогов Novell (Novell Directory Services).

ОС Windows 2000 Server может поддерживать режим симметричной мультипроцессорной обработки на 4 процессорах (Symmetric Multiprocessing — SMP) и позволяет использовать до 4 Гб физической памяти. По этой причине ОС Windows 2000 Server рекомендуется для использования в сетях среднего размера. Другим усовершенствованием, содержащимся в ОС Windows 2000 Server, является встроенная поддержка глобальных сетевых протоколов, которые широко используются в современных сетях, таких как TCP/IP и Internetwork Packet Exchange (IPX)/Sequenced Packet Exchange (SPX).

Windows 2000 Advanced Server

Операционные системы Windows 2000 Server и Windows 2000 Advanced Server практически идентичны, за исключением того, что Advanced Server поддерживает аппаратное и программное обеспечение, которое требуется администратору сети среднего предприятия. ОС Advanced Server представляет собой более мощную операционную систему сервера приложений, которая включает в себя все функции ОС Windows 2000 Server и добавляет к ним более высокие уровни доступности и масштабируемости, которые требуются крупным сетям. ОС Windows 2000 Advanced Server поддерживает симметричную многопроцессорную обработку (SMP), максимум восемь процессоров и является идеальным решением для интенсивной работы с базами данных. ОС Advanced Server также обеспечивает поддержку самого современного аппаратного обеспечения, поддерживающего *сети предприятия (enterprise network)*. Например, Advanced Server поддерживает более 4 Гб физической памяти.

Операционная система Windows 2003 Server

Корпорация Microsoft разработала операционную систему Windows 2003 Server, которая может служить в качестве безопасной и надежной операционной системы для поддержки Web-сайтов и FTP-сайтов на уровне предприятия и в этом качестве конкурировать с операционными системами Linux и UNIX Server. Однако Windows 2003 Server имеет и свои уникальные функции. Например, в связи с растущим количеством электронной торговли, основанных на Web компаний и компаний, расширяющих свои службы на всемирную сеть Internet, возникла необходимость в серверной операционной системе, которая была бы способна обеспечить безопасные и надежные Web-службы и службы передачи файлов по протоколу FTP. ОС Windows 2003 Server специально разрабатывалась на основе ядра Windows 2000 Server для поддержки таких видов служб. ОС Windows 2003 Server обеспечивает поддержку Web-служб XML (XML Web

Services) для компаний, имеющих средний и высокий объем передачи Web-данных. Эта функция предназначена для того, чтобы реализовать всю логику приложений на уровне сервера. В то же время настольные системы конечного пользователя выполняют только роль обычного терминала, который только отображает данные, полученные от сервера через соединение с Internet или интранет-сеть. Предполагается, что эта функция повысит уровень безопасности и надежности сети. ОС 2003 Server обеспечивает поддержку компаний, которые только начали свою работу в этой новой сфере бизнеса, а также компаний и предприятий, которые представляли коммерческие решения, основанные на использовании Internet, в течение последнего времени.

Операционные системы UNIX и Linux

Серверные операционные системы UNIX и Linux, хотя и имеют много схожих черт, обладают также отчетливыми различиями. В следующем разделе описываются различные версии операционных систем UNIX и Linux и приводятся примеры сред, для которых оптимальной является та или иная версия этих ОС. Выбор такой оптимальной версии для ее установки в сети определяется конкретными потребностями данной сети.

Происхождение ОС UNIX

Аббревиатура о UNIX относится к группе операционных систем, берущих свое начало в разработках лабораторий корпорации Bell, начатых в 1969 году. С самого начала ОС UNIX предназначалась для поддержки многих пользователей и мультитасочности. UNIX была также одной из первых операционных систем, включающих в себя поддержку работы в сети Internet. История ОС UNIX, насчитывающая ныне более 30 лет, достаточно сложна и запутанна, поскольку в ее разработке принимали участие многие компании и организации.

ОС UNIX была изначально написана на языке Ассемблер, который представляет собой примитивный набор инструкций, управляющих выполнением внутренних инструкций компьютера. Однако ОС UNIX могла работать только на конкретном компьютере. В 1971 году Деннис Ритчи (Dennis Ritchie) разработал язык программирования C. В 1973 году Ритчи и его коллега по лаборатории Bell программист Кен Томпсон (Ken Thompson) переписали программы системы UNIX на языке C. Поскольку язык C является языком высокого уровня, перенос системы UNIX на другой компьютер стал требовать гораздо меньше усилий программиста. Решение разработать такую переносную операционную систему оказалось ключевым для успеха этой операционной системы. В течение 70-х годов XX в. операционная система UNIX получила дальнейшее развитие благодаря работам программистов лабораторий корпорации Bell и нескольких университетов, особенно расположенного в Беркли (Berkeley) Калифорнийского университета.

Когда ОС UNIX впервые появилась на рынке операционных систем в 80-х годах XX в. она использовалась на мощных сетевых серверах, а не на настольных компьютерах. В настоящее время существуют десятки различных версий ОС UNIX, включая следующие:

- HP-UX (версия UNIX корпорации Hewlett Packard);
- Berkeley Software Design, Inc., (версия BSD UNIX, на основе которой были разработаны производные системы, такие как FreeBSD);
- Santa Cruz Operation (SCO) UNIX;
- Sun Solaris;
- AIX (версия UNIX корпорации IBM).

В целом ОС UNIX в ее различных формах продолжает упрочивать свои позиции в качестве надежной и безопасной операционной системы, особенно эффективной для критически важных приложений, от работы которой во многом зависит работа коммерческих и иных организаций. ОС UNIX также тесно интегрирована с протоколами TCP/IP. Сам стек протоколов TCP/IP в целом вырос из ОС UNIX в связи с потребностями коммуникаций между локальными сетями LAN и распределенными сетями (Wide-Area Network — WAN).

Операционная система корпорации Sun Microsystems Solaris Operating Environment и ее ядро, SunOS, представляет собой высокопроизводительную, универсальную 64-битовую реализацию ОС UNIX. ОС Solaris может работать на самых разных типах компьютеров — от персональных компьютеров на основе процессора Intel до мощных мэйнфреймов и суперкомпьютеров. В настоящее время ОС Solaris является наиболее широко используемой во всем мире версией UNIX для крупных сетей и Web-сайтов сети Internet. Корпорация Sun также является разработчиком технологии Java, построенной по принципу “Однажды написана, работает везде” (“Write Once, Run Anywhere”).

Несмотря на популярность операционных систем Microsoft Windows в корпоративных локальных сетях LAN, большинство Internet-серверов используют мощные системы UNIX. Хотя ОС UNIX обычно ассоциируется с дорогостоящим аппаратным обеспечением и поэтому считается “недружественным к пользователю”, последние разработки, включая создание операционной системы Linux, изменили это представление.

Происхождение операционной системы Linux

В 1991 году финский студент по имени Линус Торвалдс (Linus Torvalds) начал работу над новой операционной системой для персонального компьютера на базе процессора Intel 80386. Неудовлетворенный состоянием и возможностями настольных операционных систем, таких как DOS, и высокой стоимостью и трудностями с лицензированием, связанными с коммерческой ОС UNIX, Торвалдс поставил перед собой задачу создать операционную систему, которая была бы подобна UNIX по своим возможностям, но использовала бы открытый программный код и была абсолютно бесплатна.

Хотя это и не было его первоначальным намерением, работа Торвалдса привела к объединению усилий программистов во всем мире с целью создания ОС Linux — операционной системы с открытым кодом, которая бы выглядела и работала подобно ОС UNIX. К концу 90-х годов операционная система Linux стала конкурентоспособной альтернативой ОС UNIX в сфере серверных операционных систем и ОС Windows в сфере операционных систем для настольных компьютеров. Популярность Linux для настольных персональных компьютеров также повысила интерес к использованию дистрибути-

вов UNIX, таких как FreeBSD и Sun Solaris в настольных системах. Различные версии Linux могут в настоящее время работать практически на любом 32-разрядном процессоре, включая Intel 80x86, Motorola 68000, Alpha и PowerPC.

Как и UNIX, Linux имеет множество версий. Некоторые из них могут быть бесплатно загружены из Internet, другие распространяются коммерческим путем. Ниже приведены несколько наиболее популярных версий ОС Linux:

- RedHat Linux, распространяемая RedHat Software
- SCO Linux, распространяемая SCO
- Xandros Linux
- Slackware
- Debian GNU/Linux
- SuSE Linux

Linux является одной из наиболее мощных и надежных операционных систем. Вследствие этого Linux уже попытался вторгнуться на рынок платформ для крупных сетей и на рынок серверов для предприятий. Значительно реже Linux используется в качестве корпоративной настольной операционной системы.

Хотя для Linux были разработаны графические пользовательские интерфейсы (Graphical User Interface — GUI), которые делают ее более дружелюбной к пользователю, большинство начинающих считают Linux более трудным в использовании, чем операционные системы MacOS or Windows. В настоящее время многие компании (такие как RedHat, SuSE, SCO и Xandros) прилагают усилия к тому. Чтобы сделать Linux эффективной операционной системой для настольных персональных компьютеров.

