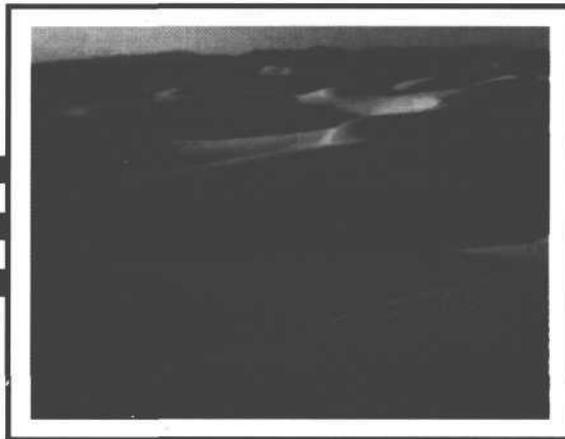


CCNA

Бестселлер
1

Cisco Certified Network Associate

Учебное руководство



Экзамен
640-507

Второе издание

Тодд Леммл

Свыше **100 000** пользователей
выбрали это учебное руководство



Издательство "Лори"

CCNA

Cisco Certified

Network Associate

Study Guide

Second Edition

Todd Lammle



CCNA
Cisco Certified
Network Associate

Учебное руководство

Экзамен 640-507

Второе издание

Тодд Лэммл



CCNA™
Cisco® Certified Network Associate
Study Guide
Second Edition
Todd Lammle
Copyright 2000
All rights reserved

CCNA
Cisco Certified Network Associate
Учебное руководство
Экзамен 640-507
Тодд Лэммл
Второе издание
Переводчик М. Кузьмин
Научный редактор А. Головки
Корректор Н. Литвинова
Верстка М. Алиевой

Copyright © 2000 SYBEX Inc., 1151 Marina Village Parkway, Alameda, CA 94501
All rights reserved.

Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

ISBN 0-7821-2647-2

© Издательство "ЛОРИ", 2002

Изд. N : OAI (03)
ЛР N : 070612 30.09.97 г.
ISBN 5-85582-180-3

Подписано в печать 5.07.2002 Формат 70x100/16
Печать офсетная
Печ.л. 36 Тираж 3200 Заказ N 646
Цена договорная

Издательство "ЛОРИ". Москва, 123557 Б. Тишинский пер., д. 40, корп. 2
Телефон для оптовых покупателей: (095) 259-01-62
WWW.LORY-PRESS.RU

Отпечатано в типографии ООО "Типография ИПО профсоюзов Профиздат"
109044, Москва, ул. Крутицкий вал д. 18

Эта книга посвящается всем техническим инструкторам Cisco - неизвестным героям учебных курсов. Им приходится много и напряженно трудиться, чтобы заработать на хлеб насущный. Но их награда в успехах студентов, которые становятся тем, кем хотели стать.

Благодарности

Мы благодарны очень многим! Даже трудно сообразить, с чего начать.

Прежде всего, искренне благодарю Линду Ли — технического редактора этой книги. Спасибо Нейлу Эдди, который неизменно присутствует в благодарностях ко всем моим книгам. Без него не было бы моего первого учебного курса CCNA и моей первой книги в издательстве Sybex.

Сузан Берг и Лиза Дюран выполнили огромную работу по согласованию и поддержке плана подготовки книги к печати. Благодарю Патрика Ремсейна и Эрика Гуннета, тщательно проверивших каждую главу книги. Большое спасибо Слли Энгелфрид, Мерилин Смит и Ребекке Райдер за помощь в редактировании глав этой книги, а также корректорам Молли Гловер, Дженифер Кемпбелл и Лауре О'Коннелл. Кроме того, благодарю Маурин Форрис за окончательную правку текста и Тони Джоник за подготовку иллюстраций.

Содержание

1 Введение в объединенные сети	1
Модели объединенных сетей	2
Многоуровневый коммуникационный подход	2
Достоинства базовой модели	3
Базовая модель OSI	3
Уровни модели OSI	5
Сети Ethernet	18
Дуплексная и полудуплексная сеть Ethernet	19
Ethernet на канальном уровне	20
Ethernet на физическом уровне	25
Инкапсуляция данных	26
Трёхуровневая иерархическая модель компании Cisco	28
Базовый уровень	29
Уровень распространения	31
Уровень доступа	31
Кабели и подключение устройств Cisco	32
Кабели Ethernet для локальных сетей	32
Требования к носителям и соединителям Ethernet	33
Соединитель UTP (RJ-45)	34
Кабели региональных сетей	36
Выбор устройств Cisco	40
Концентраторы Cisco	40
Маршрутизаторы Cisco	41
Переключатели Cisco	42
Упражнения	44
Упражнение 1.1. Модель OSI	44
Упражнение 1.2. Уровни OSI и устройства	45
Упражнение 1.3. Выявление доменов конфликтов и доменов широковещательных рассылок	46
Проверочные вопросы	47
Ответы к упражнениям	50
Ответы к упражнению 1.1	50
Ответы к упражнению 1.2	51
Ответы к упражнению 1.3	51
Ответы на проверочные вопросы	52
2 Технологии коммутации	53
Коммутация на уровне 2	54
Недостатки коммутации на уровне 2	54
Сравнение применения мостов с коммутацией в локальной сети	55

Три функции коммутации уровня 2	55
Изучение адресов	55
Решение о пересылке и фильтрации	57
Исключение зацикливания	57
Протокол STP Spanning-Tree Protocol	58
Действие алгоритма покрывающего дерева	59
Выбор корневого моста	59
Выбор назначенных портов	61
Состояния портов в алгоритме покрывающего дерева	61
Пример использования алгоритма покрывающего дерева	62
Типы переключателей локальных сетей	63
Режим "сохранить и передать"	64
Сквозной режим (реальное время)	64
Бесфрагментный режим	65
Упражнение	65
Проверочные вопросы	66
Ответы к упражнению	69
Ответы на проверочные вопросы	70
3 Протокол Интернета	71
Модели TCP/IP и DoD	72
Протоколы уровня процессов/приложений	73
Протоколы уровня взаимодействия хостов	78
Протоколы уровня Интернета	85
Адресация IP	93
Термины IP-адресации	93
Иерархическая схема IP-адресации	94
Выделение подсетей	100
Маска подсети	101
Выделение подсетей в классе C	102
Выделение подсетей в классе B	109
Выделение подсетей в классе A	115
Упражнение	118
Проверочные вопросы	118
Ответы к упражнению	122
Ответы на проверочные вопросы	122
4 Конфигурация и команды управления IOS	123
Пользовательский интерфейс маршрутизатора Cisco	124
Операционная система IOS в маршрутизаторах Cisco	124
Подключение к маршрутизатору Cisco	124
Включение маршрутизатора	125
Интерфейс командной строки	130
Регистрация (вход) в маршрутизатор	131
Обзор режимов маршрутизатора	132
Приглашения интерфейса CLI	133
Возможности редактирования и вывода справки	135

Сбор основной информации о маршрутизации.	139
Установка паролей.	140
Баннеры	146
Интерфейсы маршрутизатора	147
Имена хостов.	151
Описание.	151
Просмотр и сохранение конфигурации	152
Проверка конфигурации.	154
Упражнение.	158
Лабораторные работы.	159
Лабораторная работа 4.1. Регистрация в маршрутизаторе	159
Лабораторная работа 4.2. Использование редактирования и возможностей справки	160
Лабораторная работа 4.3. Сохранение конфигурации маршрутизатора.	161
Лабораторная работа 4.4. Установка паролей	162
Лабораторная работа 4.5. Настройка имени хоста, описания, IP-адреса и тактовой частоты.	164
Проверочные вопросы.	165
Ответы к упражнению.	169
Ответы к проверочным вопросам.	169
5 Маршрутизация по протоколу IP	171
Маршрутизация.	172
Процесс IP-маршрутизации	172
IP-маршрутизация в крупных сетях.	176
IP-маршрутизация в сети.	180
Статическая маршрутизация.	181
Маршрутизация по умолчанию.	186
Динамическая маршрутизация.	187
Административное расстояние	188
Протоколы маршрутизации	189
Петля маршрутизации.	191
Протокол RIP.	194
Таймеры RIP.	195
Настройка маршрутизации по протоколу RIP.	195
Проверка таблиц маршрутизации для протокола RIP	197
Удержание распространения информации по протоколу RIP	199
Протокол IGRP.	199
Таймеры IGRP.	200
Настройка маршрутизации по протоколу IGRP.	200
Настройка IGRP в объединенной сети.	201
2621A	201
2501A	202
2501B.	202
2501C.	202

Проверка таблиц маршрутизации	
по протоколу IGRP	203
Проверка конфигурации	204
Команда Show Protocols	205
Команда Show IP Protocol	205
Команда Debug IP RIP	207
Команда Debug IP IGRP	208
Упражнение	209
Лабораторная работа	210
Лабораторная работа 5.1. Создание статических путей	210
Лабораторная работа 5.2. Динамическая маршрутизация по протоколу RIP	212
Лабораторная работа 5.3. Динамическая маршрутизация по протоколу IGRP	213
Проверочные вопросы	214
Ответы к упражнению	217
Ответы к проверочным вопросам	218
6 Виртуальные локальные сети (VLAN)	219
Виртуальные локальные сети (Virtual LAN)	220
Управление широкополосными рассылками	220
Безопасность	221
Гибкость и масштабируемость	222
Членство в сети VLAN	223
Статические сети VLAN	223
Динамические сети VLAN	224
Идентификация сетей VLAN	224
Маркировка кадров	225
Методы идентификации VLAN	225
Протокол ISL	226
Магистральные связи	227
Маршрутизация между сетями VLAN	227
Протокол VTP	228
Режимы VTP	229
Номер версии конфигурации	230
Сокращение действия VTP	231
Упражнение	231
Проверочные вопросы	232
Ответы к упражнению	235
Ответы на проверочные вопросы	236
7 Управление объединенными сетями Cisco	237
Компоненты маршрутизаторов Cisco	238
Последовательность загрузки маршрутизатора	239
Управление конфигурационными регистрами	239
Разряды конфигурационного регистра	239

Проверка текущего значения конфигурационного регистра	241
Изменение конфигурационного регистра	241
Восстановление пароля.	242
Резервное копирование и восстановление Cisco IOS	245
Проверка флэш-памяти.	245
Резервное копирование Cisco IOS.	246
Восстановление и обновление Cisco IOS в маршрутизаторе	248
Резервное копирование и восстановление конфигурации в устройстве Cisco	250
Резервное копирование конфигурации маршрутизатора Cisco.	251
Восстановление конфигурации маршрутизатора Cisco	252
Стирание конфигурации.	253
Использование протокола Cisco Discovery Protocol	254
Получение информации по протоколу CDP о таймере и времени удержания	254
Получение информации от соседних устройств.	255
Получение информации о трафике в интерфейсе	257
Получение информации о портах и об интерфейсах.	257
Использование Telnet	259
Одновременный доступ по Telnet к нескольким устройствам	260
Проверка подключения по Telnet	262
Проверка пользователей Telnet	262
Закрытие сеанса Telnet.	262
Разрешение имен хостов.	264
Построение таблицы хостов.	264
Использование DNS для разрешения имен	266
Проверка сетевых подключений.	268
Использование команды Ping.	268
Использование команды Tracert	269
Упражнение.	270
Лабораторные работы.	270
Лабораторная работа 7.1. Резервное копирование IOS маршрутизатора.	270
Лабораторная работа 7.2. Обновление или восстановление IOS в маршрутизаторе.	271
Лабораторная работа 7.3. Резервное копирование конфигурации маршрутизатора.	271
Лабораторная работа 7.4. Использование протокола CDP	272
Лабораторная работа 7.5. Использование Telnet	273
Лабораторная работа 7.6. Разрешение имен хостов.	274
Проверочные вопросы.	275
Ответы к упражнению.	278
Ответы на проверочные вопросы.	279

8	Конфигурация сетей Novell IPX	281
	Введение в Novell IPX	282
	Стек протоколов Novell IPX	282
	Связь между клиентом и сервером	284
	Связь между серверами	285
	IPX-адресация	289
	Инкапсуляция	290
	Активизация IPX в маршрутизаторах Cisco	292
	Разрешение маршрутизации по протоколу IPX	292
	Разрешение IPX в определенном интерфейсе	292
	Настройка объединенной сети на протокол IPX	294
	Настройка IPX в маршрутизаторе 2621A	294
	Настройка IPX в маршрутизаторе 2501A	294
	Настройка IPX в маршрутизаторе 2501B	295
	Настройка IPX в маршрутизаторе 2501C	295
	Проверка таблиц маршрутизации IPX	295
	Добавление дополнительных адресов	297
	Настройка дополнительного адреса	298
	Подинтерфейс	298
	Настройка в объединенной сети нескольких типов кадров Ethernet	299
	Настройка нескольких типов кадров в маршрутизаторе 2621A	299
	Настройка нескольких типов кадров в маршрутизаторе 2501A	300
	Настройка нескольких типов кадров в маршрутизаторе 2501B	301
	Настройка нескольких типов кадров в маршрутизаторе 2501C	301
	Проверка таблицы маршрутизации IPX	302
	Мониторинг IPX в маршрутизаторе Cisco	303
	Show IPX Servers	303
	Show IPX Route	304
	Show IPX Traffic	305
	Show IPX Interfaces	306
	Show Protocols	307
	Debug IPX	307
	RouterA#IPX Ping	309
	Упражнение	310
	Лабораторные работы	310
	Лабораторная работа 8.1. Настройка протокола Internetworking Packet Exchange (IPX)	311
	Лабораторная работа 8.2. Добавление в сети IPX дополнительного сетевого адреса и нескольких типов кадров	312
	Проверочные вопросы	314
	Ответы к упражнению	317
	Ответы на проверочные вопросы	318

9 Управление трафиком с помощью списков доступа 319

Список доступа	320
Стандартный список доступа IP	322
Управление доступом VTU (Telnet)	326
Улучшенные списки доступа IP	326
Мониторинг списков доступа IP	332
Списки доступа IPX	332
Стандартный список доступа IPX	332
Улучшенные списки доступа IPX	334
Фильтры SAP стека IPX	334
Проверка списков доступа IPX	335
Упражнение	336
Лабораторные работы	337
Лабораторная работа 9.1. Стандартные списки доступа IP	337
Лабораторная работа 9.2. Улучшенный список доступа IP	338
Лабораторная работа 9.3. Стандартный список доступа IPX	340
Проверочные вопросы	341
Ответы к упражнению	345
Ответы на проверочные вопросы	345

10 Протоколы региональных сетей 347

Региональные сети	348
Определения из области региональных сетей	348
Типы подключения региональных сетей	349
Поддержка региональной сети	350
Протокол HDLC	351
Протокол PPP	352
Параметры настройки Link Control Protocol (LCP)	353
Процедура установки сеанса PPP	353
Методы аутентификации PPP	354
Настройка PPP в маршрутизаторе Cisco	354
Настройка аутентификации PPP	355
Проверка инкапсуляции PPP	356
Frame Relay	357
Термины Frame Relay	357
Инкапсуляция Frame Relay	359
Идентификатор Data Link Connection Identifier (DLCI)	360
Local Management Interface (LMI)	361
Подинтерфейсы	362
Отображение Frame Relay	366
Управление нагрузкой в Frame Relay	367
CIR (Committed Information Rate)	367
Мониторинг Frame Relay	368
Integrated Services Digital Network (ISDN)	371
Компоненты ISDN	372
Basic Rate Interface (BRI)	375
Primary Rate Interface (PRI) . Л	375

ISDN в маршрутизаторах Cisco	376
Dial-on-Demand Routing (DDR)	377
Настройка DDR	377
Настройка статических путей	378
Указание "интересного" трафика	378
Настройка информации о набираемом номере	378
Необязательные команды	380
DDR со списками доступа	381
Проверка работы ISDN	381
Упражнение	382
Лабораторные работы	383
Лабораторная работа 10.1. Настройка инкапсуляции PPP и аутентификации	383
Лабораторная работа 10.2. Настройка и мониторинг HDLC	384
Лабораторная работа 10.3. Настройка Frame Relay и подинтерфейсов	385
Лабораторная работа 10.4. Настройка ISDN и интерфейсов BRI	386
Проверочные вопросы	389
Ответы к упражнению	392
Ответы на проверочные вопросы	393

Приложения

A	Пример сертификационного экзамена	395
	Вопросы сертификационного экзамена	396
	Ответы на вопросы сертификационного экзамена	407
B	Настройка переключателя Catalyst 1900	409
	Возможности переключателей 1900	410
	Три варианта настройки	411
	Подключение к консольному порту	411
	Запуск переключателя 1900	412
	Подключение к порту Ethernet	413
	Команды настройки IOS в переключателе Cisco 1900	414
	Установка паролей	414
	Установка имени хоста	417
	Установка информации IP	418
	Настройка интерфейсов переключателя	419
	Настройка описания интерфейса	422
	Настройка дуплексного режима порта	423
	Проверка соединений по протоколу IP	424
	Стирание конфигурации переключателя	425
	Обслуживание таблиц MAC-адресов	425
	Установка постоянных и статических MAC-адресов	427
	Настройка безопасности порта	429
	Команда Show Version	430

Изменение типа коммутации локальной сети.	431
Настройка сетей VLAN.	431
Присваивание коммутируемых портов сети VLAN.	433
Настройка транковых портов	434
Очистка магистральных связей в сети VLAN	435
Проверка магистральных связей	436
Настройка маршрутизации ISL	437
Настройка VTP	438
Настройка домена	438
Добавление в домен VTP	439
Сокращение действия VTP.	440
Восстановление и обновление IOS в переключателе Catalyst 1900	440
Резервное копирование и восстановление конфигурации Catalyst 1900.	441
Протокол CDP в переключателях 1900	442
Упражнение	443
Лабораторные работы.	444
Лабораторная работа В.1. Обслуживание переключателя серии 1900.	444
Лабораторная работа В.2. Операции переключателя 1900	445
Лабораторная работа В.3. Создание сетей VLAN.	446
Лабораторная работа В.4. Присваивание коммутируемых портов сетям VLAN.	447
Лабораторная работа В.5. Настройка магистральных связей	449
Лабораторная работа В.6. Настройка VTP.	450
Лабораторная работа В.7. Настройка маршрутизации между сетями VLAN с помощью ISL	451
Проверочные вопросы	452
Ответы к упражнению	456
Ответы на проверочные вопросы.	457
С Справочник команд Cisco.	459
Глоссарий	469

Введение

Эта книга познакомит вас с программой квалификационных экзаменов Cisco и поможет получить сертификат CCNA. Изучив предлагаемый материал, вы освоите современные сетевые технологии глубже, чем это необходимо для получения таких популярных сертификатов, как MCSE и CNE. Перед вами откроется дверь в мир объединенных сетей.

Компания Cisco — краткая история

Многие читатели уже знакомы с компанией Cisco и ее деятельностью. Однако новичков, только что получивших сертификат MCSE, а возможно, и тех, кто работает с сетями более десяти лет, но хотел бы освежить в памяти новые технологии, мы познакомим с краткой историей компании Cisco.

В начале 80-х годов супруги Лен (Len) и Сэнди (Sandy) Босэк (Bosack), работавшие в разных отделах вычислительной техники Станфордского университета, основали компанию cisco Systems (обратите внимание на строчную букву *c*). Они испытывали затруднения при организации взаимодействия несовместимых систем и поэтому создали у себя дома шлюзовый сервер, чтобы решить эту задачу на основе протокола IP. В 1984 г. Cisco Systems создала небольшой коммерческий шлюзовый сервер, в корне изменивший технологию организации сетей. Некоторые считают, что компанию предполагалось назвать San Francisco Systems, но документ разорвался при передаче юристам. Кто знает? В 1992 г. название компании изменилось на Cisco Systems, Inc.

Первым продуктом, поступившим в продажу, стал AGS (Advanced Gateway Server — усовершенствованный шлюзовый сервер). Позже появились MGS (Mid-Range Gateway Server — средний шлюзовый сервер), CGS (Compact Gateway Server — компактный шлюзовый сервер), IGS (Integrated Gateway Server — интегрированный шлюзовый сервер) и AGS+.

В 1993 г. компания Cisco выпустила прекрасный маршрутизатор серии 4000, а позднее — еще более впечатляющие маршрутизаторы серий 7000, 2000 и 3000. Они по-прежнему применяются и совершенствуются (кажется, почти ежедневно).

Компания Cisco Systems стала непревзойденным мировым лидером в области объединения сетей с Интернетом. Предлагаемые ею решения позволяют легко связывать пользователей, работающих на разнообразных компьютерах в несовместимых сетях. С помощью продукции Cisco упрощаются доступ к информации и ее передача независимо от различий во времени, расположении и платформы компьютеров.

Для объединения сетей компания Cisco Systems предлагает решение, основываясь на котором, пользователи могут создать эффективную информационную инфраструктуру как в собственных сетях, так и при соединении с сетями других владельцев. Этот подход является важной составляющей при объединении сетей и создании Интернета, поскольку наличие общей архитектуры с предоставлением всем пользователям согласованных услуг является в настоящее время обязательным требованием. И кроме того, так как компания Cisco Systems создала такой широкий диапазон услуг и средств для объединенных сетей и Интернета,

пользователи, нуждающиеся в регулярном доступе к своим сетям или к Интернету, могут беспрепятственно удовлетворять свои потребности, и это сделало продукцию Cisco Systems обязательной для применения.

Компания Cisco создала множество разнообразных устройств, используемых для организации информационных сетей на основе программного обеспечения Cisco IOS (Internetwork Operating System — межсетевая операционная система). Cisco IOS предоставляет сетевые услуги, подготавливая почву для внедрения сетевой службы технической поддержки и организации профессиональных служб для поддержки и оптимизации всех сетевых операций.

Наряду с разработкой Cisco IOS, одно из подразделений Cisco создало программу Cisco Certified Internetwork Expert (CCIE — сертифицированный эксперт Cisco по объединенным сетям) специально для обучения персонала эффективному управлению сетями, содержащими всевозможные устройства Cisco. Расчет был прост: если вы собираетесь покупать для своей сети новое оборудование Cisco, прежде всего нужно добиться того, чтобы сеть функционировала корректно.

Однако наличие широкого круга разнообразных устройств — не единственная причина грандиозного успеха Cisco. В условиях жесткого соперничества многие компании-конкуренты были вынуждены прекратить свою деятельность. С усложнением устройств необходимо иметь квалифицированный персонал, умеющий устанавливать их, управлять ими и устранять неисправности в них. Эта проблема не так проста, поэтому в Cisco создана программа CCIE для обучения сотрудников, поддерживающих работоспособность более сложных сетей. Эта программа, называемая докторантурой по сетевым технологиям, имела большой успех. И Cisco постоянно совершенствует ее с тем, чтобы она отражала требования к современной объединенной сетевой среде.