Когда ОС Linux будет реализована в качестве операционной системы для настольных систем, возникнет вопрос о поддержке приложений для нее. По сравнению с ОС Windows количество коммерчески продуктивных приложений для Linux сравнительно невелико. Однако некоторые разработчики предлагают программное обеспечение, которое эмулирует Windows-среду (такие как ABI и WINE). Это позволяет запускать в среде Linux приложения для ОС Windows. Кроме того, такие компании, как Corel и Borland, создают Linux-версии своих офисных программных пакетов и других популярных программ.

Работа в сети ОС Linux

Последние дистрибутивы ОС Linux имеют встроенные сетевые компоненты для подсоединения к локальным сетям LAN, установки удаленных соединений с сетью Internet или с другой удаленной сетью. Фактически стек протоколов TCP/IP интегрирован в ядро ОС Linux вместо реализации его в виде отдельной подсистемы.

Ниже описаны некоторые преимущества ОС Linux в качестве настольной операционной системы и сетевого клиента.

- Linux является подлинной 32-битовой операционной системой.
- Она поддерживает приоритетную многозадачность и виртуальную память.
- Код системы является открытым и доступен каждому для усовершенствования и улучшения.

- Согласно генеральной общественной лицензии (General Public License — GPL) GNU эта операционная система доступна бесплатно, как и другие версии ОС UNIX, такие как FreeBSD и NetBSD. ОС Linux является программным обеспечением с открытым кодом. Это означает что код-источник общедоступен и может быть модифицирован пользователем для его индивидуальных потребностей. ОС Linux может также свободно распространяться между пользователями. Такой подход прямо противоположен концепции коммерческого программного обеспечения, в которой исходный код не является общедоступным и каждый пользователь должен оплачивать лицензию на право использования данного программного продукта. Коммерческое программное обеспечение основано на авторском праве, которое ограничивает право пользователя вносить изменения в исходный код и распространять копии своего экземпляра. ОС Linux может быть бесплатно загружена с многих Web-сайтов.

Распространение ОС Linux

Многие коммерческие компании и некоммерческие организации распространяют ОС Linux вместе с различными комбинациями приложений, утилит и другого программного обеспечения. Такие комбинации операционной системы и программного обеспечения называются дистрибутивами. Например, компания Red Hat, Inc. предлагает на компакт-дисках программный пакет, включающий в себя ОС Linux, исходный код и руководства вместе с набором приложений и других программных продуктов за умеренную плату. Эти дополнительные продукты включают в себя набор офисных программ, графических приложений, программное обеспечение Web-сервера и т.д. Имеется также поддержка пользователей. Пакет Red Hat включает также программное обеспечение Sun StarOffice.

Первичным компонентом любого дистрибутива является ядро Linux. Кроме ядра и приложений дистрибутив также включает в себя средства инсталляции, загрузчик и программы-утилиты. Некоторые дистрибутивы имеют графическую оболочку и ориентированы на начинающего пользователя. Другие ближе к базовой версии и предназначены для разработчиков и пользователей, уже знакомых с ОС UNIX.

Ниже приводится алфавитный список некоторых наиболее распространенных дистрибутивов Linux и Web-сайты, с которых их можно загрузить.

- SCO openLinux — www.sco.com
- Xandros Desktop Linux — www.xandros.com
- Debian GNU/Linux — www.debian.org
- Mandrake Linux — www.mandrakelinux.com
- Red Hat Linux — www.redhat.com
- Slackware Linux — www.slackware.com
- SuSE Linux — www.suse.com
- Turbo Linux — www.turbolinux.com
- United Linux — www.unitedlinux.com

Графические интерфейсы пользователя (GUI) для ОС Linux/UNIX

Обе ОС — UNIX и Linux могут работать с графическими интерфейсами GUI. Поскольку существует много различных версий UNIX и Linux, имеются, соответственно, буквально десятки популярных графических интерфейсов, из которых может выбирать пользователь. Например, при установке ОС Red Hat 8.x по умолчанию устанавливается GNOME Desktop Environment (рис. 16.9), который используется как стандартный графический интерфейс для всех пользователей.

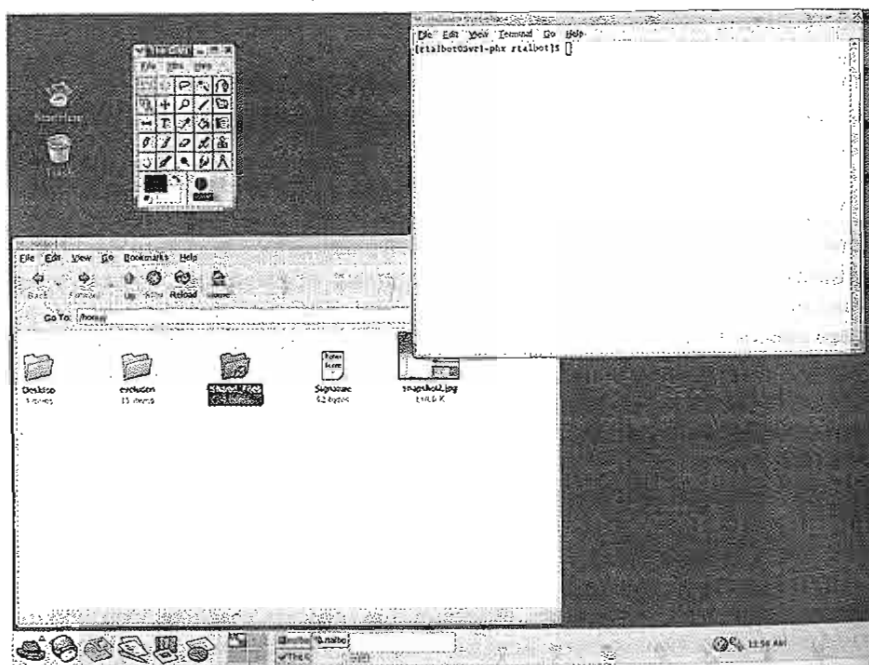


Рис. 16.9. Графический интерфейс GNOME

Хотя для ОС Linux могут быть сконфигурированы другие графические интерфейсы, такие, например, как K Desktop Environment (KDE), показанный на рис. 16.10, интерфейс GNOME в настоящее время становится «стандартным» графическим интерфейсом для ОС UNIX и Linux. При отображении графического интерфейса обе операционные системы Linux и UNIX опираются на базовую систему X Window System. Эта система представляет собой программное обеспечение, которое взаимодействует с системным аппаратным обеспечением и с графическими приложениями, включая диспетчер окон. Диспетчер окон представляет собой программное обеспечение, отвечающее за установку размеров окон, в которых работают другие программы, их расположение на экране и прорисовку.

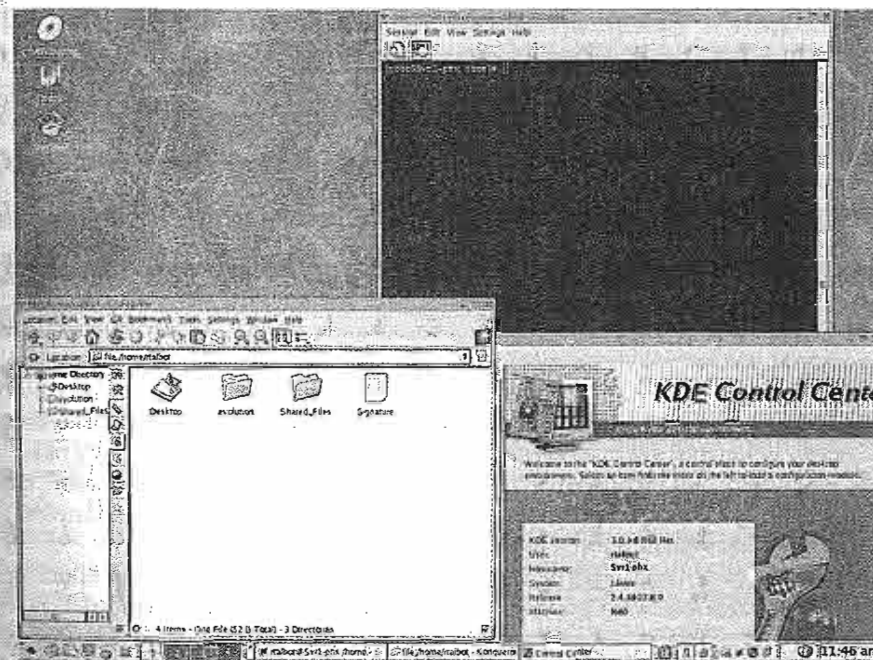


Рис. 16.10. Графический интерфейс KDE

Операционная система Macintosh OS X

Компьютеры корпорации Apple Macintosh были предназначены для облегчения работы в одноранговых сетях (в рабочих группах). Фактически сетевые интерфейсы являются частью аппаратных и сетевых компонентов, встроенных в операционную систему Macintosh. Для систем Macintosh имеются также сетевые адаптеры Ethernet и Token Ring.

Система Macintosh, или просто Mac, популярна во многих образовательных учреждениях и в отделах корпораций, использующих графические приложения. Компьютеры Mac могут быть соединены друг с другом, образуя рабочую группу, и совместно работать с файловыми серверами AppleShare. Они также могут образовывать локальную сеть персональных компьютеров, включающую в себя серверы Microsoft, NetWare или UNIX. Операционная система Macintosh, Mac OS X, иногда называется Apple-системой 10 (Apple-system 10). Некоторые функции ОС MAC OS X реализованы в графическом интерфейсе (GUI), называемом Aqua. Этот интерфейс можно назвать гибридом графических интерфейсов ОС Microsoft Windows XP и Linux X Window System. ОС MAC OS X предназначена для выполнения таких функций как навигация в Internet, редактирование видео и фотоизображений, игры на домашнем компьютере, предоставляя, вместе с тем, функции, реализующие мощные и допускающие индивидуальную настройку средства, требуемые профессионалам IT от операционной системы. ОС MAC OS X полностью совместима с прежними версиями операционных систем MAC.

ОС MAC OS X предоставляет пользователю новую функцию, позволяющую осуществлять соединения сетей AppleTalk и Windows. Ядром MAC OS X является мощная операционная система Darwin, основанная на ОС UNIX и обеспечивающая вы-

сокую устойчивость и производительность. Усовершенствованные функции MAC OS X включают в себя защищенную память, приоритетную многозадачность, усовершенствованное управление памятью и поддержку симметричного многопроцессорного режима. Это делает ОС Mac OS X серьезным конкурентом на рынке операционных систем.

Концепция серверной службы

Сетевые операционные системы NOS предназначены для поддержки сетевых процессов для клиентов и одноранговых устройств. Сетевые службы включают в себя навигацию в World Wide Web, совместное использование файлов, электронную почту, службу каталогов, удаленное управление и службу печати. Удаленное управление представляет собой мощную службу, которая позволяет сетевому администратору конфигурировать сетевые системы, находящиеся от него на расстоянии в несколько километров. Следует отметить, что эти сетевые процессы называются по-разному в различных ОС — например, они называются “службами” в Windows 2000 и “демонами” в ОС UNIX и Linux. По существу, они выполняют одни и те же функции, однако способ их загрузки и режим взаимодействия с NOS различны в разных ОС.

В зависимости от типа NOS некоторые из этих ключевых сетевых процессов могут быть активизированы по умолчанию уже при установке ОС. Наиболее популярные сетевые процессы в своей работе опираются на стек протоколов TCP/IP. Поскольку TCP/IP является открытым и широко известным набором протоколов, основанные на нем службы особенно подвержены несанкционированному сканированию и враждебным атакам. Такие атаки, как “отказ в обслуживании” (Denial-of-service — DoS), внедрение компьютерных вирусов и быстро распространяющихся Internet-червей (Internet worms) заставили проектировщиков NOS пересмотреть свои представления о том, какие сетевые службы должны устанавливаться и активизироваться автоматически.

Последние версии популярных сетевых операционных систем, такие как Windows 2000 и Red Hat Linux 8.X, ограничивают количество сетевых служб, которые “включаются” по умолчанию. При установке NOS ключевые службы следует конфигурировать и активизировать вручную.

Если пользователю требуется выполнить печать в сетевой среде, поддерживающей службу печати, то задание отправляется в соответствующую очередь на выбранный принтер. Поступающие задания на печать устанавливаются в очередь и обслуживаются по принципу “первым пришел — первым ушел” (first-in, first-out — FIFO). Это означает, что при добавлении в очередь нового задания оно помещается в конец списка заданий ожидающих печати и распечатываются после того, как выполнены все предшествующие задания. Время ожидания может оказаться достаточно длительным, в зависимости от объема заданий находящихся в очереди перед данным заданием. Сетевая служба печати предоставляет системному администратору необходимые средства для управления большим количеством заданий на печать, поступающих из всех областей сети. Эти средства позволяют задавать приоритеты, паузы и даже отмену заданий печати, ожидающих своей очереди.

Совместное использование файлов

Возможность совместного использования файлов является важной сетевой службой. В настоящее время используется большое количество протоколов и приложений, позволяющих осуществлять такое совместное использование. В корпоративных или домашних сетях совместное использование файлов обычно осуществляется с помощью протоколов Windows File Sharing или Network File Sharing. В таких средах конечный пользователь может даже не знать где расположен данный файл — на локальном жестком диске или на удаленном сервере. Протоколы Windows File Sharing и Network File Sharing позволяют пользователю легко осуществлять операции по перемещению, созданию или удалению файлов в удаленных каталогах.

Протокол FTP и передача файлов

Многие организации делают доступными свои файлы для удаленных сотрудников, потребителей и вообще любым пользователям с помощью протокола передачи файлов FTP. Службы FTP становятся доступными любым пользователям через Web-службы. Например, пользователь может выйти на Web-сайт, прочитать на Web-странице о произошедшем обновлении программного обеспечения и загрузить это обновленное программное обеспечение с помощью протокола FTP. Небольшие компании часто используют для служб FTP и HTTP один сервер, в то время как крупные компании часто выделяют для служб FTP выделенные серверы.

Хотя клиенты протокола FTP должны вводить свои аутентификационные данные, многие FTP-серверы сконфигурированы для анонимного доступа. При автономном доступе к серверу пользователю не требуется иметь в системе свою учетную запись. Протокол FTP позволяет пользователю загружать свои файлы на сервер, переименовывать их и удалять, поэтому сетевой администратор должен быть аккуратным при конфигурировании сервера FTP и устанавливать определенные уровни доступа пользователей.

FTP является протоколом, ориентированным на сеансы. Клиент должен открыть сеанс на уровне приложения, выполнить аутентификацию (ввести свои аутентификационные данные), а затем выполнить требуемые ему действия, такие как загрузка файлов на свой компьютер или, наоборот, на сервер. Если сеанс пользователя в течение заданного времени не активен, то сервер может отключать клиента. Это время бездействия называется интервалом простоя (idle timeout). Этот интервал простоя протокола FTP зависит используемого программного обеспечения.

Web-службы

В настоящее время “Всемирная паутина” (World Wide Web) является самой заметной сетевой службой. Менее чем за десятилетие она стала глобальной сетью распространения информации, электронной торговли, образования и развлечений. Миллионы компаний, организаций и отдельных пользователей поддерживают свои Web-сайты в Internet. Эти Web-сайты представляют собой наборы Web-страниц, которые хранятся на сервере или на группе серверов.

World Wide Web основана на модели “клиент-сервер”. В начале работы клиент пытается установить сеанс с Web-сервером. После того как сеанс установлен, клиент может запросить данные на сервере. Обычно управление запросами клиентов и передачей ин-

формации с сервера осуществляет протокол HTTP. В процессе роста Web-службы стали включать в себя не только протокол HTML, который транслируется Web-браузером и передает Web-страницы которые читает пользователь, но и генерирование сценариев XML, которые используются компьютерными программами. Ранее при описании работы сервера Microsoft .NET обсуждался вопрос о том, как серверы используют сценарии XML с Web-службами. Программное обеспечение Web-клиента включает в себя Web-браузеры с графическим интерфейсом (GUI), такие как Netscape Navigator или Internet Explorer. Web-страницы располагаются на компьютерах, на которых работает программное обеспечение Web-служб. Двумя наиболее часто используемыми пакетами программного обеспечения Web-серверов являются Microsoft Internet Information Services (IIS) и Apache Web Server. Пакет Microsoft IIS может работать только на платформах Windows, в то время как Apache Web Server обычно используется на платформах UNIX и Linux.

Имеются десятки других Web-серверных программ. Какой-либо тип Web-службы имеется практически для любой используемой в настоящее время операционной системы.

Служба DNS

Служба DNS преобразует имя в Internet (такое, например, как www.cisco.com) в соответствующий IP-адрес. Многие приложения в своей работе опираются на службы каталогов, которые предоставляет им служба DNS. Имена удаленных систем используются Web-браузерами, программами электронной почты и передачи файлов.

Протокол DNS позволяет этим клиентам осуществлять запросы в их сетях на серверы DNS на трансляцию имен в IP-адреса. Приложения могут использовать эти адреса для отправки своих сообщений. Без этой службы каталогов было бы практически невозможно использовать Internet.

Служба DHCP

Назначение службы DHCP состоит в предоставлении возможности индивидуальным компьютерам в IP-сети узнавать свои конфигурационные данные протокола TCP/IP от сервера или нескольких серверов DHCP. Эти серверы DHCP не имеют точной информации об индивидуальных компьютерах до тех пор, пока не поступит запрос об информации.

Основной целью работы этой службы является уменьшение объема работы сетевого администратора в крупной IP-сети. Наиболее важной частью информации, распространяемой таким образом, является IP-адрес, который идентифицирует узел или станцию в сети. Служба DHCP также позволяет восстанавливать и автоматически обновлять сетевые IP-адреса с помощью механизма аренды адресов. Этот механизм выделяет IP-адреса на какой-то период времени, затем освобождает его и при необходимости назначает новый IP-адрес. Эти операции выполняются сервером DHCP, что значительно экономит время системного администратора.