Организованные на основе программы CCIE курсы обучения Cisco Career Certifications выпускают сертифицированных специалистов с различным уровнем технической подготовки для создания и поддержки сетей. И если вы заботитесь о профессиональной подготовке или намерены систематизировать знания и продвинуться по служебной лестнице, эта книга для вас.

Сертификаты Cisco по технической поддержке сетей

Cisco создала новую систему сертификации, позволяющую получить звание эксперта и помогающую будущим специалистам оценить свой уровень подготовки. Ранее существовал лишь один тест и сложные лабораторные испытания. В новой системе сертификации принят более удачный способ подготовки к этим ужасным испытаниям, так что компания Cisco открыла дверь пошире перед теми, кто раньше не мог в нее войти. Что же представляет собой система сертификации, и какую помощь она окажет вам в получении сертификата CCIE?

Сертификат Cisco Certified Network Associate (CCNA) 2

Получение сертификата Cisco Certified Network Associate (CCNA — сертифицированный персонал сети Cisco) является первой ступенью в новой системе сертификации Cisco и предшествует получению всех существующих в настоящее время сертификатов Cisco. В новой системе Cisco реализована идея постепенного продвижения к сертификату CCIE. Теперь вы можете получить сертификат CCNA, прочитав эту книгу и уплатив \$100 за тест. Но не останавливайтесь на этом — вы можете продолжить обучение и достичь более высокой ступени Cisco Certified Network Professional (CCNP — сертифицированный профессионал по сетям Cisco). Некоторые обладатели сертификата CCNP уже имеют достаточные знания, чтобы попытаться выполнить лабораторные испытания CCIE. Однако никакая книга не заменит практического опыта, а мы еще немного расскажем о том, что нужно знать для успешного прохождения этих испытаний.

Цель получения сертификата CCNA

В отличие от компаний Microsoft и Novell, компания Cisco создала систему сертификации, чтобы дать администраторам сети некоторый набор навыков, научить будущих специалистов оценивать качество своих знаний или помочь в достижении уровня, удовлетворяющего определенному критерию. Получение сертификата CCNA является первым шагом успешного продвижения вверх по ступеням карьеры.

Программа CCNA позволяет получить не только твердые начальные знания о Cisco IOS и аппаратуре Cisco, но и общие понятия об объединенных сетях, что облегчит вашу работу с любыми сетями. После изучения этой программы будущие администраторы сетей (даже не содержащих устройства Cisco) смогут легко добиться сертификата Cisco, продемонстрировав свою работу.

Если вы добились сертификата CCNA и не охладели к Cisco и к объединенным сетям, вы находитесь на пути к успеху.

Для получения сертификата CCNA нужно быть способным выполнять следующее:

- Устанавливать, конфигурировать и работать с простой маршрутизируемой локальной сетью, с маршрутизируемой глобальной сетью, с локальными сетями с коммутацией, а также с эмуляцией локальных сетей ATM
- Понимать и уметь конфигурировать IP, IGRP, IPX, последовательные линии связи, AppleTalk, Frame Relay, IP RIP, виртуальные локальные сети, IPX RIP, Ethernet и списки доступа
- Устанавливать и/или конфигурировать любую сеть
- Оптимизировать региональную сеть, используя идеи доступа к Интернету для сокращения необходимой полосы пропускания, и снижать стоимость глобальной сети, применяя такие средства, как фильтрация по спискам доступа, выделение полосы пропускания по требованию и маршрутизация по каналам, предоставляемым по запросу

- Обеспечивать удаленный доступ при объединении аналоговых линий с традиционными, доступ к удаленной локальной сети, а также поддерживать более высокий уровень производительности, необходимый для новых приложений, например для торговли через Интернет, для мультимедиа и т. д.

Как получить сертификат **CCNA!**

Вы сделали первый шаг, купив это учебное руководство. Следующий шаг состоит в прохождении "небольшого" теста. И вот вы уже получаете сертификат CCNA. (Не думайте, что это легко!) Действительно, всего один тест, однако для того чтобы понять (и прочитать между строк), что хотят от вас авторы теста, вам понадобятся некоторые знания.

Невозможно сказать, какой объем знаний достаточен, — важно, чтобы у вас был опыт практической работы с маршрутизаторами Cisco. Если вы уже имели дело с маршрутизаторами серии 2500 — все в порядке. Но не смущайтесь, если вы новичок; в этой книге мы собрали сотни примеров конфигурации, чтобы помочь администратору сети (или тем, кто хочет им стать) в подготовке к экзамену CCNA.

Один из способов получения практического опыта работы с маршрутизаторами состоит в посещении семинара, организованного компанией Globalnet Training Solutions, Inc. (www.lammle.com), или в прохождении курса сертификации Cisco. Кроме того, в Virtual Networks/Ikon Technologies можно получить учебный набор CCNA, содержащий сведения о работе с маршрутизаторами Cisco.

Полезно также пройти через Интернет интерактивный курс университета Cyberstate University, основанный на учебных пособиях издательства Sybex по сертификации Cisco (www.cyberstateu.com). Видеокурсы по сертификации Cisco предлагает Keystone Learning Systems (www.klscorp.com).

Т ВНИМАНИЕ У Кроме книги "CCNA: Cisco Certified Network Associate Study Guide" издательства Sybex, существуют и другие полезные источники информации для подготовки к экзамену CCNA. В частности, компания CiscoTests (<http://www.networkstudyguides.com>) предлагает диалоговое учебное руководство, содержащее примеры вопросов и информацию о самых свежих версиях экзаменов CCNA, CCNP и CCIE.

Т ВНИМАНИЕ | Рекомендации по ответам на вопросы сертификационного экзамена Cisco можно найти по адресу www.boston.com.

Сертификат Cisco Certified Network Professional (CCNP)

Эта система сертификации Cisco открыла многочисленные возможности для получения сертификата Cisco, но кому нужны подготовка, оценка знаний, шелчки по носу, чтобы пройти пресловутые и часто проваливаемые двухдневные лабораторные испытания. Новая система сертификации

Cisco действительно открывает горизонты перед обладателями сертификатов CNE и MCSE, которые хотят повысить уровень своей квалификации.

Итак, вы думаете: "Что же я буду делать после сдачи экзамена CCNA?" Если вы собираетесь получить сертификат CCIE по маршрутизации и коммутации (наиболее популярный сертификат), помните, что есть несколько путей к достижению этой цели. Прежде всего можно продолжить учебу и получить сертификат Cisco Certified Network Professional (CCNP — сертифицированный профессионал по сетям Cisco). Это означает, что вам придется пройти еще четыре теста.

Программа CCNP позволяет исчерпывающе разобраться в идеях создания в настоящем и будущем объединенных сетей, содержащих не только устройства Cisco. Вы почувствуете, как выросли ваши знания и навыки за время, потраченное на получение сертификата.

Помните, что для прохождения лабораторных испытаний CCIE вовсе не обязательно получать сертификат CCNP или CCNA, однако выполнение этих тестов существенно расширит ваш опыт и упростит последний экзамен.

Что нужно знать для получения сертификата CCNP?

Для получения сертификата CCNP требуется определенный уровень профессиональных знаний. Помимо всего того, что необходимо для получения сертификата CCNA, соискатель должен:

- Уметь устанавливать, конфигурировать, работать, определять и устранять неисправности в сложных маршрутизируемых локальных и глобальных сетях, в локальных сетях с коммутацией и в службах доступа по телефонным линиям.
- Знать принципы функционирования сложных сетей, к которым относятся, например, IP, IGRP, IPX, асинхронные линии с маршрутизацией, AppleTalk, расширенные списки доступа, IP RIP, перераспределение маршрутов, IPX RIP, объединение маршрутов, OSPF, маски подсетей переменной длины, BGP, последовательные линии, IGRP, Frame Relay, ISDN, межкоммутаторные соединения (ISL), X.25, маршрутизация по каналам, предоставляемым по запросу (DDR), телефонные коммутируемые линии общего пользования (PSTN), PPP, виртуальные локальные сети, Ethernet, эмуляция локальных сетей ATM, списки доступа, 802.10, FDDI, прозрачные мосты и мосты с трансляцией.

Кроме этого, соискатель должен уметь:

- Устанавливать и/или конфигурировать сеть для повышения пропускной способности, снижения времени реакции сети, улучшения надежности и качества обслуживания
- Повышать производительность в сетях комплексных зданий, в маршрутизируемых региональных сетях и при удаленном доступе
- Повышать безопасность сети
- Создавать глобальную сеть интранет

- Обеспечивать безопасность доступа к коммутаторам и маршрутизаторам сети комплекса зданий
- Увеличивать пропускную способность при коммутации и маршрутизации для служб восстановления работоспособности
- Создавать службы поддержки очередей и маршрутизации по приоритетам

Как получить сертификат CCNP!

Для получения сертификата CCNP обладатель сертификата CCNA должен выдержать четыре экзамена:

Экзамен 640-503 В основу программы экзамена положены базовые понятия, получаемые соискателем при изучении курса ICRC. Основное внимание уделяется большим многопротокольным объединенным сетям и методам управления ими по спискам доступа, путем организации очередей, туннелирования, распределения и объединения маршрутов и каналов, предоставляемых по требованию.

Экзамен 640-504 Проверяется умение конфигурировать, наблюдать за поведением, обнаруживать и устранять неисправности устройств коммутации Cisco.

Экзамен 640-506 Здесь проверяется знание процедур обнаружения и устранения неисправностей, с которыми соискатель знакомится на учебных курсах Cisco.

Экзамен 640-505 Здесь проверяется знание процедур установки, конфигурирования, наблюдения за поведением, поиска и устранения неисправностей устройств Cisco для сетей ISDN и коммутируемых линий связи.

▼ ВНИМАНИЕ | Если вы не любите тесты, то можете сократить их число, сдав сначала экзамены CCNA и CIT, а затем более длинный экзамен 640-509 Foundation R/S (Основы маршрутизации и коммутации в сетях). В результате вы также получите сертификат CCNP, но действуйте осторожно: этот экзамен более сложный из-за того, что в его программу включен весь перечисленный выше материал. Желаем удачи! При этом вы экономите \$100, так как сдаете три теста по цене двух. Некоторые соискатели считают, что экзамен 640-509 проще выдержать, поскольку при расширенном объеме материала можно с большей вероятностью получить вопросы из разделов, которые вы лучше знаете.

▼ СОВЕТУЕМ | Вопросы и темы сертификационного экзамена могут быть изменены без предварительного уведомления. За последними новостями в этой области обратитесь на Web-сайт компании Cisco (www.cisco.com)

Сертификат Cisco Certified Internetworking Expert (CCIE)

Получив сертификат CCNP, вы начинаете думать о сертификате CCIE по маршрутизации и коммутации. Что же вы должны предпринять? Перед лабораторными испытаниями рекомендуется сдать экзамен 640-025 Cisco Internetwork Design (CID — создание объединенных сетей Cisco) и курс Installing and Maintaining Cisco Routers (IMCR — установка и поддержка маршрутизаторов Cisco). Предварительного теста для экзамена IMCR в настоящее время не существует, и Cisco считает, что для успешного прохождения лабораторных испытаний необходим двухлетний практический опыт. Преодолев все эти препятствия, вы должны сдать экзамен 350-001 CCIE-R/S Exam Qualification (Квалификационный экзамен по маршрутизации и коммутации).

Чтобы получить сертификат CCIE, необходимо:

1. Пройти все рекомендованные курсы в Authorized Cisco Training Center (Авторизованный центр практического обучения Cisco). Общие затраты составят \$15 000 — \$20 000 в зависимости от скидки, предоставляемой вашей компанией.
2. Сдать экзамен Drake/Prometric. (\$200 за экзамен, если вам удастся сдать его с первого раза.)
3. Пройти двухдневные лабораторные испытания в Cisco. Стоимость испытаний \$1000, однако многим соискателям приходится сдавать их по несколько раз. (А некоторые вообще не в состоянии пройти их!) Кроме того, экзамен можно сдать только в Сан-Хосе (Калифорния); в Research Triangle Park (Северная Каролина); в Сиднее (Австралия); в Галифаксе (Новая Шотландия); в Токио (Япония); в Брюсселе (Бельгия), так что необходимо учесть расходы на проезд (около \$1000).

Программа экзамена CCIE

Программа экзамена CCIE Router and Switching предполагает, что соискатель обладает расширенными техническими знаниями, необходимыми для поддержания оптимальной производительности и надежности сети, а также для сопровождения различных сетей, в которых используются самые разнообразные технологии. Обладатели сертификата CCIE без затруднений находят работу. Обычно эксперты завалены предложениями о работе с шестизначным окладом. И все это только потому, что достичь уровня, достаточного для сдачи экзамена CCIE, очень нелегко. Для этого необходимо:

- Уметь устанавливать, конфигурировать, работать, определять и устранять неисправности в сложных маршрутизируемых локальных и глобальных сетях, в локальных сетях с коммутацией и в службах доступа по телефонным линиям
- Диагностировать и устранять сетевые отказы
- Применять средства анализа пакетов/кадров и отладки Cisco

- Составлять документацию по применяемым методам разрешения проблем
- Знать основные особенности локальных и региональных сетей, в том числе инкапсуляцию данных в многоуровневой архитектуре, создание окон, управление потоком данных и задержками сети, алгоритмы маршрутизации по состоянию связи и по вектору расстояния, алгоритмы коммутации, методы управления, мониторинга и локализации отказов
- Знать различные корпоративные технологии, а также функции, структуры адресации, методы маршрутизации, коммутации, внедрения мостов для каждого из протоколов; технологии Cisco, включая платформы маршрутизаторов и коммутаторов, архитектуру и приложения; коммуникационные серверы; межпротокольное преобразование данных; команды конфигурирования и взаимодействие систем с сетью; интерфейсы локальных и глобальных сетей, их возможности и применение
- Иметь представление о специализированных технологиях Cisco, включая знание особенностей платформ маршрутизаторов и переключателей (а также их архитектуру и области применения), коммуникационных серверов, трансляции протоколов и приложений, команд конфигурации и влияния на сети и системы, интерфейсов локальных и региональных сетей (а также их возможности и области применения)
- Уметь разрабатывать, настраивать, устанавливать и тестировать соединения в сетях "голос поверх IP" и "голос поверх ATM"

Сертификаты Cisco в области создания сетей

Кроме сертификации специалистов по технической поддержке сетей, компания Cisco создала программу сертификации сетевых конструкторов. В ней предусмотрены две ступени: Cisco Certified Design Associate (CCDA — сертифицированный персонал по созданию сетей Cisco) и Cisco Certified Design Professional (CCDP — сертифицированный профессионал по созданию сетей Cisco). Мы настоятельно рекомендуем получить сертификаты CCDA и CCDP перед выполнением лабораторных испытаний.

Подготовка к этим экзаменам позволит получить знания, необходимые для создания маршрутизируемых локальных и глобальных сетей, локальных сетей с коммутацией и для эмуляции локальных сетей ATM.

Сертификат Cisco Certified Design Associate (CCDA)

Чтобы получить сертификат CCDA, необходимо сдать экзамен 640-441 DCN (Designing Cisco Networks, разработка сетей Cisco). Для этого требуется знание следующих вопросов:

- Создание простых маршрутизируемых локальных сетей, маршрутизируемых региональных сетей, локальных сетей с коммутацией и эмуляция локальных сетей ATM
- Адресация на сетевом уровне

- Фильтрация по спискам доступа
- Использование виртуальных локальных сетей
- Изменение размера сети

Сертификат Cisco Certified Design Professional (CCDP)

Если вы имеете сертификат CCNP и хотите получить сертификат CCDP, вам достаточно пройти тест CID 640-025. Однако если у вас нет сертификата CCNP, вам придется сдать экзамены ACRC, CLSC, CIT и CMTD.

Для получения сертификата CCDP соискатель должен знать:

- Методы создания сложных маршрутизируемых локальных сетей, маршрутизируемых региональных сетей, локальных сетей с коммутацией и эмуляции локальных сетей ATM на базе программы CCDA
- Методы построения сетей в объеме базового уровня CCDA

Кроме того, необходимо изучить следующие темы:

- Адресация на сетевом уровне в иерархической сетевой среде
- Управление трафиком по спискам доступа
- Создание иерархических сетей
- Использование виртуальных локальных сетей
- Производительность сетей: необходимая архитектура и программное обеспечение; механизм коммутации; память, стоимость и минимизация

Какие темы раскрываются в этой книге!

В книге рассматривается все, что необходимо для успешной сдачи экзамена CCNA.

Как сдать экзамен!

Вы можете сдать экзамен в одном из более чем 800 центров тестирования Sylvan Prometric Authorized Testing Center, разбросанных по всему миру. Расположение ближайшего Центра вы можете узнать по телефону (800) 755-3926. За пределами США и Канады обратитесь в местный Центр регистрации Sylvan Prometric Registration Center.

Чтобы записаться на экзамен CCNA, сделайте следующее:

1. Определите номер экзамена, который вы хотите сдать. (Экзамен CCNA имеет номер 640-507.)
2. Зарегистрируйтесь в ближайшем Центре Sylvan Prometric Registration Center. При этом вас попросят предварительно оплатить экзамен. К моменту выхода книги стоимость экзамена составляла \$100, причем сдать экзамен можно было в течение года после оплаты, назначив дату сдачи не менее чем за один день, но не более чем за 6 недель. Если вы по какой-то причине вынуждены отказаться от экзамена или перенести его на другой день, обратитесь в Центр не менее чем за 24 ч до срока. Сдача экзаменов Cisco в день регистрации невозможна.

3. При регистрации вам предоставят всю информацию о процедурах назначения даты сдачи экзамена и отказа от экзамена, сообщат ваш идентификатор и все о местоположении Центра.

Советы по сдаче экзамена CCNA

Тест CCNA содержит 70 вопросов, на которые надо ответить за 90 мин. Вы должны установить дату сдачи экзамена не менее чем за 24 ч (в отличие от экзаменов Novell и Microsoft) и не имеете права сдавать более одного экзамена в день.

Многие вопросы, особенно по синтаксису, имеют практически одинаковые варианты ответа. Запомните, что необходимо прочитать все ответы от начала до конца. Если вы укажете команду с неверным порядком аргументов или хотя бы с одним пропущенным символом, ваш ответ будет неверным.

В отличие от тестов Novell и Microsoft варианты ответов на экзамене Cisco похожи по синтаксису — некоторые конструкции ошибочны, но гораздо чаще ошибка *почти незаметна*. Иногда синтаксис конструкции корректен, но порядок элементов изменен. В вопросах Cisco следует обращать внимание на мелочи. Вот пример фрагмента:

```
access-list 101 deny ip any eq 23 denies Telnet access to all systems.
```

Он выглядит правдоподобно, и многие, видя упоминание о порте 23, вспоминают, что через этот порт производится доступ по Telnet. Хитрость в том, что пакеты IP (в отличие от пакетов UDP и TCP) нельзя фильтровать по номеру порта. Так что для практики выполняйте все упражнения, приводимые в конце глав, снова и снова, пока они не станут понятными для вас.

Кроме того, не забывайте, что правильным ответом является ответ Cisco. В вариантах ответов на многие вопросы может быть несколько правильных, однако корректен только ответ, рекомендованный Cisco.

Ниже приведены некоторые советы общего характера, полезные для сдачи экзамена:

- Приезжайте на экзамен заранее, чтобы немного расслабиться и еще раз заглянуть в учебные материалы, например в IP-таблицы, и просмотрите информацию, относящуюся к экзамену.
- Читайте вопросы *внимательно*, не глотайте слова. Убедитесь, что вы ясно и *точно* поняли, о чем идет речь в вопросе.
- Не оставляйте вопросы без ответов. Это повысит ваши шансы на успех.
- Если при выборе варианта ответа вы не уверены в правильности, используйте метод исключения, отбрасывая сначала заведомо неверные ответы. Такой подход существенно приблизит вас к успеху.
- Теперь на сертификационном экзамене Cisco на все вопросы нужно отвечать последовательно, поэтому дважды проверьте выбранный вами вариант прежде чем нажать кнопку Next.

По окончании экзамена вы немедленно получите уведомление об успехе или неудаче, отчет об экзамене и оценки по разделам. (Напечатанный отчет выдает администратор экзамена.) Результаты теста автоматически направляются в Cisco в течение пяти дней после экзамена, так что вам не нужно делать это самостоятельно. Если экзамен сдан успешно, вы получите поздравления Cisco (обычно через 2 – 4 недели).

Как пользоваться этой книгой?

Эта книга может послужить основой для серьезной подготовки к экзамену CCNA. Чтобы извлечь максимальную выгоду из чтения, вам необходимо прибегнуть к следующему методу обучения:

1. Внимательно изучите материал каждой главы и убедитесь в том, что вы все поняли и способны ответить на тестовые вопросы, перечисленные в конце главы.
2. Выполните упражнения каждой главы так, чтобы вам был понятен каждый шаг. Если у вас нет оборудования Cisco, внимательно изучите примеры.
3. Ответьте на контрольные вопросы по материалу прочитанной главы. (Ответы приведены в Приложении А.)
4. Обратите внимание на смутившие вас вопросы и проработайте соответствующие разделы книги еще раз.
5. Перед экзаменом попытайтесь ответить на практические вопросы, предложенные в приложении А.

Чтобы овладеть всем материалом книги, вы должны регулярно работать над ним. Постарайтесь учиться ежедневно, примерно в одни и те же часы и выберите для этого наиболее удобное место. При упорной работе вы быстро освоите предлагаемый материал. Желаем вам успеха!

Как связаться с автором этой книги?

К Тодду Лэммлу можно обратиться через его компанию Globalnet System Solutions, Inc. (www.lammle.com) или по адресу электронной почты todd@lammle.com.

Оценочный тест

1. Откуда загружается маршрутизатор, если конфигурационный регистр хранит значение 0x0101?
 - A. Флэш-память
 - B. ROM
 - C. Boot ROM
 - D. NVRAM

2. Каков корректный фильтр SAP с номером 1010 в интерфейсе Ethernet 0?
 - A. ip access-group 1010 in
 - B. ip access-group 1010 out**
 - C. ipx access-group 1010 in
 - D. ipx input-sap-filter 1010
 - E. ipx input-sap-filter 1010 in
3. Что выполняет устройство TE2 в соединении ISDN?
 - A. Соединяет устройство NT2 с опорной точкой U**
 - B. Соединяет интерфейс S/T с опорной точкой U
 - C. Соединяет не-ISDN терминал с ISDN через TA
 - D. Соединяет с ISDN по четырехпроводной цифровой линии на витых парах
4. Какая команда установит в маршрутизаторе идентификационное имя Atlanta, которое выводится администратору при подключении с консоли или по Telnet?
 - A. Description Atlanta Router
 - B. Banner Motd \$**
 - C. Hostname Atlanta
 - D. Host name Atlanta
 - E. Set prompt Atlanta
5. Как называются элементы PDU канального уровня?
 - A. Кадры**
 - B. Пакеты
 - C. Датаграммы
 - D. Транспорты
 - E. Сегменты
 - F. Биты
6. Каков диапазон хостов для IP-адреса 192.168.168.188 255.255.255.192?
 - A. 192.168.168.129-190**
 - B. 192.168.168.129-191
 - C. 192.168.168.128-190
 - D. 192.168.168.128-192
7. Каковы номера для стандартных списков доступа IP?
 - A. 1 – 10**
 - B. 1 – 99
 - C. 100 – 199
 - D. 1000 – 1999

8. Если команда `show interface serial 0` выведет показанное ниже сообщение, то в чем причина?
- ```
RouterA#sh int s0
Serial0 is up, line protocol is down
```
- A. Неправильно установлено значение `keepalives` (поддержание активности) между линиями "точка-точка".
  - B. К интерфейсу не подключен кабель.
  - C. Администратору необходимо выполнить в интерфейсе команду `no shutdown`.
  - D. Неисправен интерфейс.
9. Какая команда покажет для интерфейса адреса IPX (выберите все правильные ответы)?
- A. `show ipx address int e0`
  - B. `show protocol`
  - C. `show ipx protocol`
  - D. `show ipx interface`
10. Как создать путь по умолчанию?
- A. Установкой всех единиц в секции сети и маски
  - B. Указав статический путь, используя все нули в секции сети и маски
  - C. Используя 255 в секции сети и маски
  - D. Выполнив `login <имя, пароль>`
11. Что такое магистральная связь?
- A. Связь, принадлежащая только одной сети VLAN и являющаяся основной ("родной") для порта VLAN
  - B. Связь, способная поддерживать несколько сетей VLAN
  - C. Порт переключателя, подключенный к Интернету
  - D. Поддержка передачи данных и голоса в одном интерфейсе
12. Какой протокол позволяет получить IP-адрес по известному адресу Ethernet?
- A. IP
  - B. ARP
  - C. RARP
  - D. TCP
13. Каков адрес широковещательной рассылки для адреса подсети 192.168.99.20 255.255.255.252?
- A. 192.168.99.127
  - B. 192.168.99.63
  - C. 192.168.99.23
  - D. 192.168.99.31

14. Какому диапазону хостов принадлежит хост с идентификатором 192.168.10.33 255.255.255.224?
- A. 192.168.10.32-63
  - B. 192.168.10.33-63
  - C. 192.168.10.33-62
  - D. 192.168.10.33-61
15. Как обрабатывает переключатель полученный интерфейсом много-адресный кадр?
- A. Передает переключателю в первой из доступных связей
  - B. Отбрасывает кадр
  - C. Выдает в сеть кадр поиска устройства
  - D. Возвращает сообщение исходной станции с запросом на разрешение имени
16. Какая команда покажет пакеты IPX RIP, посланные и полученные интерфейсом?
- A. show ip rip
  - B. sh ipx int
  - C. debug ipx routing activity
  - D. debug ipx interface
17. Каков адрес подсети для IP-адреса 192.168.100.30 255.255.255.248?
- A. 192.168.100.32
  - B. 192.168.100.24
  - C. 192.168.100.0
  - D. 192.168.100.16
18. Что такое связь доступа?
- A. Связь, принадлежащая только одной сети VLAN и являющаяся основной ("родной") для порта VLAN
  - B. Связь, способная поддержать несколько сетей VLAN
  - C. Порт переключателя, подключенный к Интернету
  - D. Поддержка передачи данных и голоса в одном интерфейсе
19. Выберите правильные утверждения (укажите все правильные варианты).
- A. PPP можно использовать в Token Ring.
  - B. PPP можно использовать в синхронных последовательных линиях.
  - C. PPP можно использовать в асинхронных последовательных линиях.
  - D. PPP лицензирован в оборудовании каждой компании-производителя.

20. Какая команда восстанавливает конфигурацию маршрутизатора Cisco из хоста TFTP?
- A. copy run tftp
  - B. copy flash tftp**
  - C. copy nvram startup
  - D. copy tftp flash
21. Что выводит команда show cdp entry \* (укажите все правильные ответы)?
- A. IP-адрес соседнего маршрутизатора**
  - B. Сведения о протоколе**
  - C. Сведения о платформе**
  - D. Сведения о возможностях устройства**
  - E. Время**
  - F. Идентификатор порта**
  - G. Время удержания**
  - H. Информацию, как и команда show version**
  - I. Идентификатор соседнего устройства**
  - J. Локальный интерфейс**
  - K. Скорость линии**
22. Что из перечисленного не реализуется на уровне распределения?
- A. Списки доступа**
  - B. Фильтрация пакетов**
  - C. Очереди**
  - D. Деление домена конфликтов**
  - E. Трансляция адресов**
  - F. Функции брандмауэра**
  - G. Создание домена широковещательных рассылок**
23. Какой метод коммутации в локальных сетях имеет фиксированное время задержки (укажите все правильные ответы)?
- A. Cut-through (сквозной)**
  - B. Store and forward (сохранить и передать)**
  - C. FragmentCheck (проверки фрагментов)**
  - D. FragmentFree (бесфрагментный режим)**
24. На каком уровне модели Cisco реализованы функции деления доменов конфликтов?
- A. Физическом**
  - B. Доступа**
  - C. Базовом**
  - D. Сетевом**

- E. Распределения
  - F. Канальном
25. Что следует ввести в приглашении, чтобы получить список всех команд, начинающихся на "cl"?
- A. Show commands cl
  - B. Cl?**
  - C. Cl?
  - D. Cl ? more
26. Что реализует сеть VLAN?
- A. Делит домен конфликтов**
  - B. Делит домен маршрутизации
  - C. Делит домен широковещательных рассылок
  - D. Обеспечивает сегментацию при фрагментации
27. Что присутствует в таблице маршрутизации (выберите все правильные ответы)?
- A. Сетевой адрес**
  - B. Метрика маршрутизации**
  - C. Выходной интерфейс для пакета**
  - D. Входной интерфейс**
28. Какая команда покажет устройства, подключенные к маршрутизатору по Telnet?
- A. show vty line
  - B. show vers**
  - C. show users
  - D. show connections
29. Что означает административное расстояние 0?
- A. Административное расстояние по умолчанию для динамической маршрутизации**
  - B. Административное расстояние по умолчанию для непосредственно подключенных путей.**
  - C. В маршрутизаторе запрещена маршрутизация
  - D. Для следующей точки назначения 0 участков
30. Какой улучшенный список доступа IP корректен?
- A. access-list 110 permit ip any host 1.1.1.1 eq ftp
  - B. access-list 10 permit tcp ip any any eq 21
  - C. access-list 99 permit udp any host 2.2.2.2 eq ip
  - D. access-list 199 permit tcp any 0.0.0.0 255.255.255.255 eq 21
31. Что справедливо для заблокированного состояния коммутируемого порта STP (выберите все правильные ответы)?

- A. Блокированный порт не пересылает никаких кадров.
  - B. Блокированный порт прослушивает элементы BPDU.
  - C. Блокированный порт пересылает все кадры.
  - D. Блокированный порт не прослушивает элементы BPDU.
32. Каков по умолчанию тип коммутации локальной сети в переключателе серии 1900?
- A. FastForward (быстрое перенаправление)
  - B. Cut-through (сквозной)
  - C. Тип 1 коммутации локальной сети
  - D. FragmentFree (с исключением фрагментов)
  - E. Store and forward (сохранить и передать)
33. Что справедливо для разрешенных паролей (выберите все правильные ответы)?
- A. Разрешенный пароль шифрован по умолчанию.
  - B. Разрешенный секрет шифрован по умолчанию.
  - C. Необходимо сначала ввести разрешенный шифрованный пароль.
  - D. Разрешенный шифрованный пароль отменяет действие разрешенного секрета.
  - E. Пароль разрешенного секрета отменяет действие разрешенного пароля.
  - F. Разрешенный шифрованный пароль отменяет действие всех остальных паролей.
34. Каково по умолчанию административное расстояние для протокола RIP?
- A. 1
  - B. 100
  - C. 120
  - D. 150
35. Если на введенную команду было получено показанное ниже сообщение, то в чем ошибка и как ее исправить (укажите все правильные ответы)?
- ```
Router#clockset 10:30:10
% Incomplete command.
```
- A. IOS не поддерживает часы в данном маршрутизаторе.
 - B. Не завершена командная строка.
 - C. Нажмите клавишу "стрелка вверх" и введите вопросительный знак.
 - D. Нажмите клавишу "стрелка вниз", затем клавишу табуляции Tab.
 - E. Сотрите введенную команду и перезагрузите маршрутизатор.

36. Что означает 175 в показанной команде?
- ```
Ip route 150.150.0.0 255.255.0.0 150.150.150.150 175
```
- A. Следующий участок
  - B. Административное расстояние
  - C. Обновление широковещательными рассылками
  - D. Ничего, это неправильная команда
37. Что делает маршрутизатор с пакетами, для которых неизвестна сеть назначения?
- A. Перенаправляет пакет
  - B. Отбрасывает пакет
  - C. Сохраняет пакет до следующего обновления путей
  - D. Посылает широковещательную рассылку к неизвестной сети
38. Что определяет сеть и узел в адресе 7с8.0001.00с8.1234?
- A. сеть: 7с8.0001, узел: 00с8.1234
  - B. сеть: 7с8, узел: 0001.00с8.1234
  - C. сеть: 0001.00с8.1234, узел: 7с8
  - D. сеть: 7с8.0001.00с8, узел: 1234
39. Какие два типа элементов PDU используются на сетевом уровне?
- A. Данные
  - B. Путь
  - C. Статический
  - D. Динамический
  - E. Основной
  - F. Сегмент
40. Какой тип инкапсуляции Cisco служит для маркирования кадров в магистральных связях?
- A. Virtual Trunk Protocol (VTP)
  - B. 802.1q
  - C. ISL
  - D. VLANs
41. Что учитывает протокол RIP стека IPX при определении наилучшего пути к удаленной сети (выберите все правильные ответы)?
- A. Полосу пропускания линии
  - B. Счетчик участков
  - C. Надежность линии
  - D. Величину задержки, отсчитываемую в 1/18с
42. Каковы номера для улучшенных списков доступа?
- A. 1 – 10
  - B. 1 – 99

- C.** 100 – 199  
**D.** 1000 – 1999
- 43.** Что означает команда  
Access-list 110 permit ip any 0.0.0.0 255.255.255.255?  
**A.** Стандартный список доступа IP, ограничивающийся только сетью 0.0.0.0  
**B.** Улучшенный список доступа IP, ограничивающий только сетью 0.0.0.0  
**C.** Улучшенный список доступа, разрешающий любой хост или сеть  
**D.** Команда неправильная
- 44.** Что такое статическая сеть VLAN?  
**A.** VLAN, которую нельзя переименовать или удалить  
**B.** VLAN, созданная администратором  
**C.** Порты переключателя, присвоенные сети VLAN администратором  
**D.** Порты переключателя, присвоенные сети VLAN сервером VTP
- 45.** Что справедливо для команды `isdn switch-type`?  
**A.** Может вводиться только в режиме глобального конфигурирования  
**B.** Может вводиться только в режиме конфигурирования интерфейса  
**C.** Может вводиться как в режиме глобального конфигурирования, так и в режиме конфигурирования интерфейса.  
**D.** Может использоваться только для TA
- 46.** Какой механизм указывает устройству-источнику на снижение скорости при перегрузке сети Frame Relay?  
**A.** HDLC  
**B.** DLCI  
**C.** FECN  
**D.** BECN
- 47.** Какой метод используется в сетях Frame Relay для адресации цепей PVC по IP-адресам?  
**A.** ARP  
**B.** LMI  
**C.** SLARP  
**D.** DLCI
- 48.** Каковы два способа добавления в локальной сети Ethernet IPX нескольких методов инкапсуляции?  
**A.** Несколько типов кадров  
**B.** Дополнительный  
**C.** Подинтерфейс  
**D.** Виртуальный дополнительный

49. Каково типичное время перехода коммутируемого порта из состояния блокировки в состояние перенаправления трафика?
- A. 5с
  - B. 50с
  - C. 10с
  - D. 100с
50. Как обратиться по Telnet из интерфейса CLI переключателя серии 1900?
- A. telnet Atlanta.
  - B. telnet 172.16.10.1.
  - C. ping 172.16.10.1.
  - D. Не поддерживается в CLI переключателя 1900
51. Какая команда удалит MAC-адрес, автоматически введенный в фильтрующей таблице MAC-адресов?
- A. (config)#delete nvram
  - B. #delete nvram
  - C. (config)#clear mac-address-table dynamic
  - D. #clear mac-address-table dynamic
52. Какую команду следует ввести для полной очистки конфигурации в переключателе 1900 (укажите все правильные ответы)?
- A. Clear config
  - B. Delete nvram
  - C. Delete vtp
  - D. Delete start
  - E. Erase startup-config
  - F. Just reboot the switch.
53. Какая команда покажет состояние магистральной связи в порту 27 переключателя серии 1900?
- A. Show port 27
  - B. Show trunk
  - C. Show trunk B
  - D. Show trunk f0/27
  - E. Show trunk e0/27
54. Что следует ввести в консольном приглашении переключателя серии 1900 для вывода статистики получения и приема информации VTP?
- A. Show vtp stat
  - B. Show stat
  - C. Sh vtp domain
  - D. Sh int e0/9

## Ответы на оценочный тест

1. В (см. главу 7)
2. D (см. главу 9)
3. D (см. главу 10)
4. C (см. главу 4)
5. A (см. главу 1)
6. A (см. главу 3)
7. В (см. главу 9)
8. A (см. главу 4)
9. В, D (см. главу 8)
10. В (см. главу 5)
11. В (см. главу 6)
12. C (см. главу 3)
13. C (см. главу 3)
14. C (см. главу 3)
15. C (см. главу 2)
16. В (см. главу 8)
17. В (см. главу 3)
18. A (см. главу 6)
19. В, C (см. главу 10)
20. A (см. главу 7)
21. A, B, C, D, F, G, H, I, J  
(см. главу 7)
22. D (см. главу 1)
23. A, D (см. главу 2)
24. В (см. главу 1)
25. C (см. главу 4)
26. C (см. главу 6)
27. A, B, C (см. главу 1)
28. C (см. главу 7)
29. В (см. главу 5)
30. D (см. главу 9)
31. A, B (см. главу 2)
32. D (см. главу 2)
33. В, E (см. главу 4)
34. C (см. главу 5)
35. В, C (см. главу 4)
36. В (см. главу 5)
37. В (см. главу 5)
38. В (см. главу 8)
39. A, B (см. главу 1)
40. C (см. главу 6)
41. В, D (см. главу 8)
42. C (см. главу 9)
43. C (см. главу 9)
44. C (см. главу 6)
45. C (см. главу 10)
46. D (см. главу 10)
47. D (см. главу 10)
48. В, C (см. главу 8)
49. В (см. главу 2)
50. D (см. приложение В)
51. D (см. приложение В)
52. В, C (см. приложение В)
53. C (см. приложение В)
54. A (см. приложение В)

Table of Contents

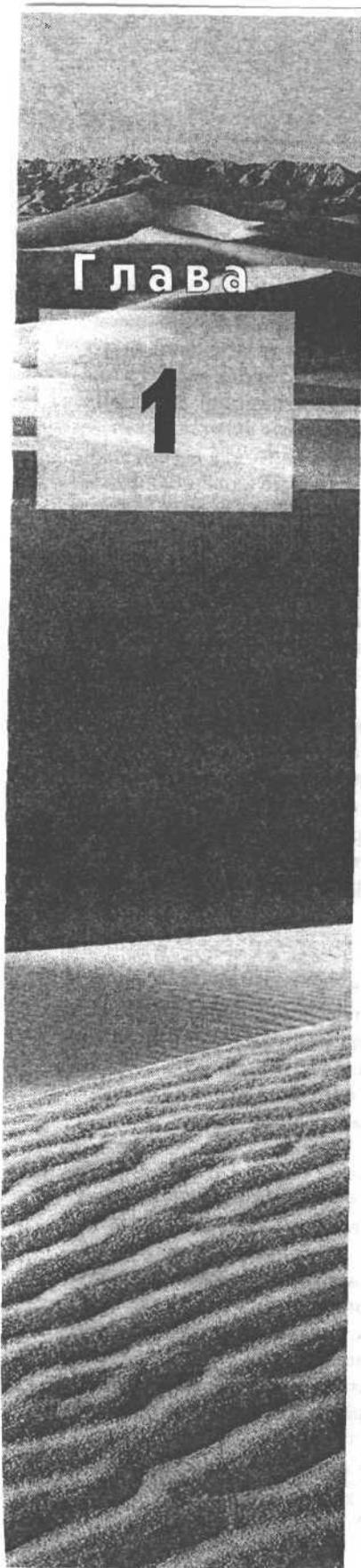
- 1. Introduction
- 2. Theoretical background
- 3. Methodology
- 4. Results
- 5. Discussion
- 6. Conclusion
- 7. References
- 8. Appendix
- 9. Glossary
- 10. Index

Table of Contents

- 1. Introduction
- 2. Theoretical background
- 3. Methodology
- 4. Results
- 5. Discussion
- 6. Conclusion
- 7. References
- 8. Appendix
- 9. Glossary
- 10. Index

Table of Contents

- 1. Introduction
- 2. Theoretical background
- 3. Methodology
- 4. Results
- 5. Discussion
- 6. Conclusion
- 7. References
- 8. Appendix
- 9. Glossary
- 10. Index



Глава

1

# Введение в объединенные сети

## Модели объединенных сетей

В первых вычислительных сетях взаимодействовать друг с другом могли компьютеры только одного производителя. Например, сети потребителей создавались либо на основе DECnet, либо в соответствии с рекомендациями IBM, причем совместное использование этих технологий было невозможно. В начале 80-х годов для преодоления этого препятствия Международная организация по стандартизации (International Standards Organization, ISO) разработала модель OSI (*Open Systems Interconnection* — взаимодействие открытых систем). Цель разработки состояла в том, чтобы способствовать созданию сетевых устройств, которые могли бы функционировать в единой среде. Хотя полная совместимость, скорее всего, недостижима, как и всеобщий мир на нашей планете, однако грандиозная цель была обозначена.

Модель OSI является основной моделью, определяющей архитектуру сети. Она описывает, каким образом прикладные программы, выполняемые на разных компьютерах, обмениваются данными и сетевой информацией по сетевому носителю. В рамках базовой модели OSI механизм обмена разделен на несколько уровней.

Компания Cisco создала собственную трехуровневую модель, помогающую разрабатывать, внедрять и обслуживать сети любого размера. Знание уровней этой модели позволит лучше понять концепции Cisco в области объединенных сетей. Кроме того, знание распределения разных устройств по уровням этой модели позволит правильно выбрать и приобрести оборудование Cisco, отвечающее требованиям конкретной сети. В этой главе рассматриваются модель OSI и трехуровневая иерархическая модель Cisco.

## Многоуровневый коммуникационный подход

*Базовая модель* (reference model) является концептуальной основой коммуникационного процесса. Она определяет все задачи, решаемые при организации эффективного взаимодействия систем, группируя их по так называемым *уровням* (layer). Коммуникационная система, разработанная с учетом базовой модели OSI, имеет *многоуровневую архитектуру* (layered architecture).

Рассмотрим следующий пример. Вы с друзьями хотите создать свою фирму. Прежде всего, следует подумать о том, что конкретно необходимо производить, кто создаст нужные изделия, в какой последовательности и как участники производственного процесса будут взаимодействовать друг с другом. Распределите эти задачи между отделами фирмы. Предположим, что решено образовать отдел приема заказов, отдел учета и отдел сбыта, каждый из которых имеет собственные задачи, причем персонал отдела в основном занят только их решением.

В этом примере отделы можно рассматривать как уровни коммуникационной системы. Для успешной работы фирмы персонал каждого отдела должен иметь определенные полномочия, тесно взаимодействовать с персоналом других отделов и компетентно выполнять собственные

обязанности. В процессе планирования вы, вероятно, делаете заметки, описывая все свои действия, чтобы в дальнейшем упростить обсуждение совокупности стандартов, составляющих служебную инструкцию, регламентирующую деятельность фирмы. Эта инструкция могла бы рассматриваться как аналог базовой модели.

Начальник каждого отдела, руководствуясь частью служебной инструкции, относящейся к его отделу, разрабатывает практические методы выполнения задач, стоящих перед отделом. Эти методы перечисляются в сборнике стандартных рабочих процедур и должны строго исполняться. Процедуры предназначены для различных целей и имеют разную степень важности и обязательности выполнения. Если вы договариваетесь о партнерстве или приобретении другой фирмы, эти процедуры должны выполняться и вашими партнерами, чтобы была достигнута совместимость их и вашей деятельности.

Подобным образом разработчики программного обеспечения могут использовать базовую модель. Она помогает разобраться в процессе взаимодействия компьютеров, и понять, какие виды функций должны быть реализованы на каждом уровне. Протокол, созданный для некоторого уровня, определяет функции именно этого, а не какого-либо иного уровня. Другие протоколы и уровни предназначены для выполнения других функций. На техническом языке это свойство называется *связыванием* (binding). Коммуникационные процессы, связанные друг с другом, сгруппированы вместе и протекают на одном конкретном уровне.

## Достоинства базовой модели

Использование базовой модели OSI, как и модели Cisco, имеет многочисленные достоинства. Основной целью любой модели является совместимость оборудования разных производителей. Отметим преимущества моделей OSI и Cisco:

- Деление сложных сетевых операций на легко управляемые уровни
- Изменения на одном уровне не действуют на другие уровни модели, что позволяет разработчикам приложений специализироваться на определенных и ограниченных задачах
- Определение стандартных интерфейсов для простой интеграции оборудования различных компаний

## Базовая модель OSI

Базовая (ссылочная) модель OSI была создана в конце 70-х годов для описания пересылки данных между сетевыми узлами. Важнейшей целью спецификации модели OSI была помощь в описании передачи данных между разнородными хостами, например между компьютером с операционной системой (ОС) Unix и персональным компьютером (ПК).

Модель OSI не является физической, но устанавливает набор рекомендаций для разработчиков приложений. Он призван стандартизировать создание и внедрение сетевых программ. Кроме того, модель OSI

формирует каркас (framework) для создания и внедрения сетевых стандартов, устройств и схем объединения сетей.