Управление сетью

По мере того, как сеть развивается и расширяется, она становится все более важным и необходимым ресурсом организации, как показано на рис. 16.11. Однако чем больший объем ресурсов предоставляет сеть своим пользователям и чем сложнее она

становится, тем больше становится вероятность каких-либо сбоев или неполадок. Однако нехватка сетевых ресурсов или просто невысокая производительность сети являются неприемлемыми для пользователей. Сетевым администратором должен активно управлять сетью, диагностировать возникающие проблемы, предотвращать неблагоприятные ситуации и обеспечивать наивысшую возможную производительность сети. На каком-то этапе сеть становится слишком большой для того чтобы эти задачи могли быть решены сетевым администратором и требуют использования средств автоматического управления сетью.

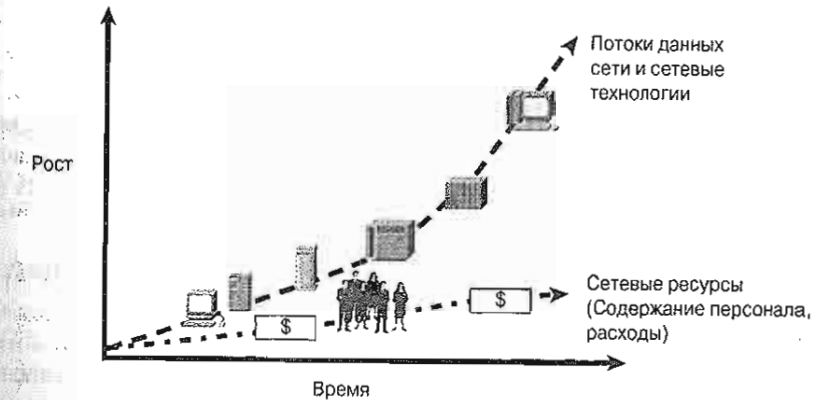


Рис. 16.11. Эволюция сети

Управление сетью включает в себя приведенные ниже аспекты.

- Мониторинг доступности сети.
- Усовершенствованная автоматизация.
- Мониторинг времени отклика сети.
- Обеспечение безопасности в сети.
- Перенаправление потоков данных.
- Возможность восстановления работоспособности сети.
- Регистрация новых пользователей.

В качестве движущих мотивов введения автоматического управления сетью выступают описанные ниже факторы.

- **Управление корпоративными ресурсами** — без эффективного контроля сетевых ресурсов они не будут давать той отдачи, которая требуется организации.
- **Контроль сложной структуры сети** — в результате существенного роста числа сетевых компонентов, пользователей, интерфейсов, протоколов и типов оборудования от разных производителей возникает угроза утраты контроля над сетью и ее ресурсами, что может сделать невозможным управление сетью.
- **Усовершенствование предоставляемых служб** — пользователи ожидают сохранения или даже улучшения качества служб несмотря на рост сети и повышение уровня распределенности ресурсов.

- **Сбалансированность выполнения различных требований к сети** — приложениям пользователей должен обеспечиваться определенный уровень поддержки с конкретными требованиями по производительности, доступности и безопасности.
- **Сокращение времени простоев** — внесение при проектировании сети определенной степени избыточности позволяет добиться высокого уровня доступности ресурсов.
- **Контроль расходов** — мониторинг использования сетевых ресурсов и управление ими позволяет удовлетворять потребности пользователя с приемлемым уровнем затрат.

Эталонная модель OSI и модель управления сетью

Для выполнения описанных выше требований потребовался более глубокий анализ происходящих в сети процессов. Международная организация по стандартизации (International Organization for Standardization — ISO) создала комитет для разработки модели сетевого управления под руководством группы OSI.

Эта модель включает в себя четыре части:

- организационную;
- информационную;
- коммуникационную;
- функциональную.

На рис. 16.12 проиллюстрирован структурный подход к сетевому управлению от верхнего уровня к нижнему, при котором основная модель делится на четыре субмодели. Эта модель признана стандартом группы OSI.

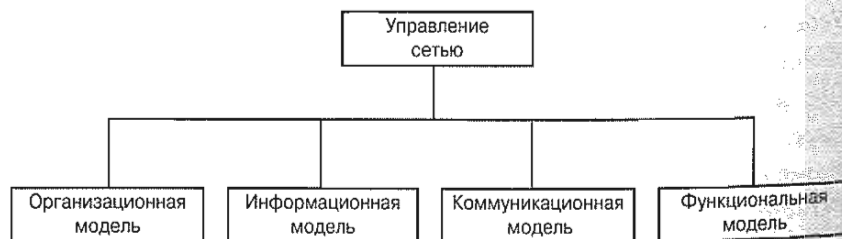


Рис. 16.12. Модель управления сетью

Организационная модель описывает компоненты управления сетью (менеджер, агент и т.д.) и связи между ними. Расположение этих компонент приводит к разработке различных типов архитектуры сети, которые будут рассмотрены далее.

Информационная модель описывает структуру и способ хранения информации управления сетевыми объектами. Эта информация хранится в базе данных, называемой информационной базой управления (Management Information Base — MIB). Для определения синтаксиса и семантики управляющей информации, хранящейся в базе MIB, используется промышленный стандарт структуры управляющей информации (Structure of Management Information — SMI). База MIB и структура SMI будут более подробно описаны далее.

Коммуникационная модель описывает передачу данных управления между агентом управления и менеджером. Она включает в себя транспортный протокол, протокол приложений, команды, применяемые для связи и ответы на них.

Функциональная модель включает в себя приложения управления сетью, относящиеся к системе управления сетью (network management system — NMS). Модель управления сетью OSI определяет пять функциональных зон (иногда называемых моделью FCAPS):

- ошибки;
- конфигурация;
- учет;
- производительность;
- безопасность.

Эта модель управления сетью получила широкое признание у производителей как удобный и полезный способ описания требований к любой системе управления сетью.

Стандарты: SNMP и CMIP

Для того, чтобы стало возможным общее управление сетями с различными платформами, необходимы стандарты управления сетями, которых бы придерживались производители, реализуя их в своих продуктах. Возникли два основных стандарта:

- **Простой протокол управления сетью (SNMP)** — сообщество IETF;
- **Общий протокол информации управления (Common Management Information Protocol — CMIP)** — сообщество телекоммуникаций (Telecommunications Community).

Аббревиатура SNMP в действительности относится к набору стандартов управления сетями, включающего в себя протокол, спецификацию структуры базы данных и набор объектов для данных. Протокол SNMP был принят в качестве стандарта для объединенных сетей TCP/IP (TCP/IP Internets) в 1989 году и стал весьма популярным. Обновление этого протокола, известное как версия 2c (SNMP version 2c — SNMPv2c), было принято в 1993 году. Протокол SNMPv2c поддерживает централизованное и распределенное управление сетью и включает в себя усовершенствования в SMI, в протокольных операциях, в архитектуре управления и в обеспечении безопасности. Он был предназначен для использования в сетях на базе OSI, а также в сетях на основе протокола TCP/IP.

С тех пор была создана новая версия этого протокола — SNMPv3. Для устранения недостатков версий SNMPv1 и SNMPv2c, в версии SNMPv3 обеспечивается безопасный доступ к базе MIB с использованием аутентификации при получении доступа и шифровании пакетов при их передаче по сети. Протокол CMIP представляет собой протокол управления сетью группы OSI, созданный и стандартизованный организацией ISO для мониторинга и управления гетерогенными сетями.

Функционирование протокола SNMP

Протокол SNMP является протоколом уровня приложений и предназначен для облегчения обмена информацией управления между устройствами сети. Используя протокол SNMP для получения доступа к информации управления, отражающей

объем передачи на интерфейс или на ряд открытых TCP-соединений в пакетах в секунду, сетевым администраторам становится легче управлять производительностью сети, обнаруживать и разрешать возникающие в ней проблемы. В настоящее время протокол SNMP является наиболее популярным протоколом для управления различными коммерческими, университетскими и исследовательскими объединенными сетями. Стандартизация процессов управления сетями продолжается несмотря на то, что производители разрабатывают и выпускают на рынок свои фирменные приложения для управления сетью, основанные на протоколе SNMP. Протокол SNMP сравнительно прост, однако его набор функций достаточно эффективен для разрешения сложных проблем, которые могут возникать в процессе управления гетерогенными сетями.

Организационная модель сетевого управления на основе протокола SNMP включает в себя четыре элемента:

- станция управления сетью;
- агент управления;
- база данных управления (MIB);
- протокол управления сетью.

Станция NMS обычно представляет собой отдельную рабочую станцию, однако может быть реализована и для нескольких систем. Станция NMS включает в себя набор программных продуктов, который называется приложением управления сетью. Это приложение включает в себя графический интерфейс GUI, который позволяет авторизованным сетевым менеджерам управлять сетью. Оно отвечает на команды пользователя и другие полученные команды, предназначенные для агентов управления во всей сети. Агентами управления являются ключевые сетевые платформы и устройства, другие узлы маршрутизации станции, маршрутизаторы, мосты и концентраторы, на которых установлен протокол SNMP, в результате чего ими можно управлять. Они отвечают на запросы информации и на запросы действий от станций NMS (опрос) и могут предоставлять станциям NMS важную информацию и без соответствующего запроса (с помощью команд `trap`). Вся информация управления сетью конкретного агента хранится в базе MIB этого агента. Агент может вести сбор и учет следующей информации:

- количество и состояние его виртуальных каналов (*circuits*);
- количество полученных сообщений об ошибках различных типов;
- количество байтов и пакетов полученных устройством и отправленных им;
- максимальная длина выходной очереди (для маршрутизаторов и других устройств объединенных сетей);
- количество полученных и отправленных широковебательных сообщений;
- информация об отключенных и новых включенных интерфейсах.