В модели OSI установлены семь уровней, объединяемых в две группы. Три верхних уровня описывают функции приложения на оконечной рабочей станции для взаимодействия с другими приложениями и пользователями. Четыре нижних уровня определяют процедуру пересылки данных между оконечными точками сети. На рис. 1.1 показаны функции трех верхних уровней модели OSI, а на рис. 1.2 — функции четырех нижних уровней этой модели.

|                       |                                                                         |
|-----------------------|-------------------------------------------------------------------------|
| Уровень приложений    | • Обеспечивает пользовательский интерфейс                               |
| Уровень представлений | • Представление данных<br>• Управление процессами, например шифрованием |
| Сеансовый уровень     | • Разделение данных разных приложений                                   |
| Транспортный уровень  |                                                                         |
| Сетевой уровень       |                                                                         |
| Канальный уровень     |                                                                         |
| Физический уровень    |                                                                         |

Рис. 1.1. Верхние уровни модели OSI

|                      |                                                                                                                                                                                 |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Транспортный уровень | • Обеспечивает надежную или ненадежную доставку<br>• Проводит коррекцию ошибок перед повторной передачей данных                                                                 |
| Сетевой уровень      | • Обеспечивает логическую адресацию, где путь определяется маршрутизаторами                                                                                                     |
| Канальный уровень    | • Разделяет пакеты на байты и объединяет байты в кадры<br>• Обеспечивает адресацию на уровне носителя с помощью MAC-адресов<br>• Выполняет выявление ошибок, но не их коррекцию |
| Физический уровень   | • Перемещает между устройствами биты данных<br>• Определяет уровни напряжений, скорость передачи в линии и распределение линий в разъемах.                                      |

Рис. 1.2. Нижние уровни модели OSI

На рис. 1.1 видно, что на уровне приложений реализован пользовательский интерфейс. Все верхние уровни модели отвечают за коммуникацию приложений на разных хостах. Ни один из верхних уровней не

обязан ничего знать о сетевых операциях или сетевых адресах. Для этого используются четыре нижних уровня (см. рис. 1.2).

Четыре нижних уровня специфицируют передачу данных либо по физическим проводам, либо через переключатели и маршрутизаторы, а также процедуру восстановления потока данных между передающим хостом и приложением на принимающем хосте.

## Уровни модели OSI

Международная организация по стандартизации (International Standards Organization, ISO) является законодателем в мире сетевых протоколов. Ею разработана базовая модель OSI в качестве основы для открытого множества сетевых протоколов. Эта модель определяет правила сетевого взаимодействия и до сих пор остается самым популярным средством сопоставления семейств протоколов. В модели OSI предусмотрены семь уровней:

- Уровень приложений
- Уровень представлений
- Сеансовый уровень
- Транспортный уровень
- Сетевой уровень
- Канальный уровень (или уровень связи данных)
- Физический уровень

На рис. 1.3 показаны функции уровней модели OSI.

|                       |                                                             |
|-----------------------|-------------------------------------------------------------|
| Уровень приложений    | • Службы печати, сообщений, баз данных, файлов и приложений |
| Уровень представлений | • Службы шифрования данных, сжатия и преобразования         |
| Сеансовый уровень     | • Управление диалогом                                       |
| Транспортный уровень  | • Соединение между конечными точками                        |
| Сетевой уровень       | • Маршрутизация                                             |
| Канальный уровень     | • Формирование кадров                                       |
| Физический уровень    | • Физическая топология                                      |

Рис. 1.3. Функции уровней модели OSI

## Уровень приложений

*Уровень приложений* модели OSI поддерживает компоненты, определяющие взаимодействие пользователей с компьютерами. Этот уровень ответствен за идентификацию и установление доступности предполагаемого партнера по диалогу. Здесь же определяется, достаточно ли ресурсов для взаимодействия.

Хотя приложения иногда требуют доступ к ресурсам только настольного компьютера, они могут объединять взаимодействующие компоненты нескольких сетевых приложений, например служб пересылки файлов и электронной почты, процессов управления сетью, процессов клиент/сервер и службы определения местоположения информации. Многие сетевые приложения допускают организацию их взаимодействия в сети уровня предприятия, но при объединении сетей в будущем потребуются преодолеть ограничения на размер сети. С начала 90-х годов транзакции и обмен информацией между организациями приобрели столь широкий размах, что стали жизненно необходимыми. Были созданы приложения для межсетевого взаимодействия, к которым относятся:

**WWW (World Wide Web — "Всемирная паутина")** Связывает бесчисленные серверы (их количество растет с каждым днем), поддерживающие различные форматы данных. Большинство серверов, являясь мультимедийными, допускают использование графических, текстовых, видео- и даже аудиоданных. Доступ к Web-серверам и просмотр информации упрощаются при использовании Netscape Navigator, Internet Explorer и других браузеров, подобных Mosaic.

**Шлюзы электронной почты** Могут использовать протокол SMTP или стандарт X.400 для доставки сообщений между различными приложениями электронной почты.

**Электронный обмен данными** Это набор специализированных стандартов и процессов, упрощающих пересылку между фирмами финансовой документации, касающейся, например бухгалтерского учета, распространения и получения продукции, а также ведомостей заказов и инвентаризационных документов.

**Специализированные доски объявлений** К ним относятся многочисленные дискуссионные группы в Интернете, участники которых могут связываться или взаимодействовать друг с другом, либо посылая сообщения, либо ведя беседу в реальном времени. Доски объявлений могут совместно использовать общедоступное программное обеспечение.

**Утилиты навигации по Интернету** Приложения типа Gopher и WAIS, а также поисковые программы, подобные Yahoo!, Excite и Alta Vista, помогают пользователям определить местоположение в Интернете необходимых ресурсов и информации.

**Службы пересылки финансовой информации** Являются пределом мечтаний финансового сообщества. Собирают и продают своим подписчикам информацию об инвестициях, торговле, состоянии потребительского рынка, валютных курсах, а также банковские данные.

## Уровень представлений

Название этого уровня отражает его назначение. Здесь данные форматируются, или, как иногда говорят, транслируются для представления их на уровне приложений. Для удобства передачи данные перед пересылкой приводятся к стандартному формату. Компьютеры настраиваются на их получение; принятые данные преобразуются в формат, пригодный для чтения (например, транслируются из кода EBCDIC в код ASCII). За счет службы преобразования на уровне представления можно гарантировать, что данные с уровня приложений одной системы попадут на этот же уровень другой системы. Модель OSI имеет протокол, определяющий способ переформатирования стандартных данных. На этом уровне выполняются также уплотнение, разуплотнение, кодирование и декодирование данных. Некоторые стандарты уровня представлений включены в мультимедийные операции. Ниже перечислены форматы для представления графических и визуальных данных:

**PICT** Формат изображений, используемый в программах Macintosh или PowerPC для передачи графических данных QuickDraw.

**TIFF** Стандартный графический формат для растровых изображений с высоким разрешением.

**JPEG** Стандарт, разработанный Объединенной группой экспертов по фотографии (JPEG).

Следующие стандарты приняты для представления движущихся изображений и аудиоданных:

**MIDI** Интерфейс, используемый для цифрового представления музыки.

**MPEG** Стандарт, разработанный Группой экспертов по движущимся изображениям с целью уплотнения и кодирования движущихся видеоизображений для компакт-дисков, становится все более популярным. Он используется для хранения изображений в цифровой форме и допускает скорость передачи до 1.5 Мбит/с.

**Quick Time** Формат, используемый в программах Macintosh или PowerPC для управления аудио- и видеоданными в соответствующих приложениях.

## Сеансовый уровень

Основная функция, выполняемая на *сеансовом уровне*, напоминает работу посредника или судьи — управление диалогом между устройствами, называемыми также узлами. Взаимодействие систем, организуемое на этом уровне, может происходить в трех различных режимах: *симплексном* (simplex), *полудуплексном* (half-duplex) и *полнодуплексном* (full-duplex). Сеансовый уровень обычно занимается отделением данных одного приложения от информации другого приложения.

Ниже приведены некоторые протоколы и интерфейсы сеансового уровня:

**NFS** (Network File System — сетевая файловая система) Создана компанией Sun Microsystems и используется на рабочих станциях Unix вместе с TCP/IP, чтобы сделать доступ к удаленным ресурсам прозрачным для пользователя.

**SQL** (Structured Query Language — язык структурированных запросов) На языке SQL, разработанном компанией IBM, пользователь может в несложной форме определить свои требования к информации, доступ к которой производится на локальных или удаленных системах.

**RPC** (Remote Procedure Call — вызов удаленных процедур) Является простым инструментом переадресации в среде клиент/сервер. Процедуры RPC создаются на компьютере клиента и выполняются на сервере.

**X Window** , Широко применяется на интеллектуальных терминалах для связи с удаленными компьютерами Unix и позволяет работать с этими компьютерами, как с локальными.

**ASP** (AppleTalk Session Protocol — сеансовый протокол AppleTalk) Применяется в среде клиент/сервер. Предназначен для установления и поддержки сеанса между машинами клиента и сервера по протоколу ASP.

**DNA SCP** (Digital Network Architecture Session Control Protocol — протокол сеансового уровня DNA) Является протоколом сеансового уровня в сетях DECnet.

## Транспортный уровень

Службы *транспортного уровня* осуществляют сегментирование и сборку данных, поступающих от приложений более высоких уровней, и организуют единый поток данных. Они обеспечивают транспортировку данных между конечными точками и устанавливают логическое соединение между хостами отправителя и получателя в объединенной сети.

Читатели, знакомые с протоколами TCP и UDP (см. главу 3), знают, что TCP обеспечивает гарантированную (надежную) доставку данных, а UDP — этого не делает. Разработчик приложения может выбрать для доставки данных любой из этих протоколов.

Службы транспортного уровня отвечают за работу механизмов мультиплексирования приложений верхних уровней, установление соединения и закрытие виртуальных каналов. Кроме того, они скрывают от более высоких уровней подробности процессов, происходящих в сетевой среде. Они делают передачу данных прозрачной.

## Управление потоком

Сохранение целостности данных достигается за счет применения механизма управления потоком данных и предоставления пользователю возможности выбора протокола надежной транспортировки данных между системами. *Управление потоком* данных не позволяет хосту-отправителю передавать данные так, чтобы переполнились буферы приема данных на хосте-получателе, поскольку переполнение приводит к потере данных.

Протокол надежной доставки данных применяется в сеансах связи, ориентированных на установление соединения между системами, причем надежность доставки гарантируется тем, что:

- Отправитель получает подтверждение от принимающей стороны о доставке сегментов данных
- Любые неподтвержденные сегменты передаются повторно
- Принятые сегменты упорядочиваются в соответствии с последовательностью их передачи
- Во избежание перегрузки сети, переполнения буферов и потери данных используется управление потоком данных

### Коммуникации, ориентированные на создание соединений

Согласно протоколу надежной транспортировки, по запросу одного из пользователей производится установление соединения. На рис. 1.4 представлен обычный процесс с установлением соединения между передающей и принимающей системами, Прикладные программы обоих хостов начинаются с уведомления своих операционных систем о необходимости инициализации соединения. Операционные системы обмениваются сообщениями, подтверждающими согласие и готовность обеих сторон начать обмен данными. После завершения синхронизации соединение считается установленным, и начинается собственно передача данных.

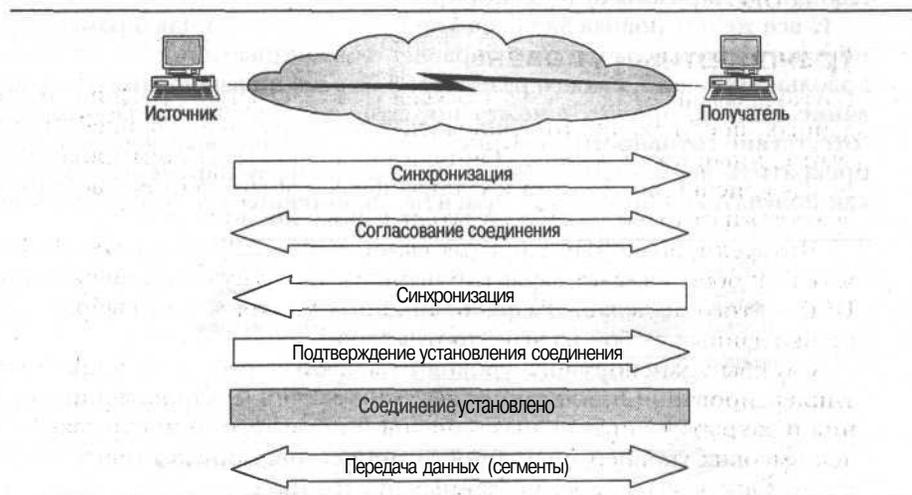


Рис. 1.4. Взаимодействие с установлением соединения

В процессе передачи информации обе машины периодически проверяют друг друга, связываясь через программное обеспечение протокола, чтобы удостовериться в существовании соединения и в корректности передачи данных.

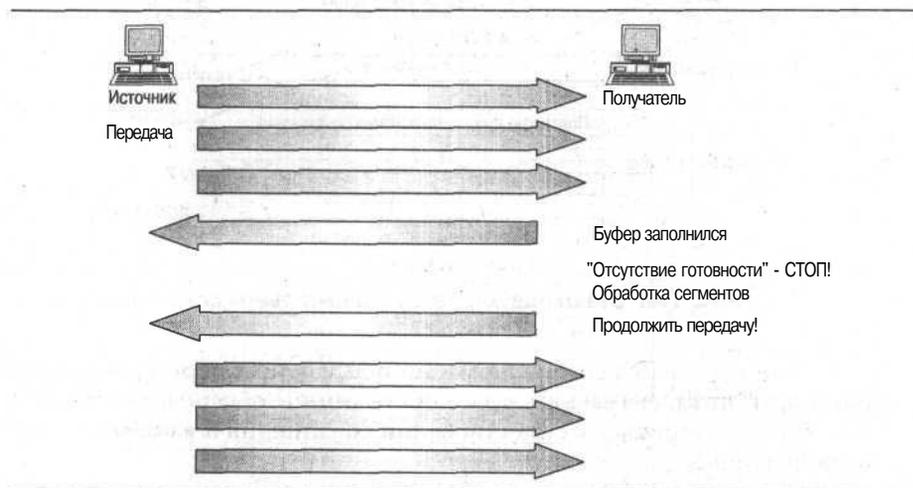
Ниже кратко описаны шаги сеанса, ориентированного на установление соединения (см. рис. 1.4):

- Первый сегмент "согласия на установление соединения" является запросом на синхронизацию.
- Вторым и третьим сегментами подтверждается получение запроса и определяются параметры соединения между хостами.
- Последний сегмент также является подтверждением, оповещающим получателя о том, что достигнуто согласие на установление соединения и что соединение установлено. После этого может начаться передача данных.

Во время передачи данных может возникнуть перегрузка из-за того, что высокоскоростной компьютер создает трафик быстрее, чем сеть передает данные, или потому, что несколько компьютеров одновременно посылают датаграммы через один шлюз или одному получателю. В последнем случае перегрузка шлюза или получателя не всегда вызывается единственным источником. Перегрузка напоминает проезд через сужение дороги — слишком интенсивный трафик при небольшой пропускной способности.

Обычно дело не в конкретной машине, а в том, что дорога забита машинами. Если компьютер не успевает обработать поступающий поток датаграмм, он сохраняет их в памяти. *Буферизация* решает проблему перегрузки только, если лавинный поток носит кратковременный характер. Однако если длительность мощного потока датаграмм велика, буферная память устройства в конце концов переполнится, и любые вновь поступающие датаграммы будут игнорироваться.

И все же нет повода для беспокойства: реализованная в рамках транспортного протокола система управления лавинными потоками работает довольно успешно. Вместо разгрузки ресурсов и разрешения на отбрасывание данных, протокол может послать хосту-источнику лавины сигнал "отсутствие готовности" (см. рис. 1.5). Этот сигнал вынуждает источник прекратить передачу сегментов перегруженному партнеру. После того как получатель обработает сегменты, скопившиеся в буферной памяти,



**Рис. 1.5.** Управление потоком передаваемых сегментов

он отправит источнику сигнал "готовность". Получив разрешение, хост-источник продолжит передачу.

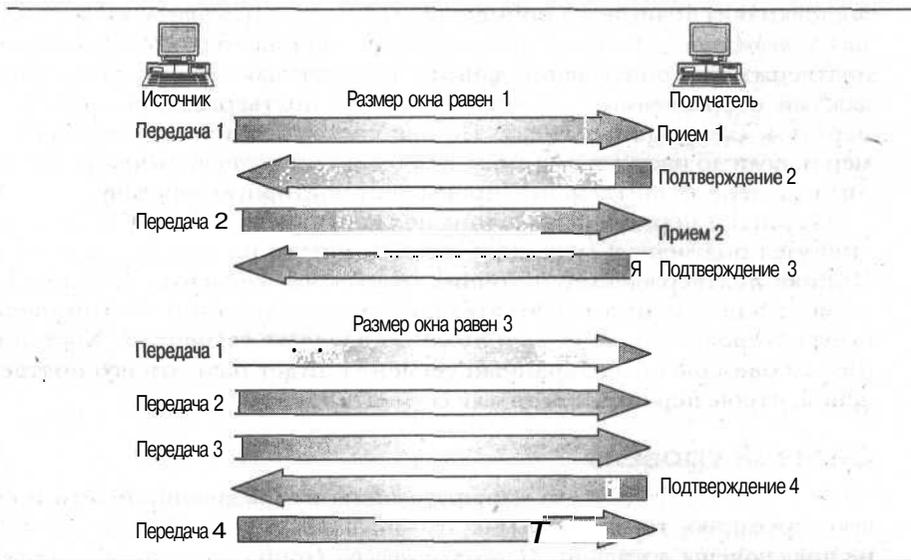
В принципе, при надежной и ориентированной на соединение доставке данных датаграммы поступают на принимающий хост в той последовательности, в которой были отправлены. Если теряется, дублируется или искажается один из сегментов, то фиксируется ошибка всего процесса передачи данных. Чтобы решать такие проблемы, принимающий хост обязан подтверждать получение сегментов данных.

**Использование окон**

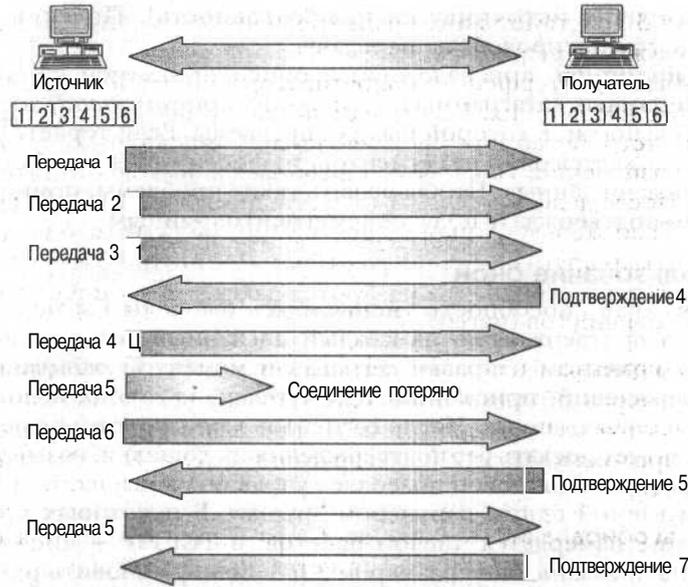
Пропускная способность уменьшилась бы, если бы передающий хост ожидал подтверждения на каждый посланный сегмент, поэтому время между моментом отправки сегмента и моментом окончания обработки подтверждений, присланных получателем, источник использует для передачи новых данных. Число сегментов данных, которое передающая машина может послать без подтверждения их доставки, называется *окном*.

Использование окон позволяет управлять количеством информации, передаваемой одним партнером другому. В некоторых протоколах это значение измеряется числом пакетов, в TCP/IP — числом байтов. На рис. 1.6 показаны окна размером 1 и 3. Если установить размер окна равным 1, перед отправкой очередного сегмента хост-источник будет ожидать подтверждения предыдущего.

Если размер окна равен 3, до получения подтверждения можно отправить три сегмента. В нашем упрощенном примере и источник, и получатель являются рабочими станциями. В действительности так бывает редко; чаще всего подтверждения и пакеты перемешиваются, поскольку они перемещаются по сети и проходят через маршрутизаторы. Маршрутизация усложняет ситуацию, но к этой теме мы обратимся позднее.



**Рис. 1.6.** Использование окон



**Рис. 1.7.** Обеспечение надежности доставки данных на транспортном уровне

### Подтверждение

При надежной доставке данных гарантируется целостность потока данных, которые одна машина посылает другой по исправному каналу. Это означает, что данные не будут дублироваться или теряться. Надежность доставки обеспечивается применением метода *положительного подтверждения с повтором передачи*. Принимающая машина отправляет передающей подтверждения о получении данных. Передающая сторона регистрирует каждый отправленный сегмент и ожидает подтверждения, прежде чем передать следующий сегмент. Послав сегмент, источник запускает таймер и, если до наступления тайм-аута от принимающей стороны не поступит подтверждение сегмента, производит повторную передачу.

На рис. 1.7 передающая машина послала сегменты 1, 2 и 3. Принимающий узел подтверждает их получение запросом на передачу сегмента 4. Приняв подтверждение, источник отправляет сегменты 4, 5 и 6. Если сегмент 5 не достигнет получателя, последний уведомит об этом передающую сторону запросом на повторную передачу сегмента 5. Хост-источник заново пошлет потерянный сегмент и будет ожидать его подтверждения, чтобы перейти к отправке сегмента 7.

### Сетевой уровень

*Сетевой уровень* отвечает за маршрутизацию в объединенной сети и сетевую адресацию, т.е. за пересылку трафика между устройствами, которые не подключены локально. *Маршрутизаторы* (router) или иные устройства

уровня 3 действуют на сетевом уровне и обеспечивают в объединенной сети службу маршрутизации.

Когда в интерфейс маршрутизатора поступает пакет, проверяется IP-адрес назначения. Если пакет не направлен самому маршрутизатору, то это устройство ищет в своей таблице маршрутизации целевой адрес сети назначения. После этого выбирается выходной интерфейс для пакета. После деления на кадры пакет пересылается за пределы локальной сети. Если же в таблице маршрутизации не будет найдена сеть назначения, то маршрутизатор просто отбрасывает (отвергает) пакет.

На сетевом уровне используются пакеты двух типов: данных и обновлений маршрутов (путей).