Станция NMS выполняет функцию мониторинга, путем извлечения соответствующих значений из своей базы MIB. Станция NMS может вызвать выполнение у агента определенных действий или изменить конфигурацию агента. Связь между менеджером и агентом осуществляется с помощью протокола управления сетью

уровня приложений. Протокол SNMP функционирует через протокол UDP, используя порт 151/152. Связь между менеджером и агентом основана на обмене сообщениями. Основными являются три типа сообщений:

- **сообщение Get** — это сообщение позволяет станции управления извлечь значение объекта базы MIB от агента;
- **сообщение Set** — позволяет станции управления установить значение объекта базы MIB у агента;
- **сообщение Trap** — по этому сообщению агент уведомляет станцию управления о значительных событиях.

Такую модель называют двухуровневой (*two-tier*) (рис. 16.13). При этом, однако, предполагается, что все элементы сети могут управляться протоколом SNMP. Однако это не всегда так, поскольку некоторые устройства могут иметь фирменный интерфейс управления. В таких случаях используется трехуровневая модель, показанная на рис. 16.14. Сетевой менеджер, которому требуется получить информацию от такого фирменного узла или управлять им, осуществляет связь с прокси-агентом. Этот прокси-агент транслирует запрос менеджера в форму, соответствующую запрашиваемой системе и использует соответствующий ей фирменный протокол управления для связи с ней. Ответ или отклик запрашиваемой системы аналогичным образом вновь транслируется в сообщения протокола SNMP и передается менеджеру.

Другим типичным приложением управления сетью является передача некоторых функций управления сетью модулю удаленного мониторинга (*Remote Monitoring — RMON*), который локально собирает информацию, после чего менеджер периодически запрашивает у него и получает собранную информацию.

Станция NMS представляет собой обычную рабочую станцию, на которой работает обычная операционная система, как показано на рис. 16.15. Она обычно имеет достаточно большой объем оперативной памяти RAM для того, чтобы в ней могли работать все приложения управления сетью, работающие одновременно. У менеджера работает обычный стек сетевых протоколов, такой как TCP/IP. Работа приложений управления сетью базируется на операционной системе узла и архитектуре коммуникации. В качестве примеров приложений управления сетью можно привести CiscoWorks2000, HP OpenView и SNMPc.

Как уже говорилось выше, менеджер может быть отдельной централизованной рабочей станцией, которая рассылает запросы всем агентам, независимо от того, где они расположены, как показано на рис. 16.16. В распределенной сети более целесообразно использование децентрализованной архитектуры, с локальной станцией NMS на каждом узле. Эти распределенные станции NMS могут работать в архитектуре «клиент-сервер», в которой одна станция NMS выступает в качестве ведущего сервера, а другие выполняют роль клиентов, которые передают данные ведущему серверу для централизованного хранения как показано на рис. 16.17. Альтернативным является вариант в котором все распределенные станции NMS играют одинаковые роли; при этом каждая из них имеет свои собственные базы данных и, таким образом, информация управления сетью распределена между одноранговыми станциями NMS, как показано на рис. 16.18.

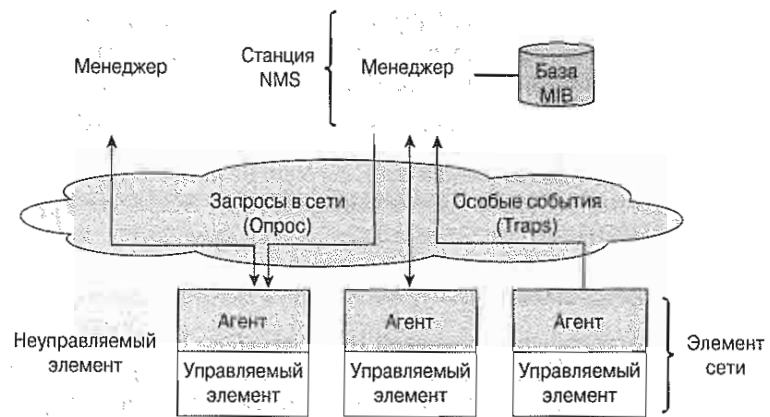


Рис. 16.13. Двухуровневая модель сетевого управления



Рис. 16.14. Трехуровневая модель сетевого управления

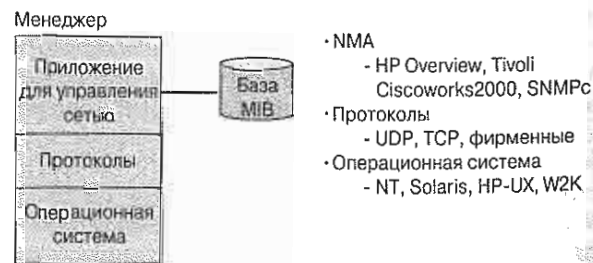


Рис. 16.15. Организационная модель



Рис. 16.16. Централизованная структура управления сетью

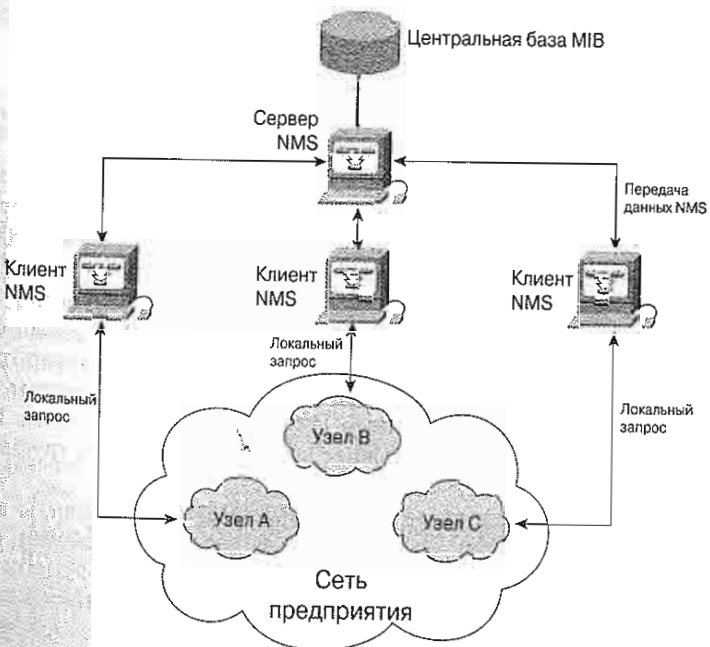


Рис. 16.17. Иерархическая структура управления сетью

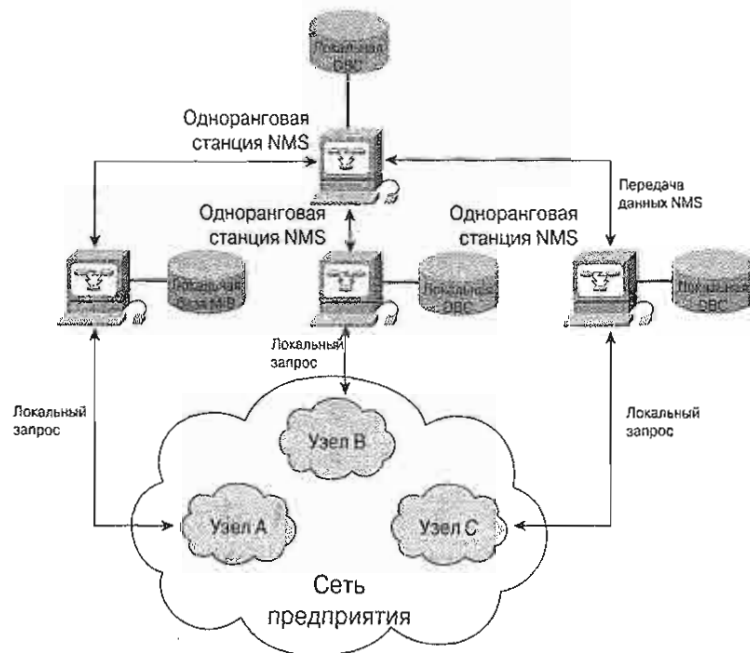


Рис. 16.18. Распределенная структура управления сетью

Структура информации управления сетью и баз данных MIB

База MIB используется для хранения структурированной информации, описывающей элементы сети и их атрибуты. Эта структура определена в интерфейсе SMI, который определяет типы данных которые могут быть использованы для хранения объектов, имена этих объектов и способ их кодировки для передачи по сети.

Базы MIB могут быть глубоко структурированными хранилищами информации об устройствах сети. Существует много стандартных баз MIB, однако большинство фирменных баз MIB используются только для устройств конкретного производителя. Базы MIB первоначального интерфейса SMI были распределены по восьми различным группам, в целом насчитывающим 114 управляемых объектам. При определении баз MIB-II, заменяющих в настоящее время базы MIB-I, к группам были добавлены новые группы.

Все управляемые объекты в среде протокола SNMP организованы в иерархическую или древовидную структуру, как показано на рис. 16.19. Объекты, являющиеся "листьями" дерева представляют собой реальные управляемые объекты, каждый из которых представляет управляемый ресурс, процесс или связанную с ними информацию. Каждый управляемый объект уникальным образом идентифицируется некоторым номером в десятично-точечной записи, которая сохраняется в пределах всего дерева SMI. Идентификатор каждого объекта описывается с использованием абстрактной синтаксической нотации ASN.1 (ASN — abstract syntax notation).

Протокол SNMP использует эти идентификаторы объектов для определения переменных баз MIB, которые требуются для извлечения данных или их изменения.

Объекты, находящиеся в общедоступном домене, описываются в базах MIB, введенных и описанных в спецификациях RFC (Request For Comments — RFC).

Производители оборудования призываются к тому, чтобы обнародовать определения своих баз MIB. После того, как определено назначенное значение предприятия, ответственность за создание и поддержку подчиненных поддеревьев ложится на производителя.

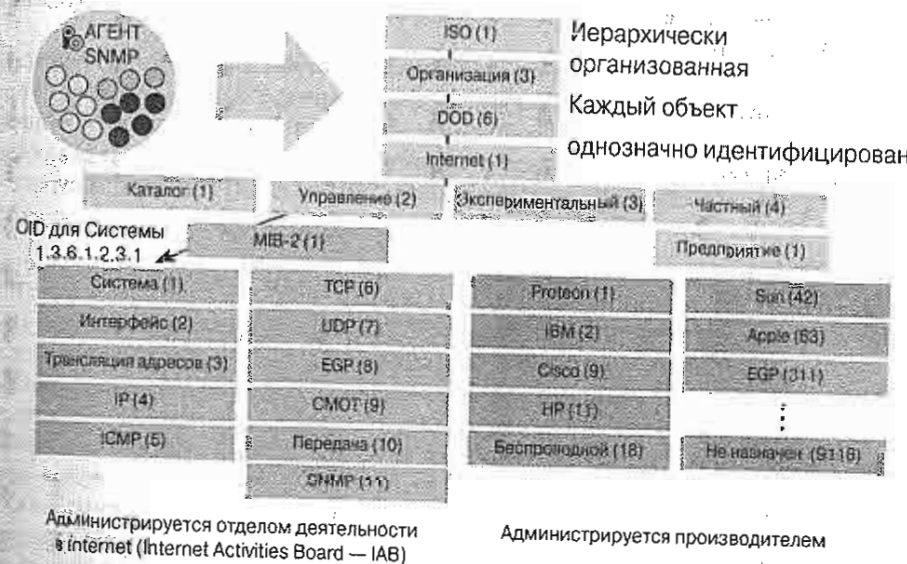


Рис. 16.19. Иерархическая структура управления

Протокол SNMP

Агентом называется функция программного обеспечения, которая встроена в большинство сетевых устройств (рис. 16.20). Агент отвечает за обработку запросов протокола SNMP, поступающих от менеджера управления сетью. Он также отвечает за выполнение стандартных операций, которые поддерживают значения переменных, определенных в различных поддерживаемых базах MIB.

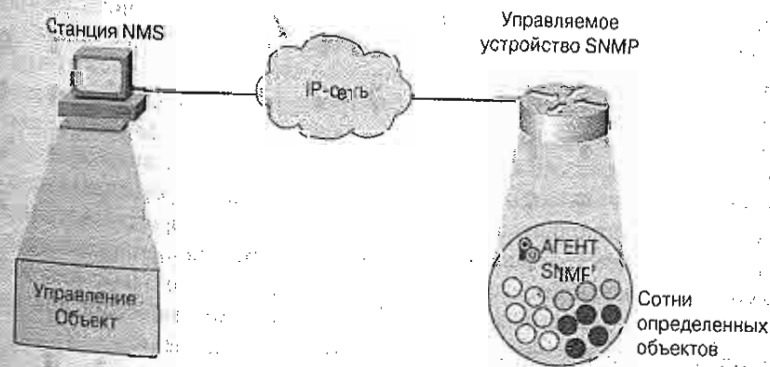


Рис. 16.20. Управление сетью на основе агентов

Взаимодействие между менеджером и агентом облегчается при использовании “протокола вопросов и ответов”, т.е. протокола SNMP. Термин “простой” в названии протокола связан с ограниченным количеством типов сообщений, которые являются частью первоначальной спецификации протокола. При его создании была избрана стратегия облегчения для разработчиков встраивания функций управления в сетевые устройства. Первоначальная спецификация этого протокола получила название SNMPv1 (версия 1).

На рис. 16.21 показаны три типа сообщений протокола SNMP, отправляемых станциями управления NMS: GetRequest, GetNextRequest и SetRequest. Агент управления подтверждает получение сообщений этих трех типов в виде сообщения GetResponse. Кроме этого агент может отправить сообщение Trap в виде реакции на событие, которое может оказать влияние на базу MIB и связанные с ней ресурсы.

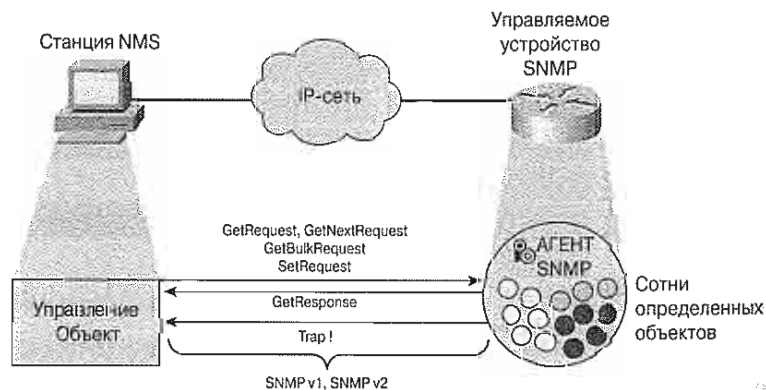


Рис. 16.21. Три типа сообщений протокола SNMP

Быстрое появление второй версии протокола — SNMPv2c (версия 2с) было реакцией на заметные ограничения протокола SNMPv1. Наиболее заметными улучшениями были введение нового типа сообщений GetBulk Request и добавление 64-битовых счетчиков. Получение информации с помощью сообщений GetRequest и GetNextRequest оказалось неэффективным методом сбора информации от структур табличных данных устройств сети. Протокол SNMPv1 позволял запросить за один раз значение лишь одной переменной. Введение сообщения-запроса GetBulk Request позволило устранить этот недостаток. При его использовании менеджер получает “весь объем” информации с помощью лишь одного запроса. Введение 64-битовых счетчиков в базах MIB было призвано решить проблемы слишком быстрого переполнения счетчиков, которое было особенно заметно в высокоскоростных каналах, таких как Gigabit Ethernet.

Субъект управления также называется менеджером или станцией NMS, как показано на рис. 16.22. Он отвечает за отправку запроса на информацию от агента. Такие запросы имеют специфический характер. Менеджер обрабатывает полученную информацию несколькими типичными способами. Эта информация может быть записана в журнал для дальнейшего анализа, отображена с помощью какой-либо графической утилиты или соотнесена с заранее заданными значениями для выяснения вопроса о превышении некоторых заданных пороговых значений.

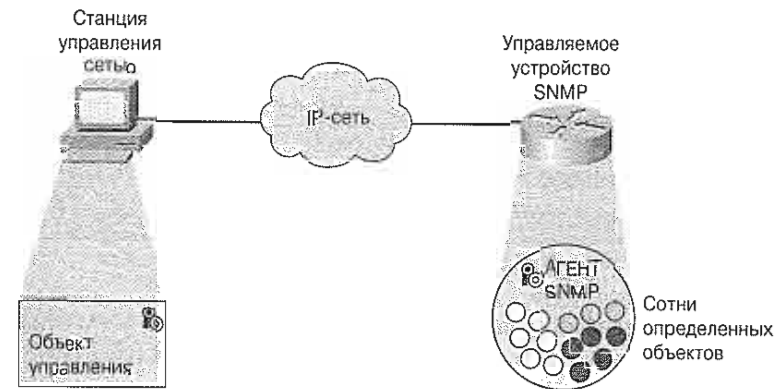


Рис. 16.22. Объект и субъекты управления

Не все функции менеджера связаны с получением данных. Есть также возможность внести изменения в значения переменных на управляемом устройстве. Это позволяет контролировать конфигурацию управляемого устройства.

Взаимодействие между менеджером и управляемым устройством вызывает увеличение объема передачи данных по сети. Поэтому при установке менеджеров в сети требуется соблюдать определенную осторожность. Энергичные стратегии мониторинга могут отрицательно повлиять на производительность сети. Интенсивность использования полосы пропускания может возрасти и создать проблемы в среде распределенных сетей WAN. Другой аспект воздействия мониторинга сети на ее работу связан с управляемыми устройствами. Этим устройствам приходится обрабатывать запросы менеджера; эти функции не должны оказываться более важными, чем производительные функции устройств.

Общей рекомендацией в данном случае является стремление получать минимум информации и, по возможности, реже. Поэтому следует определить, какие устройства и каналы наиболее важны и какой уровень подробности данных является необходимым.