**Пакеты данных** Используются для пересылки пользовательской информации через объединенную сеть. Применяемые для этого протоколы называются маршрутизируемыми протоколами. Примерами могут служить протоколы IP и IPX (об адресации в сетях IP см. в главе 3, а о IPX — в главе 8).

**Пакеты обновления маршрутов** Служат для уведомления соседних маршрутизаторов о подключенных сетях, известных маршрутизатору объединенной сети. Такие протоколы называются протоколами маршрутизации (например, RIP, EIGRP, OSPF и т.д.). Пакеты обновления маршрутов помогают создавать и поддерживать таблицы маршрутизации во всех маршрутизаторах.

Пример таблицы маршрутизации показан на рис. 1.8.

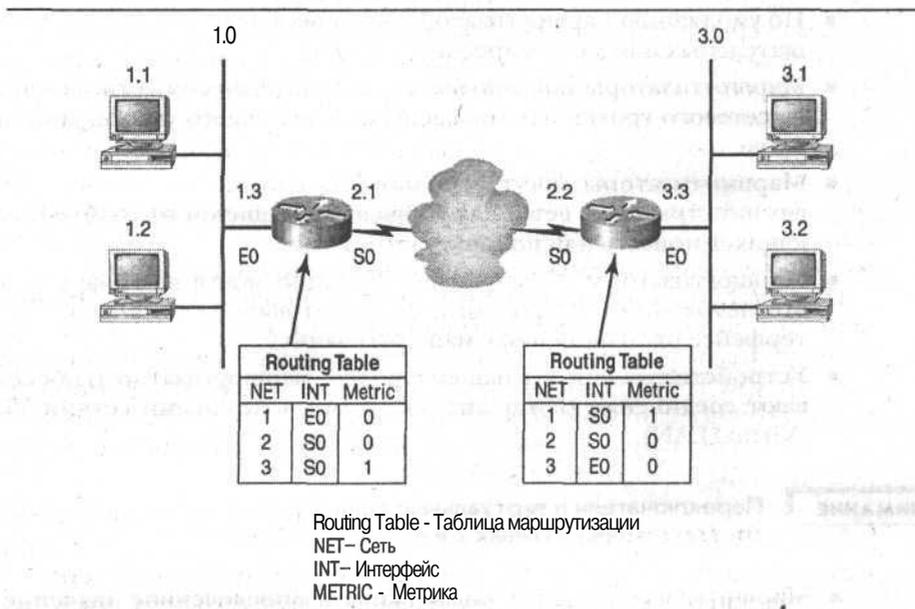


Рис. 1.8. Таблица маршрутизации в маршрутизаторе

В таблице маршрутизации хранится следующая информация:

**Сетевой адрес** Сетевой адрес конкретного протокола. Маршрутизатор обязан поддерживать отдельные таблицы для каждого протокола маршрутизации, поскольку каждый протокол маршрутизатора придерживается собственной схемы адресации. Можно считать эти таблицы дорожными знаками на разных языках, которыми пользуются все участники дорожного движения.

**Интерфейс** Выходной интерфейс для пакета, отправляемого в определенную сеть.

**Метрика** Расстояние до удаленной сети. Разные протоколы маршрутизации пользуются различными методами для вычисления этого расстояния. Протоколы маршрутизации мы обсудим в главе 5. Однако отметим, что некоторые протоколы пользуются счетчиком участков (количеством маршрутизаторов, которые пакет пройдет во время движения к удаленной сети), другие — полосой пропускания, задержкой в линии или счетчиком тиков (1/18 с).

Маршрутизаторы делят сеть на *широковещательные домены*, т.е. по умолчанию широковещательные рассылки не проходят сквозь маршрутизаторы. Кроме того, маршрутизаторы делят сеть на домены коллизий (конфликтов), что реализуется переключателями на уровне 2. Каждый интерфейс маршрутизатора связан с отдельной сетью и имеет уникальный идентификатор этой сети. Все хосты такой сети, к которым подключается маршрутизатор, будут иметь одинаковые сетевые номера.

Несколько характерных особенностей маршрутизаторов:

- По умолчанию маршрутизаторы не пересылают никаких широковещательных или многоадресных пакетов.
- Маршрутизаторы пользуются логическим адресом сети из заголовка сетевого уровня для определения следующего участка при пересылке пакета.
- Маршрутизаторы могут использовать списки доступа, созданные администратором сети, для управления защитой от пакетов, пытающихся попасть или покинуть интерфейс.
- Маршрутизаторы обеспечивают функции моста на уровне 2, если это необходимо. Кроме того, он может выполняться в данном интерфейсе одновременно с маршрутизацией.
- Устройства уровня 3 (в нашем случае — маршрутизаторы) обеспечивают соединения между виртуальными локальными сетями VLAN (Virtual LAN).

**▼ ВНИМАНИЕ**

Переключатели и виртуальные локальные сети VLAN рассмотрены соответственно в главах 2 и 6.

- Маршрутизаторы могут поддерживать определенное значение качества обслуживания QoS (Quality of Service) для отдельных типов сетевого трафика.

## Канальный уровень

*Канальный уровень* (Data Link Layer или уровень связи данных) обеспечивает доставку сообщения на правильное устройство и трансляцию содержимого сообщения с сетевого уровня в биты физического уровня для последующей пересылки по сети. Происходит форматирование сообщения в *кадры данных* и добавление настроенного *заголовка*, содержащего адреса источника и назначения. Эта добавленная информация является своеобразной капсулой, заключающей в себе исходное сообщение также как капсулы спутников вмещают в себя двигатели, навигационное оборудование и другие приборы. Отдельные части капсулы сообщения нужны только на определенных этапах запуска спутника. Аналогично отдельные части капсулы сообщения используются только для определенных этапов перемещения информации в сети. На рис. 1.9 показан канальный уровень по спецификациям Ethernet и ШЕЕ. Заметим, что стандарт IEEE 802.2 используется совместно с другими стандартами IEEE, расширяя их функциональные возможности.

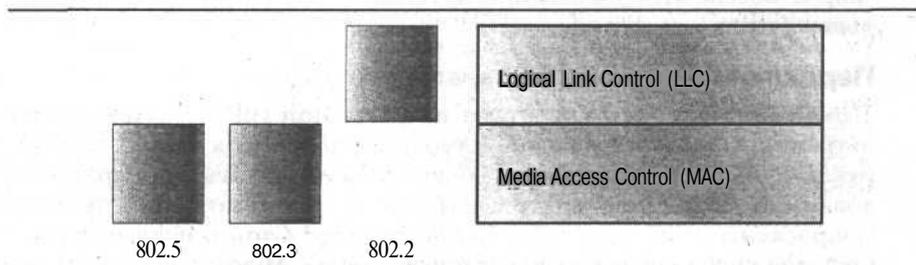


Рис. 1.9. Канальный уровень

Работающий на сетевом уровне маршрутизатор не заботится о достижении конкретного хоста, поскольку должен передать данные только в определенную сеть. Маршрутизатор отслеживает наилучший маршрут достижения этой сети, а уникальная идентификация каждого устройства в локальной сети возложена на канальный уровень.

Для хоста, отправляющего пакеты другим хостам или обеспечивающим пересылку пакетов между маршрутизаторами, канальный уровень использует аппаратную адресацию. Каждый пересылаемый между маршрутизаторами пакет делится на кадры с управляющей информацией для канального уровня. Однако эта информация удаляется на принимающем маршрутизаторе, который оставляет только исходный и неизменный при пересылке пакет. Деление на пакеты выполняется на каждом участке и до достижения целевого хоста. Важно понимать, что пакет никогда не изменяется по пути следования. Сначала выполняется инкапсуляция пакета для добавления дополнительной информации, необходимой в носителях разного типа.

Согласно спецификации IEEE Ethernet, канальный уровень делится на два подуровня:

**Управление доступом к носителю MAC (Media Access Control, 802.3)**

Определяет способ внедрения пакетов в среду передачи (носитель). Коммуникационный носитель предоставляется первому обратившемуся пользователю, причем полоса пропускания носителя используется одновременно несколькими пакетами. В этой же спецификации определена физическая адресация, а также логическая топология. Логической топологией называется путь сигнала в физической топологии. На подуровне управления доступом к носителю установлены правила для линии связи, уведомления об ошибках (но не их коррекции), последовательности доставки кадров, а также необязательные средства управления потоком.

**Управление логическими связями LLC (Logical Link Control, 802.2)** Этот подуровень отвечает за идентификацию протоколов сетевого уровня и выполнение инкапсуляции данных. Заголовок LLC указывает каналному уровню на порядок обработки пакета после получения его кадров. Например, хост получает кадр и анализирует заголовок LLC, чтобы выявить принадлежность пакета протоколу IP сетевого уровня. На подуровне LLC можно обеспечить управление потоком и последовательностью контрольных битов.

**Переключатели и мосты канального уровня**

*Переключатели и мосты* работают на канальном уровне и производят фильтрацию сетевого трафика с помощью аппаратных (MAC) адресов. Переключение (коммутация) на уровне 2 может считаться аппаратно реализованной функцией мостов, поскольку используются специальные микросхемы ASIC (*Application-Specific Integrated Circuits*, интегральные микросхемы специализированного применения). Микросхемы ASIC способны работать с гигабитовыми скоростями и очень малыми задержками.

Переключатели и мосты читают каждый входящий в сеть кадр. Устройства уровня 2 добавляют в таблицу фильтрации аппаратный адрес источника из кадра, чтобы отслеживать порт, который получает данную последовательность кадров. Переключатель должен точно знать о местоположении устройства.

После создания таблицы фильтрации устройством уровня 2, сетевое устройство начинает только пересылать кадры в сегмент сети, где находится аппаратный адрес точки назначения. Если устройство назначения присутствует в том же сегменте, что и кадр, то устройство уровня 2 блокирует распространение этого кадра в другие сегменты сети. Если же точка назначения находится в ином сегменте, то кадр только пересылается в подобный сегмент без какой-либо обработки. Этот процесс называется прозрачным исполнением функции моста (*transparent bridging*, прозрачным мостованием).

Если кадр попадает в интерфейс устройства уровня 2 (переключателя) и в таблице фильтрации неизвестен аппаратный адрес точки назначения, то устройство пересылает кадр во все подключенные сегменты. Если на этот кадр откликнется "неизвестное" переключателю устройство, то переключатель обновит свою таблицу фильтрации, добавив в нее полученные сведения об откликнувшемся устройстве. Адрес назначения

в пересылаемом кадре иногда является адресом широковещательной рассылки. В этом случае переключатель по умолчанию формирует широковещательные рассылки во всех подключенных сегментах.

Все устройства, которые получают широковещательную рассылку, считаются принадлежащими одному широковещательному домену. Устройство уровня 2 распространяет далее шторм широковещательных рассылок далее на уровне 2. Единственным способом устранения такого распространения шторма на все объединенные сети являются устройства уровня 3 (маршрутизаторы).

Основное преимущество переключателей в сравнении с концентраторами состоит в том, что в объединенной сети каждый коммутируемый порт образует собственный домен конфликтов (коллизий), а концентратор объединенной сети формирует один общий домен конфликтов. Заметим, что переключатели и мосты не разделяют на части широковещательные домены, поскольку распространяют все Широковещательные рассылки.

Еще одним достоинством переключателей в локальной сети в сравнении с концентраторами является то, что каждое устройство любого сегмента может осуществлять передачу данных независимо от других устройств. Учтите, что каждый сегмент становится отдельным доменом конфликтов. Концентраторы позволяют в определенный момент времени передавать данные только одному устройству в сети.

Переключатели не могут транслировать данные в носители разного типа, т.е. каждое подключенное к переключателю устройство должно применять одинаковый тип кадров Ethernet. Если нужно подключить переключатель Token Ring или другую локальную сеть, то необходим маршрутизатор.

### **Физический уровень**

*Физический уровень* отвечает за передачу и прием битовых потоков. Биты могут иметь значение 0 или 1 подобно коду Морзе, но с числовыми значениями. Физический уровень взаимодействует с разными типами коммуникационных носителей, что приводит к различному представлению битовых значений. Иногда применяются тональные сигналы, но чаще битовые значения представлены *переходами между состояниями* — изменениями напряжения от низкого к высокому потенциалу или наоборот. Для каждого типа носителя используются специальные протоколы, определяющие используемые битовые шаблоны и метод их кодирования в сигналы носителя, а также различные физические характеристики интерфейса подключения носителя.

Физический уровень специфицирует электрические, механические, процедурные и функциональные характеристики, необходимые в процессе активизации, обслуживания и деактивизации физических соединений между системами.

На физическом уровне определен интерфейс между окончательным оборудованием данных (DTE) и окончательным оборудованием цепей передачи данных (DCE). Если окончательное оборудование цепей передачи данных

размещается у провайдера, то окончательным оборудованием данных являются подключенные устройства пользователей. Доступ к устройствам DTE наиболее часто осуществляется через модем или модуль обслуживания каналов/данных (CSU/DSU).

Соединители (разъемы) и топологии на физическом уровне определены стандартами OSI, что допускает взаимодействие разнородных систем. Для сертификационного экзамена CCNA достаточно знать только о стандартах Ethernet.

### Концентраторы на физическом уровне

*Концентратор* — это многопортовый повторитель. Как повторитель это устройство получает цифровой сигнал и усиливает, либо регенерирует его перед пересылкой во все активные порты устройства, причем не выполняется никакого анализа данных. Точно так же поступает активный концентратор. Любой полученный из сегмента цифровой сигнал передается после усиления или регенерации с входного на все активные выходные порты концентратора. Следовательно, любое подключенное к концентратору устройство находится в одном и том же домене конфликтов, а также в том же самом домене широковещательных рассылок. Домен широковещательных рассылок определяет область сети, где все устройства сегмента "слушают" все подобные рассылки.

Концентратор, как и повторитель, не анализирует сетевой трафик. Он без преобразования пересылает данные в остальные части физического носителя. Концентратор создает топологию физической звезды, поскольку становится центральным устройством, к которому подключаются остальные сетевые устройства сегмента. Однако в сетях Ethernet используется логическая шинная топология, т.е. сигнал распространяется от одного конца сети до другого. Все подключенные к концентратору устройства (или другие концентраторы) должны прослушивать все пересылаемые другими устройствами данные.

## Сети Ethernet

*Ethernet* — это метод доступа к коммуникационному носителю, позволяющий всем хостам сети совместно использовать одну полосу пропускания линии связи. Популярность Ethernet обусловлена простотой реализации, диагностики и добавлением в сетевую инфраструктуру новых технологий (например, FastEthernet и Gigabit Ethernet). Сети Ethernet используют спецификации канального и физического уровней.

В сетях Ethernet используется метод доступа CSMA/CD (*Carrier Sense Multiple Access with Collision Detect*, множественный доступ с контролем несущей и определением конфликтов). Он помогает устройствам совместно использовать полосу пропускания так, что никакие два устройства не могут одновременно осуществлять доступ к сетевому носителю. Метод CSMA/CD создан для решения проблем с конфликтами при доступе к носителю (коллизиями), когда происходит одновременная пересылка пакетов в разные узлы. Важно эффективно управлять конфликтами,

поскольку когда один из узлов в методе CSMA/CD начинает пересылку данных по сети, все остальные узлы обязаны принимать передаваемую информацию и анализировать получаемые данные. Только хосты и маршрутизаторы способны эффективно предотвратить распространение пересылки данных на всю сеть.

Опишем действие метода CSMA/CD. Когда хост собирается передавать данные по сети, он сначала проверяет наличие в линии цифрового сигнала. Если линия "чистая" (не передает данные ни один из хостов), то хост начинает пересылку данных. После этого хост уже не должен останавливаться. Передающий хост постоянно проверяет состояние линии, чтобы гарантировать отсутствие передачи данных другими хостами. Если хост замечает в линии сигнал от другого хоста, то первый хост посылает сигнал "помеха" (jam), который приводит к остановке передачи данных всеми хостами в сегменте. Сетевые узлы реагируют на сигнал "помеха" тем, что выжидают некоторое время перед следующей попыткой начала пересылки данных. Алгоритм отката после сигнала "помеха" предписывает время начала повторной пересылки данных для всех станций в сегменте конфликта. Если окажутся неудачными 15 попыток выхода из конфликта между станциями, узел регистрирует состояние тайм-аута (time-out).

## Дуплексная и полудуплексная сеть Ethernet

Полудуплексная сеть Ethernet определена в исходном стандарте 802.3 Ethernet, где предписано использование только одной пары проводников для пересылки цифровых сигналов в обоих направлениях. В таких сетях используется метод CSMA/CD для предотвращения конфликтов и выполнения повторных пересылок информации при обнаружении конфликта. Если концентратор подключен к переключателю, то он должен работать в полудуплексном режиме, поскольку оконечная станция не способна выявить конфликт доступа к носителю. Полудуплексная Ethernet (обычно ЮBaseТ) эффективна на 50 — 60 % (по крайней мере, согласно исследованиям компании Cisco). Однако в больших сетях ЮBaseТ обычно удается получить только 3 — 4 Мбит/с.

Дуплексная (полнодуплексная) сеть Ethernet использует две пары проводников вместо одной пары в полудуплексных сетях. В дуплексном режиме применяется соединение "точка-точка" между передающим и принимающим устройствами. Не возникает конфликтов, поскольку мы получаем несколько путей пересылки данных вместо одного пути в полудуплексном режиме. Дуплексная Ethernet обеспечивает 100 % эффективности в обоих направлениях, т.е. мы можем достичь скорости 20 Мбит/с в Ethernet, работающей на скорости 10 Мбит/с или 200 Мбит/с в Fast-Ethernet. Эта скорость называется композитной (aggregate rate), но она характеризует только намерение получить 100 % эффективность, хотя это и не всегда удается.

После подачи питания на порт дуплексной Ethernet, он соединяется с оконечным портом и согласовывает с ним связь по протоколу Fast-Ethernet. Этот процесс называется механизмом автоопределения (auto-detect mechanism). Такой механизм предполагает предварительное

согласование уровня обмена, т.е. выбор режима 10 или 100 Мбит/с. Затем проверяется возможность работы в дуплексном режиме. Если это неприемлемо для одного из портов, то обмен осуществляется в полудуплексном режиме.

## Ethernet на канальном уровне

Ethernet на канальном уровне отвечает за адресацию в рамках протоколов Ethernet, что обычно связано с аппаратными адресами (MAC-адресами). Кроме того, Ethernet ответственна за разделение на кадры пакетов, полученных от сетевого уровня, и за подготовку кадров к пересылке по локальной сети с помощью определенного в стандарте Ethernet метода доступа к носителю. Существуют четыре типа кадров Ethernet:

- Ethernet\_II
- IEEE 802.3
  - IEEE 802.2
- SNAP

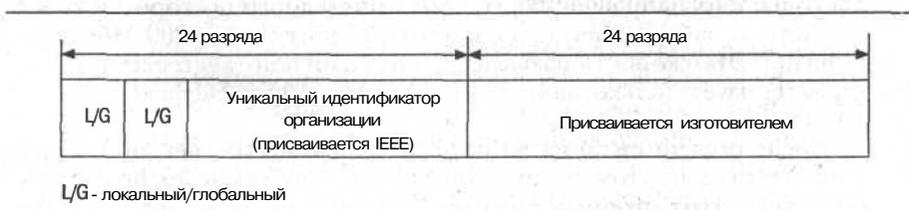
Эти типы мы рассмотрим ниже.

## Адресация Ethernet

Адресация Ethernet использует MAC-адреса (*Media Access Control*, управленые доступом к носителю), которые "прошиты" в каждой плате сетевого адаптера NIC (*Network Interface Card* – карта сетевого интерфейса) для сети Ethernet. MAC-адрес часто называют аппаратным. Он состоит из 48 разрядов и имеет канонический формат, гарантирующий, по крайней мере, одинаковый формат записи адресов для всех известных технологий локальных сетей.

На рис. 1.10 показан 48-разрядный MAC-адрес и его поля.

Уникальный идентификатор организации OUI (*Organizationally Unique Identifier*) присваивается институтом IEEE каждой компании-производителю (24 разряда или 3 байта). В свою очередь, организация присваивает глобально администрируемый адрес (*globally administered address*), который имеет длину 24 разряда (3 байта) и является уникальным (предположительно) для всех и каждого сетевого адаптера данной компании-производителя. Разряд 46 должен иметь значение 0 для глобального присвоения производителем и значение 1 при локальном управлении адресами сетевым администратором.



**Рис. 1.10.** Адресация в Ethernet на основе MAC-адресов

## Кадры Ethernet

Канальный уровень отвечает за объединение битов в байты, а байтов в *кадры* (frame). Кадры используются на канальном уровне для инкапсуляции пакетов, пришедших с сетевого уровня, и последующей пересылки пакетов по носителю. Существуют три вида носителей (точнее методов доступа к носителю): с соревнованием (Ethernet), передачи маркера (Token Ring и FDDI) и голосования (большие ЭВМ компании IBM и 100VGAnyLAN). Для экзамена CCNA нужно знать основной носитель Ethernet (с соревнованием).

Станция сети Ethernet пересылает кадры данных другой станции с помощью группы битов, называемых форматом кадра MAC. Это обеспечивает выявление ошибок с помощью циклической избыточной проверки CRC (cyclic redundancy check). Однако выполняется только выявление ошибок, но не их коррекция. Кадры 802.3 и Ethernet показаны на рис. 1.11.

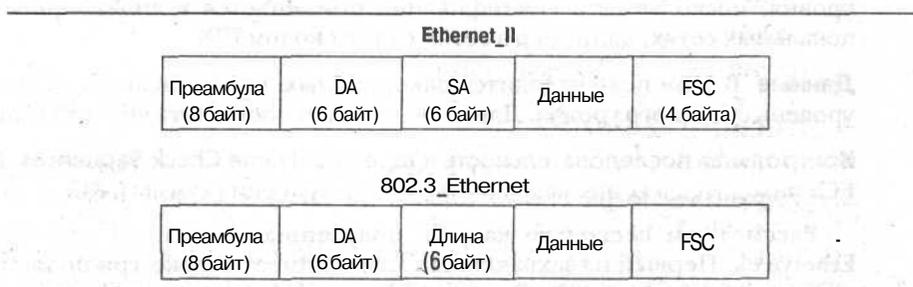


Рис. 1.11. Форматы кадров 802.3 и Ethernet

В представленном ниже списке перечислены поля для кадров типа 802.3 и Ethernet.

**Преамбула (Preamble)** Чередующийся шаблон нулей и единиц обеспечивает частоту 5 МГц в начале каждого пакета. Это позволяет принимающим устройствам настроиться на следующий далее битовый поток. В преамбуле применяется поле SFD или синхронизации (synch) для указания принимающей станции на начало секции данных в сообщении.

**SFD (Start Frame Delimiter, разделитель начала кадра)/Synch** SFD состоит из 1,0,1,0,1,0 и т.д., а поле синхронизации (synch) — из всех единиц. Поле преамбулы вместе с полем SFD/synch занимают 64 разряда.

**Адрес назначения DA (Destination Address)** В этом поле располагается 48-разрядное значение, записанное методом "первым LSB" (Least Significant Bit, наименее значимый бит). Поле DA нужно принимающей станции для определения, послан ли следующий далее пакет данному узлу. Адрес назначения может быть индивидуальным, многоадресным или широковещательным MAC-адресом. При широковещательной рассылке в поле адреса назначения установлены все единицы (все F

в шестнадцатеричном виде), что определяет заданные устройства. Однако многоадресная рассылка поступает только отдельному подмножеству узлов сети.

#### Т ВНИМАНИЕ

Шестнадцатеричная система счисления использует кроме 10 цифр первые шесть букв английского алфавита (от А до F). Поэтому один шестнадцатеричный разряд позволяет записать одну из 16 цифр.

**Адрес источника SA (Source Address)** Поле SA хранит 48-разрядный MAC-адрес, предоставленный передающим устройством. Адрес записан методом "первым LSB". Широковещательные и многоадресные рассылки не могут быть записаны в поле SA.

**Поля длины или типа** В 802.3 используется поле длины, но в кадрах Ethernet находится поле типа, определяющее протокол сетевого уровня. В спецификации 802.3 не допускается идентификация протокола верхнего уровня, поскольку эта спецификация применяется в лицензированных локальных сетях, например в сетях с протоколом IPX.

**Данные** В этом поле находится пакет данных, поступивший в канальный уровень с сетевого уровня. Длина поля может составлять 46 - 1500 байт.

**Контрольная последовательность кадра FCS (Frame Check Sequence)** Поле FCS находится в конце кадра и служит для хранения суммы CRC.

Рассмотрим несколько кадров, полученных в сетевом анализаторе Etherpeek. Первый из захваченных кадров имеет только три поля: назначения, источника и типа. Это кадр Ethernet\_II. Заметим, что в поле типа указан протокол IP (08-00 в шестнадцатеричном виде).

```
Destination: 00:60:f5:00:ff:27
Source: 00:60:f5:00:ff:2c
Protocol Type: 08-00 IP
```

Следующий кадр имеет те же самые поля, поэтому является кадром Ethernet\_II. Мы показали данный кадр, чтобы продемонстрировать иное содержимое поля типа протокола: IPX (81-37h). Заметим, что это кадр широковещательной рассылки, поскольку адрес назначения состоит из одних единиц (или всех F в шестнадцатеричном виде).

```
Destination: ff:ff:ff:ff:ff:ff Ethernet Broadcast
 (широковещательная рассылка Ethernet)
Source: 02:07:01:22:de:a4
Protocol Type: 81-37 (OC NetWare)
```

Обратите внимание на поле длины в следующем кадре. Мы видим, что это кадр 802.3. Какой протокол используется на сетевом уровне? Протокол не указан в кадре, но это будет IPX, поскольку компания Novell создала кадры типа 802.3 (еще до того, как это сделал институт IEEE,

тоже назывались "сырыми" — 802.3 Raw) исключительно для собственных серверов локальных сетей. Следовательно, это IPX.

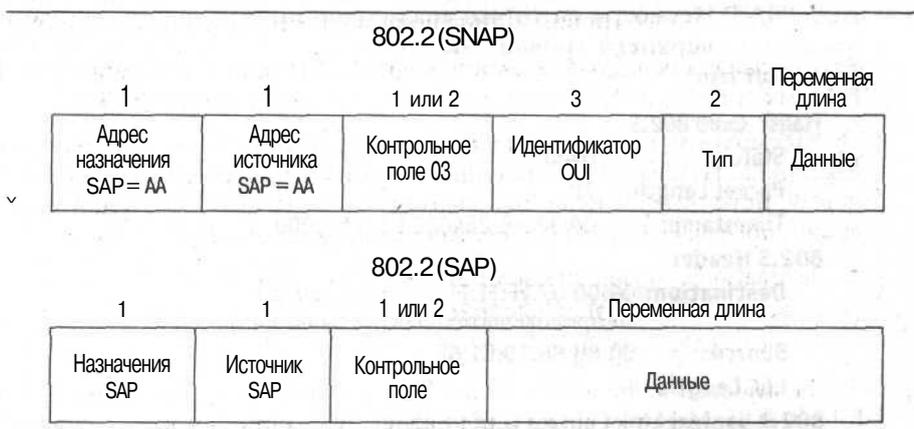
```

Flags: 0x80802.3
Status: 0x00
Packet Length: 64
Timestamp: 12:45:45.192000 06/26/1998
Destination: ff:ff:ff:ff:ff:ff Ethernet Broadcast
 (широковещательная рассылка Ethernet)
Source: 08:00:11:07:57:28
Length: 34

```

## 802.2 и SNAP

Кадры 802.3 Ethernet не могут самостоятельно указать протокол верхнего (сетевого) уровня — нужна дополнительная информация, которая (а также дополнительные данные) определена в стандарте 802.2 LLC института IEEE. На рис. 1.12 показан кадр IEEE 802.3 с LLC (802.2) и тип кадра SNAP Subnetwork Architecture Protocol (протокол архитектуры подсетей).



**Рис. 1.12.** 802.2 и SNAP

Согласно рис. 1.12, информация заголовка LLC добавляется в секцию данных.

Рассмотрим кадры 802.2 и SNAP, собранные анализатором.

### Кадр 802.2

Ниже показаны примеры кадров 802.2 после захвата анализатором протоколов. Первый кадр имеет поле длины, возможно, — это кадр 802.3? Однако он же имеет поля DSAP (назначение SAP) и SSAP (источник SAP), следовательно, это кадр 802.2 (вспомним, что кадр 802.2 — это кадр 802.3 с информацией LLC в поле данных заголовка, где отмечен использованный протокол верхнего уровня):

```

Flags: 0x80 802.3
Status: 0x02 Truncated (обрезан)
Packet Length:64
Slice Length: 51
Timestamp: 12:42:00.592000 03/26/1998
Destination: ff:ff:ff:ff:ff:ff Ethernet Broadcast
 (широковещательная рассылка Ethernet)
Source: 00:80:c7:a8:f0:3d
LLC Length: 37
Dest. SAP: 0xe0 NetWare
Source SAP: 0xe0 NetWare Individual LLC Sublayer Management Function
 (неправильная функция управления подуровня LLC)
Command: 0x03 Unnumbered Information
 (нумерованная информация)

```

### Кадр SNAP

Кадр SNAP имеет собственное поле для идентификации протокола верхнего уровня. За счет этого кадр Ethernet\_II может использоваться как кадр 802.3. Несмотря на то что анализатор протоколов показывает поле протокола верхнего уровня, мы имеем дело с полем типа Ethernet\_II (простой тип).

```

Flags: 0x80802.3
Status: 0x00
Packet Length: 78
Timestamp: 09:32:48.264000 01/04/2000

```

#### 802.3 Header

```

Destination: 09:00:07:FF:FF:FF AT Ph 2 Broadcast
 (широковещательная рассылка на уровне 2)
Source: 00:00:86:10:C1:6F
LLC Length: 60

```

#### 802.2 Logical Link Control (LLC) Header

(заголовок логического управления связью)

```

Dest. SAP: 0xAA SNAP
Source SAP: 0xAA SNAP
Command: 0x03 Unnumbered Information
 (нумерованная информация)
Protocol: 0x080007809B AppieTalk

```

Был определен кадр SNAP, поскольку поля DSAP и SSAP имеют значение AA, а в поле команды находится 3. Причина создания кадра этого типа в том, что не все протоколы способны работать с кадрами 802.3 Ethernet. Некоторые из них не имеют поля простого типа (ether-type). Для использования разработчиками приложений лицензированных протоколов в кадре LLC институт IEEE ввел формат SNAP. Формат используется не слишком часто и обычно только для AppieTalk и кадров с

лицензированным форматом. Cisco пользуется кадрами SNAP для собственного лицензированного CDP (Cisco Discovery Protocol — протокол обнаружения Cisco), который рассмотрен в главе 7.

## Ethernet на физическом уровне

В среде Ethernet с совместно используемыми концентраторами начало передачи данных одной станцией предполагает синхронизацию всех устройств на передаваемый цифровой сигнал и формат пересылаемого по линии кадра. Все устройства используют один физический носитель и прослушивают кадры в пределах одного домена конфликтов. В любой момент времени передачу может осуществлять только одно устройство. Все остальные устройства сетевого сегмента должны синхронизироваться по пересылаемому сигналу и кадру. Если одновременно два устройства начинают передачу, то возникает конфликт (коллизия). В 1984 году комитет IEEE Ethernet утвердил протокол (метод) Carrier Sense Multiple Access with Collision Detect (CSMA/CD). Этот протокол в основном предписывает режим прослушивания линии всем остальным устройствам, чтобы выявить начало передачи данных и остановить в случае конфликта собственную процедуру передачи с ожиданием следующей попытки в течение предписанного времени.

В Ethernet используется шинная топология, т.е. передача данных одним устройством предполагает распространение сигнала от одного конца сегмента до другого. Кроме того, в Ethernet определена технология передачи в основной полосе частот (baseband technology), т.е. во время передачи данных станция использует всю доступную полосу пропускания линии и не предполагает ее разделение с другими устройствами. Существуют следующие исходные стандарты IEEE 802.3:

**10Base2** Скорость передачи 10 Мбит/с, технология передачи в основной полосе частот, длина линии до 185 метров. Другое название — тонкая Ethernet (thinnet). В одном сегменте поддерживается до 30 рабочих станций.

**10Base5** Скорость передачи 10 Мбит/с, технология передачи в основной полосе частот, длина линии до 500 метров. Другое название — толстая Ethernet (thicknet).

**10BaseT** Скорость передачи 10 Мбит/с по витым парам категории 3. В отличие от сетей 10Base2 и 10Base5, каждое устройство подключается к концентратору или к переключателю, а в одном сегменте или линии может быть только один хост.

Во всех стандартах 802.3 определен интерфейс подключения элемента AUI (Attachment Unit Interface), что позволяет побитовую пересылку данных на физическом уровне с помощью метода доступа, определенно-го на канальном уровне. MAC-адреса остаются неизменными, но на физическом уровне можно поддерживать любую существующую или новую технологию. Исходный интерфейс AUI определяет 15-контактный

соединитель, что позволяет приемо-передатчику (transceiver, transmitter/receiver) обеспечить соединение между 15-контактным разъемом и витыми парами. Интерфейс AUI встроен в приемо-передатчик, а в качестве соединителей используются разъемы RJ-45.

Интерфейс AUI не поддерживает 100 Мбит/с Ethernet, поскольку необходима высокая частота передачи данных. Для 100BaseT требуется новый интерфейс, который определен в спецификации 802.3u, — интерфейс независимого носителя МП (Media Independent Interface). Он обеспечивает пропускную способность 100 Мбит/с. Интерфейс МП определяет **нибблы** (nibble), т.е. группы из четырех битов. В Gigabit Ethernet применяется интерфейс независимого гигабитного носителя GMI (Gigabit Media Independent Interface), где осуществляется одновременная передача 8 бит.

## Инкапсуляция данных

Когда хост пересылает данные по сети на другое устройство, данные *инкапсулируются* внутри информации о протоколе каждого уровня модели OSI. Каждый уровень способен взаимодействовать только с равным себе уровнем на принимающем устройстве.

Информация взаимодействия и обмена на каждом уровне называется элементом данных протокола PDU (*Protocol Data Unit*). Внутри этого элемента находится управляющая информация, которая подключена к данным каждого уровня модели. Обычно подключение происходит через добавление заголовка к полям данных. Однако может использоваться концевой элемент (trailer), находящийся после полей данных.

Каждый элемент PDU во время инкапсуляции подключается к данным на любом уровне модели OSI. Каждый PDU имеет специальное имя, зависящее от размещенной в заголовке информации. Она читается только соответствующим уровнем принимающего устройства, а затем удаляется при передаче данных на следующий верхний уровень.

На рис. 1.13 показаны элементы PDU и способ подключения управляющей информации для каждого уровня.

На рисунке видно, что при передаче информации с верхних уровней для пересылки по сети происходит преобразование данных. Поток данных доходит до транспортного уровня, где формируются виртуальные цепи за счет пересылки пакета синхронизации. Затем поток данных делится на небольшие части. Создаются заголовки транспортного уровня (элементы PDU этого уровня) для формирования сегментов. Управляющая информация подключается в виде заголовка к полям данных. Каждый сегмент нумеруется, чтобы воссоздать поток данных на принимающем устройстве.

Каждый сегмент обрабатывается на сетевом уровне для формирования сетевых адресов и маршрутизации по объединенной сети. Логическая адресация (например, IP) служит для направления сегмента в нужную сеть. Протоколы сетевого уровня добавляют управляющий заголовок к сегменту и передают сегмент на транспортный уровень. Там



Рис. 1.13. Инкапсуляция данных

формируются пакеты или датаграммы. Вспомним, что транспортный и сетевой уровни работают совместно, чтобы восстановить поток данных на принимающем хосте. Однако эти уровни не несут ответственности за помещение своих элементов PDU для направления в локальный сетевой сегмент, что является прерогативой маршрутизаторов и хостов.

На канальном уровне пакеты принимаются от сетевого уровня и перемещаются в сетевой носитель (кабель или линию беспроводной связи). Канальный уровень инкапсулирует каждый пакет в кадр, причем в заголовке кадра переносится информация об аппаратном адресе источника и хоста назначения. Если *устройство* находится в удаленной сети, то кадр направляется в маршрутизатор для доставки по объединенной сети. Когда кадр попадает в сеть назначения, для отправки кадра нужному хосту используется новый кадр.

Перед перемещением кадра по сети, его следует преобразовать в цифровой сигнал. Поскольку кадр реально состоит из логически связанной группы единиц и нулей, физический уровень выполняет инкапсуляцию этих значений в цифровые сигналы, которые могут быть прочитаны другими сетевыми устройствами той же самой локальной сети. Принимающее устройство выполнит синхронизацию по цифровому сигналу и извлечет из него точные значения единиц и нулей. После этого принимающее устройство воссоздает кадр, запускает проверку избыточной контрольной суммы (CRC), а затем сверяет полученное значение с содержимым поля FCS в заданном кадре. Если значения совпадают, из кадров формируется пакет, а сами они удаляются. Этот процесс называется деинкапсуляцией (de-encapsulation). Далее пакет обрабатывается сетевым уровнем, где проверяется адрес. Если адрес совпадает с адресом принимающего устройства, то из пакетов формируется сегмент, а

пакеты удаляются. Сегмент обрабатывается на транспортном уровне, где воссоздается лоток данных и формируется подтверждение успешного приема каждой части сегмента для передающей станции. Затем поток данных отправляется приложению верхнего уровня.

На передающем устройстве инкапсуляция выполняется так:

1. Информация пользователя преобразуется в данные для передачи по сети.
2. Данные преобразуются в сегменты, устанавливается надежное соединение между передающим и принимающим хостами.
3. Сегменты преобразуются в пакеты или датаграммы, а в заголовок каждого пакета вставляется логический адрес, чтобы пакеты можно было переслать по объединенной сети.
4. Пакеты или датаграммы разбиваются на кадры для пересылки по локальной сети. Аппаратный адрес (адрес Ethernet) позволяет уникально идентифицировать хост в сегменте локальной сети.
5. Кадры преобразуются в поток битов с использованием цифрового кодирования и схемы внедрения тактовой частоты.

## Трехуровневая иерархическая модель компании Cisco

Понятие "иерархии" напоминает отношение в семье (по крайней мере, те, кто имел старшего брата или сестру, считали себя находящимися в самом низу иерархии). Иерархическая структура помогает распределить объекты по уровням, указать связи между объектами и функции этих объектов. *Иерархия* позволяет упорядочить сложную модель, а в семейных отношениях присвоить каждому члену определенную роль.

Иерархия используется и в проектировании сетей. Следует распределить все сетевые объекты по иерархическим уровням, согласно выполняемым объектами функциям. Как и в остальных случаях, анализ одного из иерархических уровней сети позволяет не учитывать функции других уровней.

Современные крупные сети очень сложны, поскольку определяются множеством протоколов, конфигурациями и технологиями. С помощью иерархии можно упорядочить все компоненты в легко анализируемой модели. Причем, модель будет диктовать характеристики каждого иерархического уровня.

Иерархическая модель Cisco помогает в разработке, внедрении и обслуживании масштабируемых, надежных и эффективных в стоимостном выражении объединенных сетей. Компания Cisco определила три иерархических уровня (см. рис 1.14), на каждом из которых выполняются специфические сетевые функции.

В модели определены три уровня:

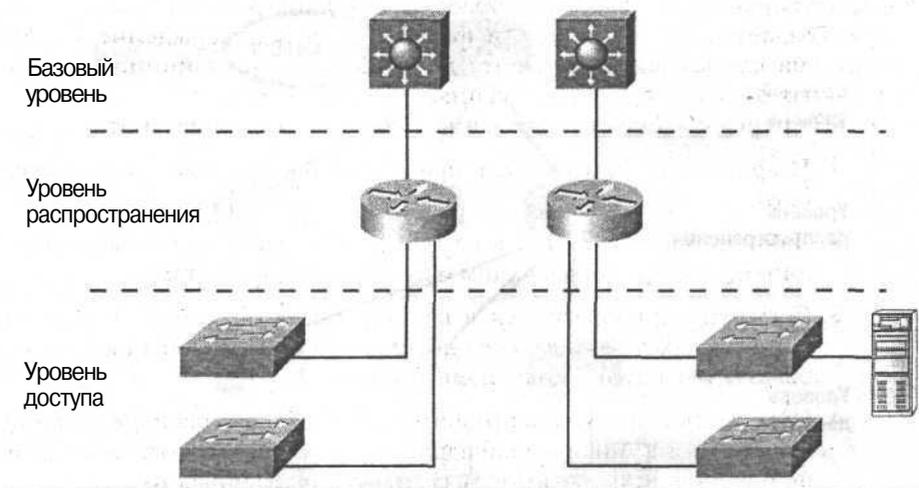


РИС. 1.14. Иерархическая модель Cisco

- Базовый уровень (Core layer)
- Уровень распространения (Distribution layer)
- Уровень доступа (Access layer)

Каждый уровень отвечает за реализацию определенных функций. Однако эти уровни являются логическими и не обязательно согласованы с физическими устройствами. В другой иерархической модели — OSI — тоже используются логические уровни иерархии. Семь таких уровней описывают функции. Однако определенный протокол не обязательно соответствует функциям. Иногда протокол отображается на несколько уровней модели OSI, а в других случаях одному уровню соответствует несколько протоколов. Аналогично, при построении физической реализации иерархической сети несколько устройств могут попасть на один уровень, либо одно устройство будет выполнять функции нескольких уровней. Следовательно, уровни являются логическими, но не физическими понятиями.

Рассмотрим типичный иерархический проект сети (см. рис. 1.15). Концепция "сохранить локальным локальный трафик" давно стала общим местом сетевых проектов, хотя и не всегда подкрепляется на концептуальном уровне. Однако иерархия подтверждает предложенную аксиому.

Рассмотрим подробнее каждый уровень иерархической модели.

## Базовый уровень

Базовый уровень формирует ядро сети. На самом верху иерархии этот уровень отвечает за быструю и надежную пересылку больших объемов трафика. Единственным предназначением базового уровня является быстрая коммутация трафика. Трафик передается на базовом уровне

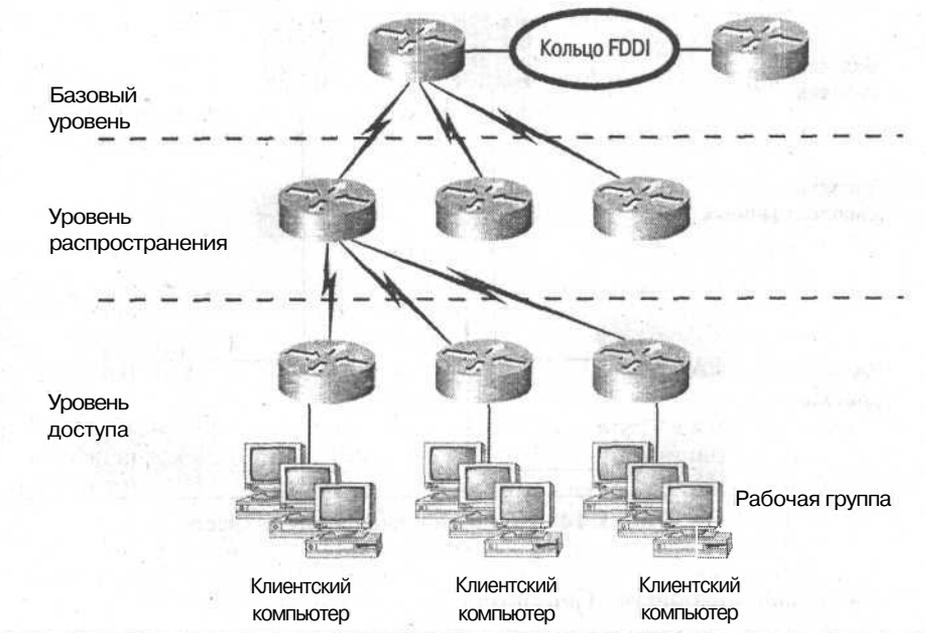


Рис. 1.15. Иерархический проект сети

совместно для нескольких пользователей. Однако на уровне распределения обрабатываются пользовательские данные, что может привести к дополнительным запросам в базовый уровень.

Если происходит ошибка на базовом уровне, то она *влияет на всех пользователей*. Следовательно, весьма важно обеспечить высокую надежность на базовом уровне. На этом уровне обрабатываются большие объемы трафика, поэтому не менее важно учитывать скорость и задержки. Отметим функции базового уровня, перейдем к особенностям его реализации:

- Ничто не должно замедлять трафик, в том числе списки доступа, маршрутизация между виртуальными локальными сетями **VLAN** и фильтрация пакетов.
- Не следует реализовывать функции доступа для рабочей группы.
- Исключите расширение базового уровня при росте размеров объединенной сети (например, при добавлении маршрутизаторов). Если на базовом уровне возникают проблемы с производительностью, лучше выбрать модернизацию, а не расширение.

Несколько рекомендаций по проектированию сети на базовом уровне:

- Обеспечьте высокую надежность. Рекомендуется применять технологии канального уровня для обеспечения скорости и избыточности (например, использовать **FDDI**, **Fast Ethernet** с избыточными связями и даже **ATM**).