Протокол SNMP использует в качестве своего транспортного протокола протокол дейтаграмм пользователя (User Datagram Protocol — UDP). Вследствие этого в протоколе SNMP возможна потеря сообщений. Протокол SNMP не имеет средств, которые бы обеспечивали гарантированную доставку, поэтому проблема утеранных модулей данных протокола (protocol data unit — PDU) должна решаться приложением, использующим протокол SNMP.

Как показано на рис. 16.23, каждое сообщение протокола SNMP содержит передаваемую открытым текстом строку (строку сообщества), такую как пароль, для ограничения доступа к управляемым устройствам. Хотя сам такой подход был достаточно плодотворным, поскольку строки сообщества передавались открытым текстом он вместе с тем поставил проблему безопасности. Создание версии SNMPv3 (версия 3) позволило устранить многие проблемы связанные с обеспечением безопасности.



Рис. 16.23. Сообщение протокола SNMP

На рис. 16.24 показано, как выглядят сообщения протокола SNMPv2c. Подробное описание этого протокола можно найти в стандарте Internet RFC 1157.

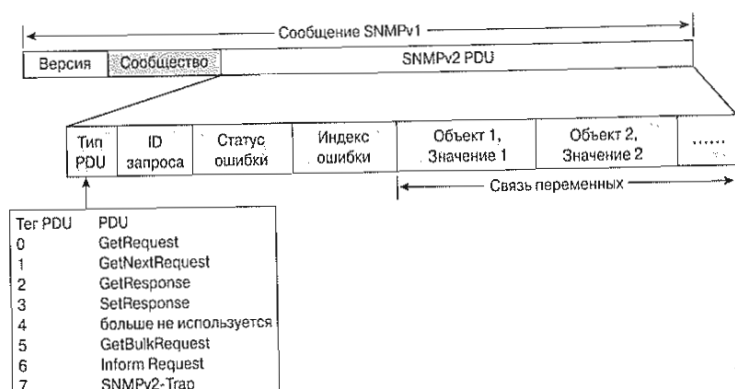


Рис. 16.24. Сообщение протокола SNMPv2c

Тот факт, что строка сообщества передается открытым текстом, не удивит никого, знакомого со стеком протоколов IP. Все поля, указанные в стеке этого протокола передаются открытым текстом, за исключением спецификаций аутентификации и шифрования.

Строка сообщества заменяла по существу систему безопасности до тех пор, пока рабочая группа версии SNMPv2 не ратифицировала механизмы безопасности. Эти вопросы были вскоре переданы рабочей группе по версии SNMPv3. Соответственно, все основанные на протоколе SNMP приложения управления сетями требовали соответствующего конфигурирования для использования соответствующих строк сообщества. Кроме этого, некоторые организации часто меняют значения строк сообщества для уменьшения риска попыток враждебных действий по несанкционированному доступу и использованию службы SNMP.

Несмотря на недостатки, связанные с использованием аутентификации, основанной на сообществах, стратегии управления по-прежнему базируются на протоколе SNMPv1. Устройства Cisco поддерживают типы сообщений протокола SNMPv3 и, соответственно, имеют большую степень безопасности, однако большинство приложений по управлению сетью не поддерживают протокол SNMPv3, как показано на рис. 16.25.

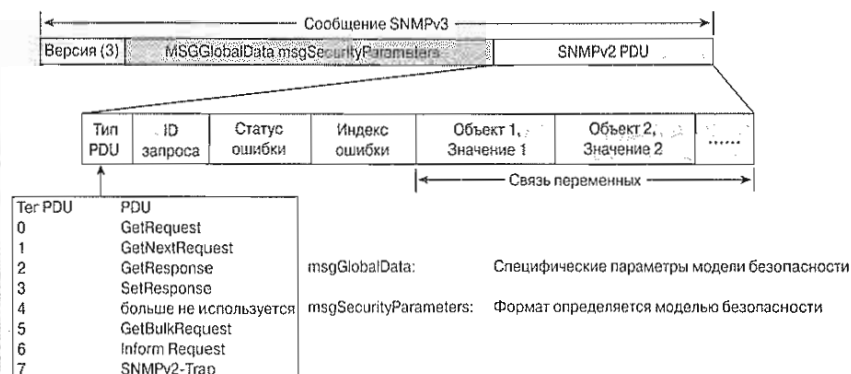


Рис. 16.25. Сообщение протокола SNMPv3

Конфигурирование протокола SNMP

Для того, чтобы станции NMS могли обмениваться данными с сетевыми устройствами, на этих устройствах должен быть установлен протокол SNMP и сконфигурированы строки сообщества. Ниже приведен обзор команд и их синтаксис для конфигурирования этих устройств.

При этом могут поддерживаться несколько строк, предназначенных только для чтения. По умолчанию в большинстве систем эта строка сообщества является общедоступной. Использование этого стандартного типа в сети предприятия не рекомендуется. Для того, чтобы используемая агентом строка сообщества имела статус "только для чтения", следует ввести следующую команду:

```
Router(config)#snmp-server community string ro
```

где:

- параметр *string* является строкой сообщества, которая выполняет функции пароля и представляет доступ к протоколу SNMP.
- параметр *ro* (необязательный) указывает на статус доступа "только для чтения". Получить доступ к объектам баз MIB должны только авторизованные станции управления сетью.

Возможна поддержка нескольких строк со статусом "только для чтения". Все объекты протокола SNMP доступны для записи в них данных.

По умолчанию в большинстве систем строка сообщества является приватной. Использовать это значение в сети предприятия не рекомендуется. Для установки атрибута "для чтения/записи" для строки сообщества используется следующая команда:

```
Router(config)#snmp-server community string rw
```

Где:

- *rw* (необязательный параметр) указывает на возможность доступа для чтения/записи. Авторизованные станции управления могут извлекать значения объектов баз данных MIB и изменять их. Для задания расположения управляемого устройства и главного системного контакта для него могут использоваться несколько строк.


```
Router(config)#snmp-server location text
Router(config)#snmp-server contact text
```

где:

параметр *text* представляет собой строку, содержащую информацию о системном расположении. Эти значения хранятся в объектах MIB sysLocation и sysContact.

Удаленный мониторинг (RMON)

Удаленный мониторинг RMON является крупным шагом вперед в развитии управления сетями. Он определяет базу данных удаленного мониторинга RMON MIB, которая дополняет базу MIB-II и предоставляет сетевому менеджеру жизненно важную информацию о сети. Примечательной функцией RMON является то, что хотя это лишь спецификация базы MIB, не вносящая изменений в лежащий в основе протокол SNMP, она представляет собой значительное расширение функций протокола SNMP. С помощью базы MIB-II сетевой менеджер может получить информацию, которая является чисто локальной и относится только к индивидуальным устройствам. Рассмотрим локальную сеть LAN, в которой имеется несколько устройств и на каждом из них действует агент протокола SNMP.

Менеджер SNMP может получить информацию об объемах данных поступивших на каждое устройство и отправленных с него, однако с помощью базы MIB-II он может получить информацию о потоках данных в целом в сети LAN. Для целей управления сетью в среде объединенных сетей, как правило, требуется лишь один монитор на каждую подсеть.

Стандарт удаленного мониторинга RMON первоначально имел название IETF RFC 1271 (в настоящее время RFC 1757) и был предназначен для активного мониторинга и диагностики в распределенных сетях на основе LAN-сетей. Устройства мониторинга, называемые агентами или тестерами, позволяют создавать в критических сетевых сегментах определяемые пользователем аварийные сигнализаторы и собирать обширные и весьма важные статистические данные путем анализа каждого фрейма в сегменте.

Для поддержки топологий Ethernet стандарт RMON подразделяет функции мониторинга на девять групп и добавляет десятую группу в RFC 1513 для уникальных параметров сетей Token Ring. Стандарт RMON был предназначен для распределенной вычислительной архитектуры, в которой агенты осуществляют обмен данными с центральной станцией управления (клиентом) при посредстве протокола SNMP. Эти агенты определили структуры баз MIB протокола SNMP для всех 9-10 групп (Ethernet или Token Ring) RMON, что позволило взаимодействовать производителям диагностических средств на основе RMON. Ниже описаны группы удаленного мониторинга RMON.

- **Группа статистики** — эта группа поддерживает статистику использования и ошибок для подсети/сегмента, в которой осуществляется мониторинг (в качестве примеров можно привести использование полосы пропускания, широковещание, многоадресную рассылку и т.д.).
- **Группа истории событий** — периодически делает статистические выборки из группы статистики и хранит их для последующего извлечения и анализа (в качестве примеров можно привести использование полосы пропускания, количество ошибок и количество пакетов).

- **Группа аварийной сигнализации** — эта группа позволяет администратору установить интервал для периодических выборок и пороговые значения для любых значений, которые фиксирует агент (примерами могут служить абсолютные или относительные значения, а также верхние и нижние пороговые значения).
- **Группа хостов (узлов)** — задает измерение различных типов данных, поступающих на узлы, подключенные к сети, или отправляемых с них (в качестве примеров можно привести количество полученных/отправленных пакетов, полученных/отправленных байтов, количество ошибок, а также широковещательных или многоадресных пакетов).
- **Группа из первых N узлов** — эта группа предоставляет отчет по первым N узлам, составленный на основе статистики группы узлов.
- **Группа матричных значений межузловой передачи** — в этой группе сохраняется статистика ошибок и использования полосы пропускания для пар узлов, которые обмениваются данными (примерами могут служить количество ошибок при передаче, байтов или пакетов).
- **Группа фильтров** — эта группа генерирует поток пакетов от фреймов, которые соответствуют заданному пользователем шаблону.
- **Группа захвата пакетов** — эта группа определяет способ помещения во внутренний буфер пакетов, соответствующих критерию фильтрации.
- **Группа событий** — задает запись в журнал для менеджера событий (соответствующих команде *trap*) вместе со временем и датой (Примером может служить генерирование отчетов на основе заданного типа аварийной ситуации).