- Учитывайте скорость. На базовом уровне необходима минимальная задержка.
- Выберите протокол маршрутизации с малым временем конвергенции. Быстрые и избыточные подключения на канальном уровне ничем не помогут при некорректных таблицах маршрутизации!

## Уровень распространения

*Уровень распространения* иногда называют уровнем рабочих групп. Он расположен между базовым уровнем и уровнем доступа. Основные функции уровня распространения состоят в маршрутизации, фильтрации и доступе к региональным сетям, а также (если необходимо) в определении правил доступа пакетов к базовому уровню. Уровень распространения обязан устанавливать наиболее быстрый способ обработки запросов к службам (например, метод файлового обращения к серверу). После определения на уровне распространения наилучшего пути доступа, запрос может быть передан на базовый уровень, где реализован скоростной транспорт запроса к нужной службе.

На уровне распространения устанавливается политика сети, а также обеспечиваются возможности гибкого описания сетевых операций. На уровне распространения выполняется несколько функций:

- Реализация инструментов, подобных спискам доступа, фильтрации пакетов или механизму запросов.
- Реализация системы безопасности и сетевых политик, включая трансляцию адресов и установку брандмауэров.
- Перераспределение между протоколами маршрутизации, включая использование статических путей.
- Маршрутизация между сетями VLAN и другие функции поддержки рабочих групп.
- Определение доменов широковещательных и многоадресных рассылок.

На уровне распределения не следует выполнять те функции, которые свойственны двум другим уровням.

## Уровень доступа

На *уровне доступа* реализовано управление пользователями и рабочими группами при обращении к ресурсам объединенной сети. Иногда уровень доступа называют уровнем настольных систем. Наибольшая часть необходимых пользователям сетевых ресурсов должна быть доступна локально. На уровне распределения выполняется перенаправление трафика к удаленным службам. Для уровня доступа характерны следующие функции:

- Постоянный контроль (из уровня распределения) за доступом и политиками
- Формирование независимых доменов конфликтов (сегментация)
- Соединение рабочих групп с уровнем распределения

Обычно на уровне доступа применяются технологии DDR или коммутация Ethernet. Здесь же можно увидеть статическую маршрутизацию (вместо протоколов динамической маршрутизации).

Как уже отмечено выше, три отдельных уровня не связаны с тремя специальными типами маршрутизаторов. Этим устройствам может быть меньше или больше, но нужно всегда помнить о разделении сетевых функций по уровням модели.

## Кабели и подключение устройств Cisco

В этом разделе книги рассматривается корпоративная сетевая среда с точки зрения необходимых для объединенной сети типов кабелей. Чтобы классифицировать кабели по типам и правильно выбрать их для устройств Cisco, следует разобраться с реализацией физического уровня в локальных сетях Ethernet.

Ethernet — это метод доступа к носителю, который специфицирован на канальном уровне, но на физическом уровне определяются требования к кабелям и сигналам. Важно понимать отличия между разными соединителями, которые объединяют устройства в сеть Ethernet. Обсудим разные типы кабелей "витая пара", используемые в современных локальных сетях Ethernet.

### Кабели Ethernet для локальных сетей

Ethernet была первоначально реализована группой компаний DIX (Digital, Intel и Xerox). Эта группа разработала первую спецификацию Ethernet для локальных сетей, которая впоследствии использовалась комитетом IEEE 802.3. Такая сеть имела скорость обмена 10 Мбит/с по коаксиальному или волоконно-оптическому кабелю, либо по кабелю "витая пара".

Институт IEEE расширил комитет 802.3 за счет организации двух новых подкомитетов: 802.3u (FastEthernet) и 802.3z (Gigabit Ethernet). В подкомитетах были разработаны спецификации для "витой пары" и волоконно-оптического носителя. На рис 1.16 показана спецификация IEEE 802.3 для первоначальной реализации физического уровня Ethernet.

Во время разработки локальной сети нужно знать о доступных носителях Ethernet. Конечно же, неплохо иметь Gigabit Ethernet на каждом настольном ПК и 10 Гбит/с между переключателями, но сегодня это не

|                                    |          |         |         |         |         |          |           |           |
|------------------------------------|----------|---------|---------|---------|---------|----------|-----------|-----------|
| Канальный уровень<br>(MAC-уровень) | Ethernet | 802.3   |         |         |         |          |           |           |
| Физический уровень                 |          | 10Base3 | 10Base5 | 10BaseT | 10BaseF | 10BaseTX | 100BaseFX | 100BaseT4 |

Рис. 1.16. Физический уровень Ethernet

выгодно с экономической точки зрения. Совместное использование и согласование разных носителей Ethernet позволит создать производительную, но экономичную современную сеть.

Ниже перечислены рекомендации по использованию различных носителей Ethernet в иерархических сетях:

- Применяйте переключатели 10 Мбит/с на уровне доступа для обеспечения хорошей производительности при небольших затратах. Связи 100 Мбит нужны для клиентов и серверов с широкой полосой пропускания. По возможности, серверы не должны работать на скорости 10 Мбит/с.
- Применяйте FastEthernet между переключателями на уровнях доступа и распределения. Связи 10 Мбит/с станут "узкими местами".
- Применяйте FastEthernet (или Gigabit) между переключателями на уровнях распределения и базовом уровне. Кроме того, между переключателями базового уровня следует использовать наиболее быстрый носитель. Двойные связи между переключателями на уровнях распределения и базовом рекомендуются для балансировки нагрузки и резервирования.

## Требования к носителям и соединителям Ethernet

Важно различать возможные скорости разных носителей Ethernet. Однако нужно учитывать и требования к соединителям (разъемам) до того, как утвердить проект сети.

Организация EIA/TIA (Electronic Industries Association и более новая Telecommunications Industry Association) выработала стандарты физического уровня для Ethernet. Спецификация EIA/TIA предписывает для Ethernet соединитель RJ (*registered jack* - *зарегистрированный соединитель*) с раскладкой по контактам 4 5 и *неэкранированной витой парой* (UTP) — RJ-45. Ниже перечислены требования к разным носителям Ethernet:

**10Base2** 50-омный коаксиальный кабель (тонкая Ethernet). До 185 метров и до 30 хостов в сегменте. Используется физическая и логическая шинная топология с соединителями AUI.

**10Base5** 50-омный коаксиальный кабель (толстая Ethernet). До 500 метров и до 208 хостов в сегменте. Используется физическая и логическая шинная топология с соединителями AUI. До 2500 метров с повторителями и до 1024 пользователями во всех сегментах.

**10BaseT** Кабели категорий 3, 4 или 5 по спецификации EIA/TIA с двумя неэкранированными витыми парами UTP (*unshielded twisted-pair*). Один пользователь в сегменте длиной до 100 метров. Используются соединители RJ-45 при физической топологии "звезда" и логической шинной топологии.

**100BaseTX** Кабели UTP категорий 5, 6 или 7 по спецификации EIA/TIA с двумя неэкранированными витыми парами. Один пользователь в сегменте длиной до 100 метров. Используются соединители RJ-45 МП при физической топологии "звезда" и логической шинной топологии.

**100BaseFX** Волоконно-оптический одномодовый кабель 62.5/125 мкм. Технология "точка-точка" при длине сегмента до 400 метров. Используются соединители ST или SC (дуплексное подключение интерфейса носителя).

**1000BaseCX** Медные экранированные витые пары длиной не более 25 метров.

**1000BaseT** Категория 5, четыре пары UTP, длина до 100 метров.

**1000BaseSX** Волоконно-оптический кабель MMF с диаметром ядра 62.5 и 50 мкм. Используется лазер 780 нм при длине до 260 метров.

**1000BaseLX** Одномодовое волокно с ядром 9 мкм, лазер 1300 нм, длина от 3 до 10 км.

**У ВНИМАНИЕ**

Сети 100VG-AnyLAN строятся на витых парах, причем это были первые локальные сети со скоростью 100 Мбит/с. Однако они несовместимы с Ethernet по сигналам (используется метод доступа к носителю с голосованием), поэтому мало распространены и постепенно отмирают.

## Соединитель UTP (RJ-45)

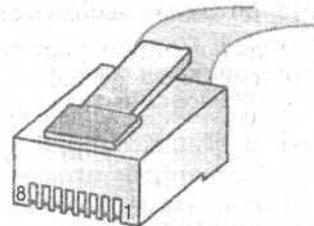
Соединитель RJ-45 позволяет увидеть состоящее из 8 цветов кодирование проводников, подключенных к контактам разъема. Используются четыре витые пары. Четыре линии (две пары) служат для передачи напряжения, поэтому называются *рабочими* (tip). Оставшиеся четыре проводника заземлены и называются *кольцевыми* (ring). Соединитель RJ-45 обжимается на концах проводников, причем контакты разъема пронумерованы слева направо от 8 до 1.

На рис. 1.17 показан кабель UTP с установленным соединителем RJ-45.

Кабель UTP имеет внутри витые пары, позволяющие устранить перекрестные наводки. Применяется неэкранированный кабель, поскольку

| Контакт | Витая пара |
|---------|------------|
| 1       | Pair 2 T2  |
| 2       | Pair 2 R2  |
| 3       | Pair 3 T3  |
| 4       | Pair 1 R1  |
| 5       | Pair 1 T1  |
| 6       | Pair 3 R3  |
| 7       | Pair 4 T4  |
| 8       | Pair 4 R4  |

T - рабочая линия  
R - кольцевая



Соединитель RJ-45

**Рис. 1.17.** Кабель UTP с разъемом RJ-45

цифровой сигнал защищен от помех скруткой витых пар. Чем больше количество скруток на дюйм, тем ниже уровень интерференции сигналов. Например, кабели категорий 5 и 6 имеют больше скруток на дюйм по сравнению с кабелем UTP категории 3.

Для построения объединенных сетей используются разные типы кабелей: прямые (straight-through) и перекрестные (crossover).

### Прямой кабель

Прямой кабель UTP предполагает одинаковое расположение линий на обоих концах. На рис. 1.18 показано распределение по контактам для такого кабеля.



Рис. 1.18. Прямой кабель UTP

Проще всего определить прямой кабель за счет совмещения друг с другом обоих его разъемов. В этом случае легко установить идентичность распределения линий по контактам.

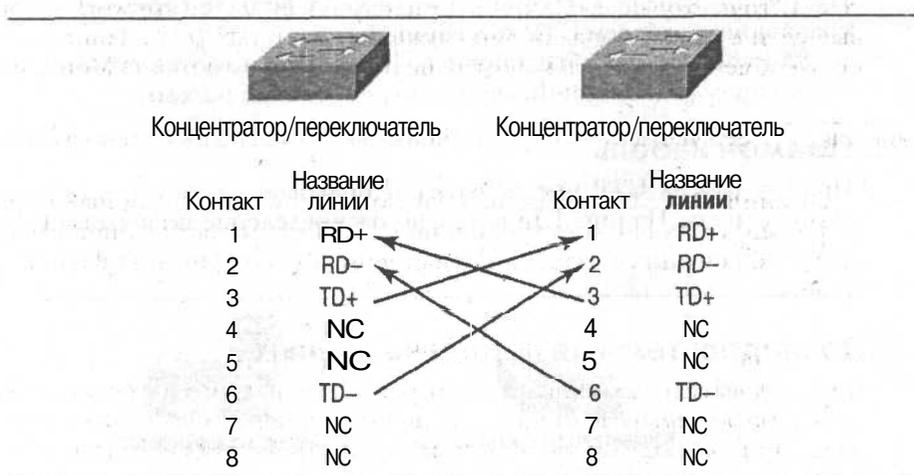
Прямой кабель используется для:

- Подключения маршрутизатора к концентратору или переключателю
- Подключения сервера к концентратору или переключателю
- Подключения рабочей станции к концентратору или переключателю

### Перекрестный кабель

В перекрестном кабеле линии "перехлестнуты" на разных концах этого кабеля. На каждой из сторон линия Transmit (передача) должна соединяться с Receive (прием), а Receive с Transmit, причем как для рабочих, так и для кольцевых проводников. На рис. 1.19 показан перекрестный кабель UTP.

Контакт 1 на одной стороне соединен с контактом 3 на другой стороне кабеля, а контакт 2 соединен с контактом 6.



**Рис. 1.19.** Перекрестный кабель UTP

Перекрестный кабель используется для:

- Подключения по исходящим (каскадным) связям (uplink) между переключателями
- Подключения концентратора к переключателю
- Подключения концентратора к другому концентратору
- Подключения интерфейса маршрутизатора к интерфейсу другого маршрутизатора
- Соединения двух ПК без использования концентратора или переключателя

**ВНИМАНИЕ** | Чтобы определить нужный для данного порта кабель, следует посмотреть на маркировку порта. Если только один из соединяемых портов имеет маркировку "X", используйте прямой кабель. Если оба порта имеют эту маркировку, то вам необходим перекрестный кабель.

## Кабели региональных сетей

Для соединения двух *региональных сетей* (WAN, wide area network) нужно знать о реализации физического уровня этих сетей в устройствах Cisco, а также характеристики последовательного соединения разных сетей WAN. В этом разделе рассматриваются требования к кабелям для соединений ISDN BRI.

Последовательные соединения Cisco поддерживают службы региональных сетей любого типа. Типичным являются выделенная линия

связи уровня HDLC (High-Level Data Link Control — высокоуровневое управление связью данных), протокол PPP (Point-to-Point Protocol — протокол "точка-точка"), ISDN (Integrated Services Digital Network — цифровые сети с интегрированными службами) и Frame Relay. Типичные скорости обмена находятся в диапазоне от 2400 бит/с до 1.544 Мбит/с (T1).

**т ВНИМАНИЕ** ( Все упомянутые типы региональных сетей рассмотрены в главе 10.

Линии HDLC, PPP и Frame Relay могут использовать одинаковые спецификации физического уровня, но в ISDN применяется иное распределение по контактам разъема и собственная спецификация физического уровня.

### Последовательная передача данных

В последовательных линиях связи региональных сетей используется *последовательная передача данных*, т.е. побитовая пересылка в сигнальном канале. При *параллельной передаче* можно одновременно переслать не менее 8 бит, но все региональные сети применяют только последовательную передачу.

Маршрутизаторы Cisco оснащены лицензированным 60-контактным последовательным соединителем, который можно приобрести в компании Cisco или у ее дистрибьюторов. Тип соединителя определяется характеристиками другого конца связи и используемым провайдером услуг кабелем, либо требованиями к конечному устройству. Существуют следующие типы соединителей: EIA/TIA-232, EIA/TIA-449, V.35 (для подключения к CSU/DSU), X.21 (применяется для связи с сетями X.25) и EIA-530.

Последовательные связи характеризуются частотой или циклами в секунду (герцами). Количество передаваемых на этой частоте данных называется *полосой пропускания* (bandwidth). Она определяет количество данных в битах в секунду (бит/с), пересылаемых по последовательному каналу связи.

### Терминальное оборудование данных

Интерфейсом маршрутизатора по умолчанию является DTE (*Data Terminal Equipment* — терминальное оборудование данных), причем интерфейс подключается к DCE (*Data Communication Equipment* — оборудование коммуникации данных), например, к CSU/DSU (*Channel Service Unit/Data Service Unit* — блок службы канала/блок службы данных). Затем CSU/DSU подключается к разделительной точке (demarc, demarcation location), которую обслуживает поставщик услуг (провайдер). Обычно разделительной точкой является розетка соединителя RJ-45, находящаяся вблизи оборудования. Провайдеры в ответ на нарекания к своей работе предлагают проверить соединение с разделительной точкой. Проблема может быть связана с оборудованием CPE (Customer Premise Equipment — оборудование в помещении потребителя), которое обслуживает не провайдер, а его клиент.

Основная идея региональных сетей состоит в соединении двух сетей DTE по сети DCE. К сети DCE относится устройство CSU/DSU, кабели и коммутаторы провайдера, а также все линии связи до устройства CSU/DSU на другом конце соединения. Сетевое устройство DCE обеспечивает тактовую частоту для подключенного к нему интерфейса DTE (т.е. последовательного интерфейса маршрутизатора).

### Фиксированные и модульные интерфейсы

Некоторые маршрутизаторы Cisco имеют фиксированные интерфейсы, но другие устройства — модульные интерфейсы. В маршрутизаторе с фиксированными интерфейсами (например, серии 2500) доступные интерфейсы нельзя изменить. Например, маршрутизатор 2501 имеет два последовательных соединителя и один интерфейс AUI типа 10BaseT. Если потребуется добавить третий последовательный интерфейс, замените весь маршрутизатор! Однако в моделях 1600, 1700, 2600, 3600 и других маршрутизаторах высокого класса применяются модульные интерфейсы, поэтому можно приобрести и установить интерфейс практически любого типа. В моделях 1600 и 1700 возможности модульной замены ограничены, поскольку используются как фиксированные, так и модульные порты, но в серии 2600 и выше доступны многочисленные последовательные интерфейсы, FastEthernet и даже голосовые модули.

### Соединения ISDN

В сети *ISDN (Integrated Services Digital Network)* с интерфейсом *BRI (Basic Rate Interface)* — интерфейс базового уровня) используются два канала *B (Bearer — несущие)* по 64 к каждый и один канал *V (Data, данных)* с емкостью 16 к для сигналов и тактовой частоты.

Маршрутизаторы *ISDN BRI* поставляются с интерфейсом *U* или интерфейсом *S/T*. Интерфейс *U* уже подготовлен для двухпроводного подключения *ISDN* и может быть сразу соединен с абонентским отводом *ISDN*. Интерфейс *S/T* предполагает использование четырехпроводного соединения, поэтому необходимо оконечное сетевое устройство *Network Termination type 1 (NT 1)* для преобразования четырехпроводного подключения в стандартную двухпроводную связь по спецификации *ISDN*.

▼ **ВНИМАНИЕ** | Сети *ISDN* рассмотрены в главе 10.

В интерфейсе *U* присутствует встроенное устройство *NT 1*. Если провайдер применяет устройство *NT 1*, то придется приобрести маршрутизатор с интерфейсом *S/T*. В большей части маршрутизаторов Cisco с интерфейсами *BRI* порты маркированы *U* или *S/T*.

Для интерфейса *ISDN BRI* необходимы соединители *RJ-45* и прямой кабель категории 5. Очень важно исключить соединение с этим интерфейсом консольного кабеля или кабеля локальной сети, поскольку может выйти из строя порт маршрутизатора. Компания Cisco утверждает о *непременном* выходе из строя, но известны случаи еженедельного неправильного подключения без каких-либо последствий.

**▼ ВНИМАНИЕ** [ Интерфейс PRI (Primary Rate Interface – интерфейс основного уровня) обеспечивает скорость линии T1 (1.544 Мбит/с) для США и скорость линии E1 (2.048) для Европы. В этой книге мы больше не будем обсуждать интерфейс PRI.

### Консольное соединение

Все устройства Cisco поставляются с консольными кабелями и соединителями, обеспечивающими подключение к устройству для настройки, проверки и мониторинга. Этот же кабель может использоваться для соединения двух ПК, поскольку является перекрестным кабелем с разъемами RJ-45.

Распределение по контактам для перекрестного консольного кабеля:

1-8

2-7

3-6

4-5

5-4

6-3

7-2

8-1

Можно сделать такой кабель из прямого кабеля RJ-45: отрежьте разъем на одной стороне, перекрутите кабель и подключите новый разъем.

Обычно для подключения к ПК применяются соединители DB9 и используется последовательный порт (com port) для взаимодействия с устройством из программы HyperTerminal. Многие устройства Cisco теперь поддерживают консольные подключения с разъемами RJ-45, но в переключателях модели Catalyst 5000 необходим соединитель DB25.

Установите программу эмуляции терминала для работы на скорости 9600 бит/с, при 8 битах данных, без проверки четности (no parity), с одним стоповым битом и без управления потоком (no flow control). В некоторых маршрутизаторах необходимо проверить в программе эмуляции терминала переход в режим непрограммируемого терминала (dumb-terminal) VT100, чтобы устранить режим автоопределения, который не сработает.

Многие маршрутизаторы имеют вспомогательный порт (aux port, auxiliary port) для подключения к модему. Можно набрать на модеме телефонный номер и подключиться к маршрутизатору через порт aux. Это откроет консольный доступ к удаленному маршрутизатору. Однако он может быть выключен, поэтому не удастся установить соединение по Telnet. Консольный и вспомогательный порты служат для управления вне основной частоты (out-of-band management), поскольку настройка маршрутизатора происходит "не по сети". Протокол Telnet считается протоколом основной частоты (in-band).

## Выбор устройств Cisco

Трехуровневая модель Cisco позволяет выбрать тип продукта для объединенной сети. Понимание действующих на каждом уровне служб и выполняемые в объединенной сети функции помогают точно определить необходимый для данных условий продукт компании Cisco. Для выбора устройства Cisco согласно требованиям конкретной сети следует собрать информацию о всех устройствах, которые будут работать в иерархии объединенной сети. Кроме того, рекомендуется рассмотреть требования к установке, портам и другим возможностям устройства.

Если предстоит связать удаленный офис или использовать региональную сеть в иных целях, необходимо выяснить тип доступной службы. В сетевом проекте не будет проку от сведений, что в крупной сети Frame Relay этот протокол поддерживается только половиной из удаленных подразделений компании. Как только будут выявлены возможности и требования провайдера, можно переходить к выбору устройства Cisco, соответствующего установленным бизнес-требованиям.

Обычно доступных вариантов не слишком много: коммутируемое асинхронное соединение, выделенная линия на 1.544 Мбит/с, Frame Relay или ISDN (перечислены наиболее популярные технологии региональных сетей). Распространяются технологии xDSL, обеспечивающие быстрые, надежные и недорогие связи по региональным сетям. Следует оценить все доступные варианты до приобретения и развертывания устройств. Например, если пользователи удаленного офиса подключаются к центральному офису компании на время более трех-четырех часов в день, то потребуются выделенная линия или Frame Relay. Если подключения нерегулярны, будет достаточно ISDN или коммутируемых соединений.

## Концентраторы Cisco

Компания Cisco выпускает широкий спектр концентраторов для различных областей применения.

Перед покупкой любого концентратора нужно выяснить, для какой совместно используемой сети он предназначен: 10 или 100 Мбит/с. Недорогие модели Cisco поддерживают только скорость 10 Мбит/с, но в моделях среднего и высшего класса допускается автоопределение и работа на скоростях 10 и 100 Мбит/с. Высококачественные устройства имеют порт сетевого управления и консольный разъем. Если у вас хватает средств на покупку качественного концентратора, то можно прикупить переключатель. На рис. 1.20 показан спектр выпускаемых Cisco концентраторов. Любой из них поддерживает каскадное подключение для увеличения количества портов.