Утилита Syslog

Утилита Cisco syslog используется для записи в журнал и основана на утилите syslog операционной системы UNIX. События в системе обычно выводятся на системную консоль, кроме случаев, когда она отключена. Утилита syslog представляет собой механизм регистрации активности и состояний ошибки для приложений, процессов и операционной системы устройств Cisco. Для того, чтобы устройства Cisco отправляли такие сообщения без запроса на станцию управления сетью, используется протокол syslog.

С каждым сообщением утилиты syslog в момент его генерации связывается соответствующая метка времени, устройство, уровень проблемы и текстовое сообщение. Эти сообщения иногда являются единственным способом узнать о неполадках внутри устройства.

Уровень проблемы свидетельствует о степени критичности ошибки, о которой говорится в сообщении, как показанного на рис. 16.26. Имеются восемь уровней сложности (0-7); при этом уровень 0 является наиболее критичным, а уровень 7 — наименее критичен. Ниже перечислены эти уровни.

- 0 — аварийная ситуация.
- 1 — оповещение.
- 2 — критическая ситуация.
- 3 — состояние ошибки.

- 4 — предупреждение.
- 5 — уведомление.
- 6 — информационное сообщение.
- 7 — отладочное сообщение.

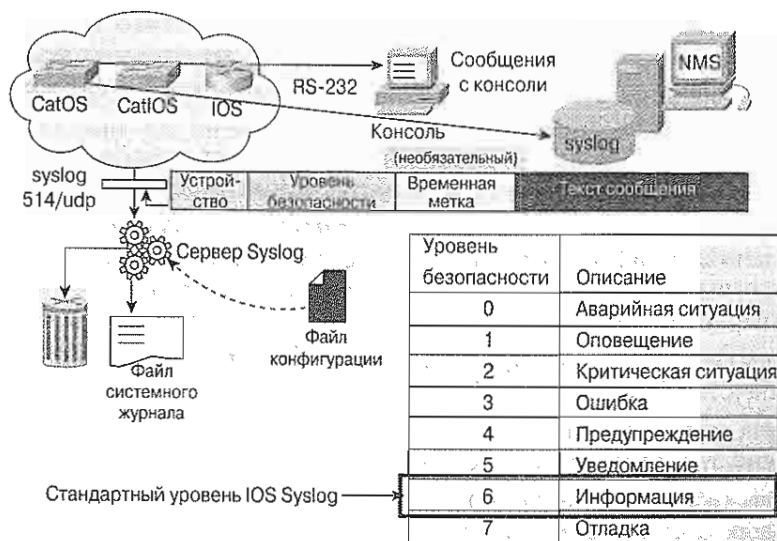


Рис. 16.26. Функционирование утилиты Syslog

Поля устройства и уровня проблемы используются для обработки сообщений. Для типовой обработки сообщений используются типы устройств от Local 0 до Local 7. Стандартное значение, принятое в операционной системе Cisco IOS, соответствует уровню проблемы 6. Эта установка может быть изменена в файле конфигурации.

Для того, чтобы станция NMS получала и регистрировала системные сообщения устройств, на них должна быть установлена утилита Syslog. Ниже приводятся команды, используемые для конфигурирования таких устройств.

Для активизации регистрации во всех поддерживаемых направлениях используется следующая команда:

```
Router(config)#logging on
```

Для отправки этих сообщений на узел сервера syslog, такой как CiscoWorks2000, используется команда:

```
Router(config)#logging hostname | ip address
```

Для установки уровня проблемы на 6-й (информационный) уровень используется команда:

```
Router(config)#logging trap informational
```

Для включения временной отметки в сообщение утилиты syslog используется команда:

```
Router(config)#service timestamps log datetime
```

Резюме

В настоящей главе были рассмотрены следующие ключевые темы и понятия:

- функции рабочей станции и сервера;
- роли, выполняемые различными устройствами в среде “клиент-сервер”;
- развитие сетевых операционных систем NOS;
- обзор различных платформ Windows;
- обзор возможных альтернатив операционным системам Windows;
- описаны причины, делающие необходимым автоматическое управление сетью;
- уровни эталонной модели OSI и модели управления сетью;
- типы средств управления сетью и соответствующие приложения;
- роль протоколов SNMP и CMIP в мониторинге сети;
- способы сбора информации и регистрации проблем, используемые программным обеспечением управления сетью.
- сбор информации о производительности сети и составление отчетов.

В дополнение к материалу, изложенному в настоящей главе, рекомендуется ознакомиться с относящимися к ней лабораторными работами (e-Lab Activities), видеоклипами (Videos) и фотографиями (PhotoZooms), которые находятся на прилагаемом к книге компакт-диске.

Глоссарий

Канал (link). Канал сетевой коммуникации, состоящий из канала или маршрута передачи данных и соответствующего оборудования, расположенного между отправителем и получателем. Иногда называется линией или каналом передачи.

Линия (circuit). Маршрут коммуникации между двумя или более точками.

Протокол Frame Relay. Промышленный протокол канального уровня, работающий с многими виртуальными каналами и использующий инкапсуляцию протокола HDLC для связи между устройствами. Протокол Frame Relay более эффективен, чем протокол X.25, замещением которого считается протокол Frame Relay.

Сеть предприятия или корпоративная сеть (enterprise network). Сеть корпорации, агентства, школы или другой организации, в которой объединены данные, коммуникации, вычислительные ресурсы и файловые серверы.

Контрольные вопросы

1. Какую из приведенных ниже характеристик сети можно изменить и выразить в конкретных цифрах?
 - A. Безопасность
 - B. Проектирование
 - C. Структура
 - D. Производительность

2. Какой тип связи между конечными станциями устанавливается в одноранговой сети?
 - A. Клиент-клиент
 - B. Клиент-сервер
 - C. Сервер-сервер
 - D. Сервер-Сеть Internet
3. Какой тип файловой системы используется в Windows NT для обеспечения безопасности?
 - A. FAT 16
 - B. FAT 32
 - C. NTFS
 - D. NFS
4. В сети "клиент-сервер" возможность доступа пользователя к одним файлам и невозможность доступа к остальным является для него:
 - A. Правом доступа
 - B. Правами
 - C. Возможностями доступа
 - D. Мерой обеспечения безопасности
5. Каков IP-адрес внутренней обратной петли?
 - A. 10.10.10.1
 - B. 255.255.255.0
 - C. 127.0.0.1
 - D. 192.0.0.1
6. Какое из приведенных ниже действий является способом предотвратить повреждения от статического электричества?
 - A. Отключение питания при работе на компьютере.
 - B. Одевать резиновые перчатки для изоляции от оборудования
 - C. Использование только пластмассовых инструментов
 - D. Использование заземляющего ремня (пояса)
7. Какой из приведенных ниже протоколов поддерживает управление сетью?
 - A. SMTP
 - B. NFS
 - C. SNMP
 - D. FTP
 - E. IPX
8. Какую из приведенных ниже команд следует использовать для вывода списка IP-установок на компьютере с ОС Windows NT?
 - A. `ip`
 - B. `ipconfig`
 - C. `winipcfg`

- D. `show ip`
- E. `config`
9. Какой из приведенных ниже методов обнаружения ошибок используется для поиска ошибок в сетях?
 - A. Считывание информации с петлевого интерфейса
 - B. "Разделяй и властвуй"
 - C. Тестирование командой `Ping`
 - D. Отслеживание ошибок
 - E. Перезагрузка сервера
10. Если сервер настроен для работы по протоколу IP, то какой из приведенных ниже протоколов должны использовать клиенты для связи с ним?
 - A. Протокол IPX
 - B. Протокол UDP
 - C. Протокол IP
 - D. Протокол Telnet
 - E. Протокол HTTP
11. Расширением какого протокола является RMON?
 - A. SNMP
 - B. UDP
 - C. IPX
 - D. PING
 - E. E. SMTP
12. Что означает опция `-n` в команде `ping`?
 - A. Сетевой номер зоны, к которой применяется команда `ping`
 - B. Опция "без повторения"
 - C. Подсчитать x раз выполнение команды `ping`
 - D. Не останавливать выполнение команды до внешнего ее прекращения
 - E. Не выполняет никаких функций
13. Каким образом RMON собирает данные от удаленных источников?
 - A. С помощью команд
 - B. С помощью таблиц
 - C. С помощью списков
 - D. С помощью проб
 - E. Путем взаимодействия с пользователем
14. Стоимость _____ оборудования для критически важных операций требуется добавить к стоимости поддержки сети.
 - A. Избыточного
 - B. Дорогостоящего
 - C. Механического
 - D. Обеспечивающего безопасность
 - E. Сварочного