При выборе конкретного устройства следует учитывать:

- Бизнес-требования (10 или 100 Мбит/с)
- Плотность портов
- Возможности управления устройством
- Простоту обслуживания

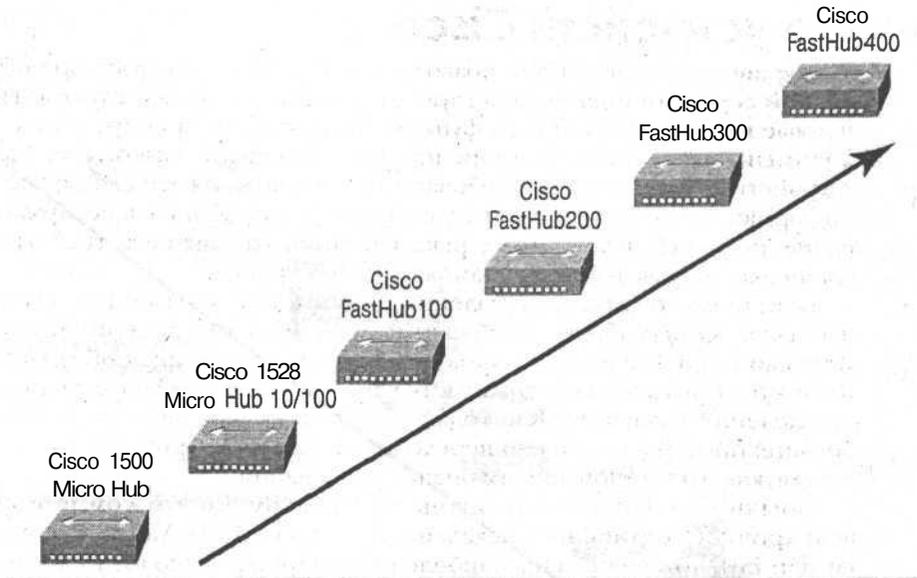


Рис. 1.20. Концентраторы Cisco

## Маршрутизаторы Cisco

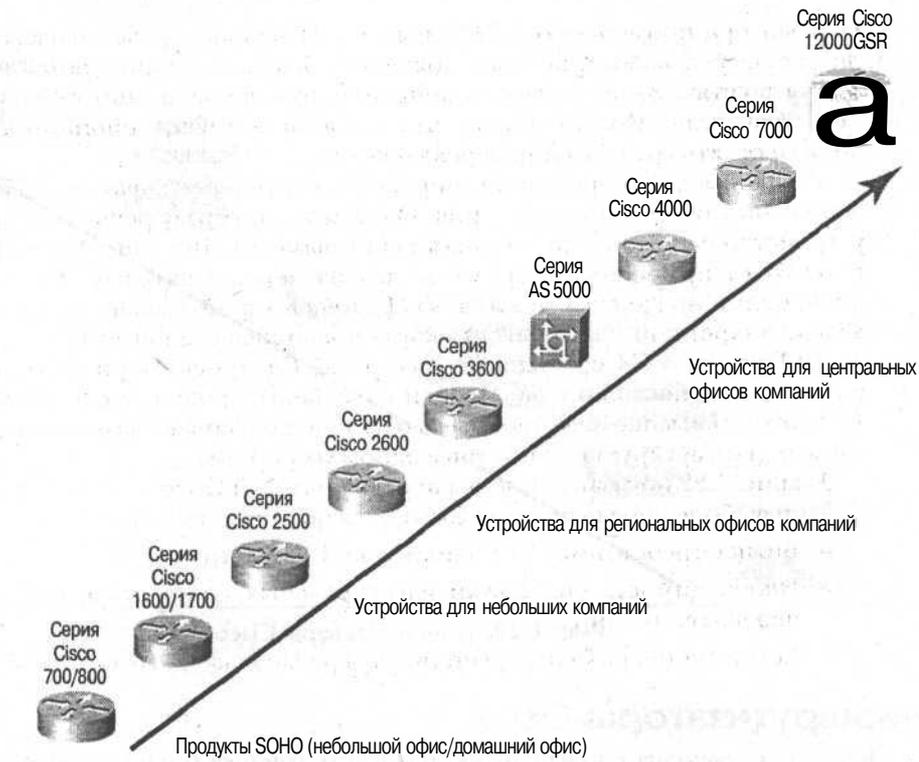
Когда речь заходит о Cisco, то, скорее всего, говорят о маршрутизаторах. Компания Cisco производит лучшие маршрутизаторы в мире. Об этом знают все.

Кажется, что Cisco ежемесячно выпускает новую модель маршрутизатора и сложно отследить все новые предложения компании. Основным критерием выбора устройства должно быть соответствие возможностей маршрутизатора бизнес-требованиям. Например, необходима поддержка IP, Frame Relay и виртуальных частных сетей (VPN), либо IPX, AppleTalk и DECnet. В любом случае можно подобрать продукт компании Cisco.

К другим характеристикам можно отнести плотность (количество) портов (port density) и скорость интерфейса. Чем выше класс устройства, тем выше плотность и скорость. Например, новые модели серии 12000 являются первыми гигабитными переключателями Cisco с прекрасными характеристиками и возможностями.

Стоимость продуктов соответствует номеру модели. Младшая модель серии переключателей 12000 не имеет карт расширения и встроенного блока питания, но стоит примерно от \$12 тыс. Диапазон цен для этой серии заканчивается на отметке \$100 тыс. для загружаемых систем. Следовательно, устройства серии 12000 не подойдут для небольших сетей.

При покупке маршрутизатора следует подумать о поддержке региональных сетей. Компания Cisco предоставляет для этого любое необходимое оборудование, но предварительно нужно выяснить технические требования у местного провайдера региональной сети.



**Рис. 1.21.** Маршрутизаторы Cisco

На рис. 1.21 показаны некоторые маршрутизаторы Cisco.

Серия Cisco 800 по большей части уже заменена серией Cisco 700, поскольку в серии 700 нельзя было запускать операционную систему Cisco IOS. Надо ожидать, что Cisco вскоре полностью откажется от производства маршрутизаторов серии 700, поскольку их трудно настраивать и обслуживать.

При выборе маршрутизатора Cisco следует учитывать:

- Область действия маршрутизации
- Плотность портов и другие технические характеристики
- Емкость устройства и его производительность
- Применяемый пользовательский интерфейс

## Переключатели Cisco

Кажется, что цены переключателей снижаются ежедневно. Из недавнего заявления компании Cisco стало известно, что цена переключателей серии Catalyst 2900 снижена на 30%. Еще четыре года назад 12-портовая карта 10/100 для переключателя Catalyst 5000 стоила \$15 тыс. Сегодня можно купить все устройство Catalyst 5000 с картами 10/100 и модулем

супервизора примерно за \$7500 и менее. Наверное, цены переключателей стали реальными, поэтому появилось больше причин для их применения в сетях. Зачем покупать концентратор, когда можно приобрести переключатель? Можно сказать, что в любом коммуникационном шкафу должен стоять хотя бы один переключатель.

Компания Cisco предлагает широкий спектр переключателей для всевозможных областей применения. Однако нужно сразу решить, будет ли устройство работать с настольными системами 10/100 или 1000 Мбит/с, либо будет применяться для связи других переключателей. Возможно, необходима поддержка режима АТМ (asynchronous transfer mode — режим асинхронной передачи), но когда появились Gigabit Ethernet и связи 10 Гбит/с, АТМ применяется все реже. Следующий критерий выбора — это плотность портов. Модели начального уровня имеют не менее 12 портов, а высококачественные модели поддерживают сотни переключаемых (коммутируемых) портов в одном устройстве.

На рис. 1.22 показана линейка переключателей Cisco.

При выборе переключателя Cisco должны учитываться:

- Бизнес-требования (10,100 или даже 1000 Мбит/с)
- Необходимость поддержки магистральных линий и связей между переключателями
- Сегментация рабочих групп (виртуальные локальные сети VLAN)

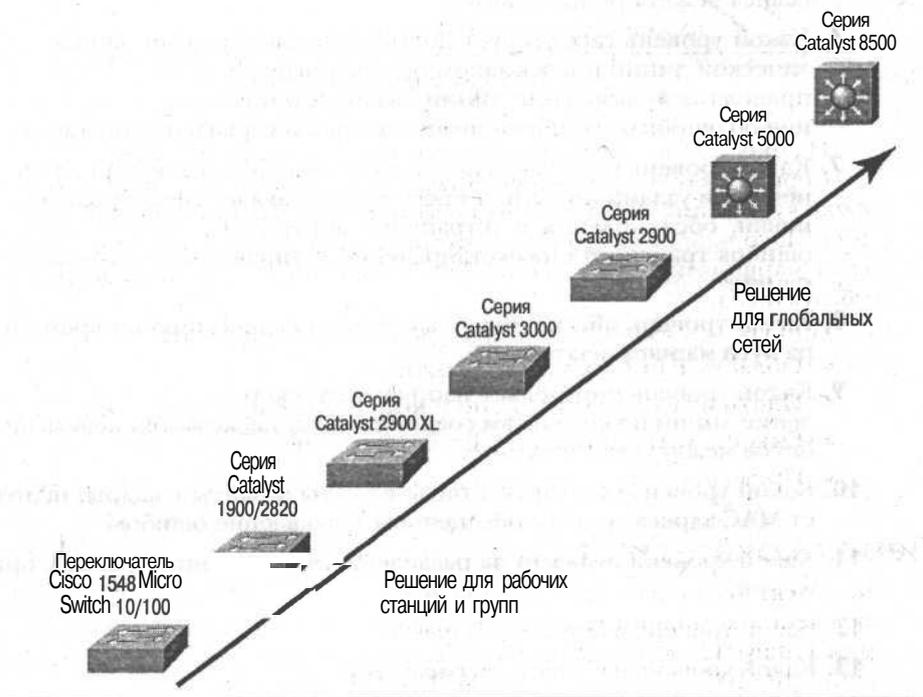


Рис. 1.22. Переключатели Cisco Catalyst

- Требуемая плотность портов
- Возможности пользовательского интерфейса

## Упражнения

### О Упражнение 1.1. Модель OS/

Ответьте на следующие вопросы о модели OSI:

1. Какой уровень выбирает и определяет коммуникационного партнера, а также ресурсы, необходимые для создания соединения; координирует работы взаимодействующих приложений; формирует согласование процедур управления целостностью данных вместе с коррекцией ошибок?
2. Какой уровень отвечает за преобразование пакетов данных канального уровня в электрические сигналы?
3. На каком уровне реализована маршрутизация, разрешение соединений и выбор пути между конечными системами?
4. Какой уровень определяет способы форматирования данных, их предварительную подготовку, кодирование и преобразование для передачи по сети?
5. Какой уровень отвечает за создание, обслуживание и прекращение сеанса между приложениями?
6. Какой уровень гарантирует достоверность передачи данных по физической линии и в основном обеспечивает физическую адресацию, правила использования линии связи, сетевую топологию, уведомление об ошибках, упорядочивание кадров и управление потоком?
7. Какой уровень используется для надежной коммуникации между конечными узлами по сети, а также предоставляет механизмы для установки, обслуживания и устранения виртуальных цепей; выявление ошибок транспорта и восстановление; и управление потоком информации?
8. Какой уровень обеспечивает логическую адресацию во время выбора пути маршрутизаторами?
9. Какой уровень определяет напряжения, скорость линии и распределение линий по контактам соединителя, а также метод перемещения битов между устройствами?
10. Какой уровень объединяет биты в байты и байты в кадры, использует MAC-адреса, а также обеспечивает выявление ошибок?
11. Какой уровень отвечает за разделение в сети данных разных приложений?
12. Какой уровень работает с кадрами?
13. Какой уровень работает с сегментами?
14. Какой уровень работает с пакетами?

15. Какой уровень работает с битами?

16. Расположите в правильном порядке элементы инкапсуляции:

- пакеты
- кадры
- биты
- сегменты

17. Расположите в правильном порядке элементы деинкапсуляции:

- пакеты
- кадры
- биты
- сегменты

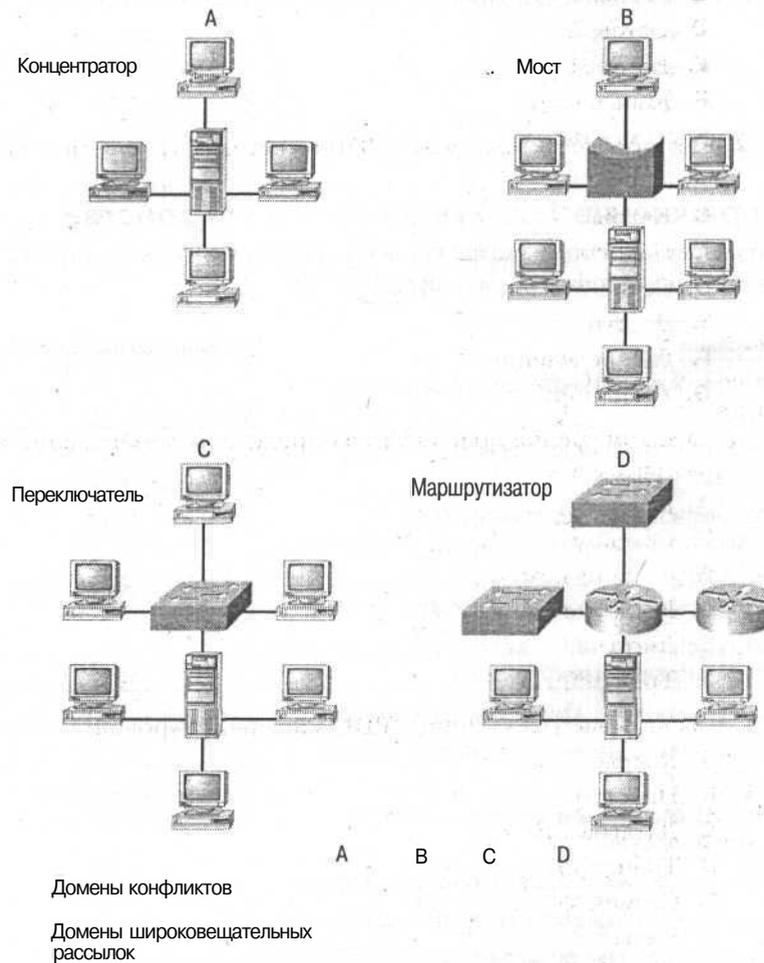
## О Упражнение 1.2. Уровни OS/ и устройства

Заполните таблицу, указав уровень модели OSI или устройство (концентратор, переключатель, маршрутизатор).

| Описание                                                                                                                      | Устройство или уровень OSI |
|-------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| На этом уровне используются логические номера портов.                                                                         |                            |
| Это устройство посылает и принимает информацию о сетевом уровне.                                                              |                            |
| Подобный уровень создает виртуальные цепи до начала передачи данных между двумя оконечными станциями.                         |                            |
| Этот уровень использует точки доступа к службам.                                                                              |                            |
| Данное устройство использует аппаратную адресацию для фильтрации сетевого трафика.                                            |                            |
| На этом уровне специфицирована сеть Ethernet.                                                                                 |                            |
| Этот уровень поддерживает управление потоком и нумерацию.                                                                     |                            |
| Такое устройство может измерять расстояние до удаленной сети.                                                                 |                            |
| На этом уровне используется логическая адресация.                                                                             |                            |
| На этом уровне определена аппаратная адресация.                                                                               |                            |
| Заданное устройство формирует один большой домен конфликтов и один большой домен широковещательных рассылок.                  |                            |
| Это устройство создает много маленьких доменов конфликтов, но сеть остается одним большим доменом широковещательных рассылок. |                            |
| Подобное устройство разделяет домены конфликтов и домены широковещательных рассылок.                                          |                            |

### О Упражнение 1.3. Выявление доменов конфликтов и доменов широковещательных рассылок

Подсчитайте на рис. 1.23 количество доменов конфликтов и доменов широковещательных рассылок в каждой из показанных сетей.



**Рис. 1.23.** Выявление доменов конфликтов и доменов широковещательных рассылок

## Проверочные вопросы

---

1. Какой уровень модели Cisco отвечает за разделение доменов конфликтов?
  - A. Физический
  - B. Доступа
  - C. Базовый
  - D. Сетевой
  - E. Распределения
  - F. Канальный
2. Как называются элементы PDU на сетевом уровне модели OSI?
  - A. Ядро
  - B. Кадры
  - C. Пакеты
  - D. Сегменты
  - E. Доступ
  - F. Распределение
  - G. Транспорт
3. На каком уровне модели Cisco определены домены широковещательных рассылок?
  - A. Базовом
  - B. Сетевом
  - C. Физическом
  - D. Распределения
  - E. Доступа
  - F. Транспортном
4. Как называются элементы PDU канального уровня?
  - A. Кадры
  - B. Пакеты
  - C. Датаграммы
  - D. Транспорт
  - E. Сегменты
  - F. Биты
5. На каком уровне модели OSI выполняется сегментация потока данных?
  - A. Физический
  - B. Канальный
  - C. Сетевой
  - D. Транспортный

- Е. Распределения
  - Ф. Доступа
6. В каких случаях нужно использовать перекрестный кабель?
    - А. Каскадное соединение переключателей
    - В. Соединение маршрутизатора с переключателем
    - С. Соединение концентратора с концентратором
    - Д. Соединение концентратора с переключателем
  7. Что использует канальный уровень для поиска хоста в локальной сети?
    - А. Логическую сетевую адресацию
    - В. Номера портов
    - С. Аппаратные адреса
    - Д. Шлюз по умолчанию
  8. Каков перекрестный кабель?
    - А. Контакты 1–8 полностью противоположны контактам на другом конце.
    - В. Контакты 1–8 полностью идентичны на обоих концах.
    - С. Контакт 1 соединен с контактом 3 на другом конце кабеля, а контакт 2 — с контактом 6.
    - Д. Контакт 2 соединен с контактом 3 на другом конце кабеля, а контакт 1 — с контактом 6.
  9. На каком уровне OSI определены маршрутизаторы?
    - А. Физическом
    - В. Транспортном
    - С. Канальном
    - Д. Сетевом
  10. На каком уровне OSI единицы и нули преобразуются в цифровые сигналы?
    - А. Физическом
    - В. Транспортном
    - С. Канальном
    - Д. Сетевом
  11. На каком уровне OSI определены мосты?
    - А. Физическом
    - В. Транспортном
    - С. Канальном
    - Д. Сетевом
  12. На каком уровне модели Cisco реализована сегментация для устранения сетевых конфликтов?

- A.** Доступа
  - B.** Физическом
  - C.** Сетевом
  - D.** Распределения
  - E.** Базовом
  - F.** Транспортном
  - G.** Канальном
13. Что используется на транспортном уровне для предотвращения переполнения буфера принимающего хоста?
- A.** Сегментация
  - B.** Пакеты
  - C.** Подтверждение
  - D.** Управление потоком
  - E.** PDU
14. Какой уровень модели OSI обеспечивает преобразование данных?
- A.** Приложений
  - B.** Представления
  - C.** Сеансов
  - D.** Транспортный
  - E.** Канальный
15. Какие функции выполняет маршрутизатор? Выберите все подходящие.
- A.** Разделение на домены конфликтов
  - B.** Разделение на домены широковещательных рассылок
  - C.** Логическую сетевую адресацию
  - D.** Фильтрацию физических адресов в локальной сети
16. На каком уровне модели Cisco обычно используются маршрутизаторы?
- A.** Доступа
  - B.** Базовом
  - C.** Сетевом
  - D.** Канальном
  - E.** Распределения
17. Сколько разрядов определено в аппаратном адресе?
- A.** 6
  - B.** 16
  - C.** 46
  - D.** 48

18. Что из перечисленного не является преимуществом модели уровней?
- A. Деление сложных сетевых операций на понятные и управляемые уровни
  - B. Изменение на одном уровне не затрагивает остальные уровни
  - C. Изменение во всех уровнях без учета одного из них
  - D. Определение стандартного интерфейса "plug-and-play" для интеграции с продуктами разных производителей
19. В каких трех спецификациях предположено использование медных кабелей с витыми парами?
- A. 100BaseFX
  - B. 100BaseTX
  - C. 100VG-AnyLAN
  - D. 10BaseT
  - E. 100BaseSX
20. Что означает "Base" в названии 10BaseT?
- A. Магистральная связь, одновременно использующая в одном проводнике несколько цифровых сигналов.
  - B. Магистральная связь, одновременно передающая только один цифровой сигнал.

## Ответы к упражнениям

---

### О Ответы к упражнению 1.1

- 1. Уровень приложений
- 2. Физический уровень
- 3. Сетевой уровень
- 4. Уровень представлений
- 5. Уровень сеансов
- 6. Канальный уровень
- 7. Транспортный уровень
- 8. Сетевой уровень
- 9. Физический уровень
- 10. Канальный уровень
- 11. Уровень сеансов
- 12. Канальный уровень
- 13. Транспортный уровень

14. Сетевой уровень  
 15. Физический уровень  
 16. Сегменты, пакеты, кадры, биты  
 17. Биты, кадры, пакеты, сегменты

### О Ответы к упражнению 1.2

| Описание                                                                                                                       | Устройство или уровень OSI       |
|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| На этом уровне используются логические номера портов.                                                                          | Транспортный уровень             |
| Это устройство посылает и принимает информацию о сетевом уровне.                                                               | Маршрутизатор                    |
| Подобный уровень создает виртуальные цепи до начала передачи данных между двумя оконечными станциями.                          | Транспортный уровень             |
| Этот уровень использует точки доступа к службам.                                                                               | Подуровень LLC канального уровня |
| Данное устройство использует аппаратную адресацию для фильтрации сетевого трафика.                                             | Мост или переключатель           |
| На этом уровне специфицирована сеть Ethernet.                                                                                  | Канальный и физический уровни    |
| Этот уровень поддерживает управление потоком и нумерацию.                                                                      | Транспортный уровень             |
| Такое устройство может измерять расстояние до удаленной сети.                                                                  | Маршрутизатор                    |
| На этом уровне используется логическая адресация.                                                                              | Сетевой уровень                  |
| На этом уровне определена аппаратная адресация.                                                                                | Подуровень MAC канального уровня |
| Заданное устройство формирует один большой домен конфликтов и один большой домен ширококвещательных рассылок.                  | Концентратор                     |
| Это устройство создает много маленьких доменов конфликтов, но сеть остается одним большим доменом ширококвещательных рассылок. | Переключатель или мост           |
| Подобное устройство разделяет домены конфликтов и домены ширококвещательных рассылок.                                          | Маршрутизатор                    |

### О Ответы к упражнению 1.3

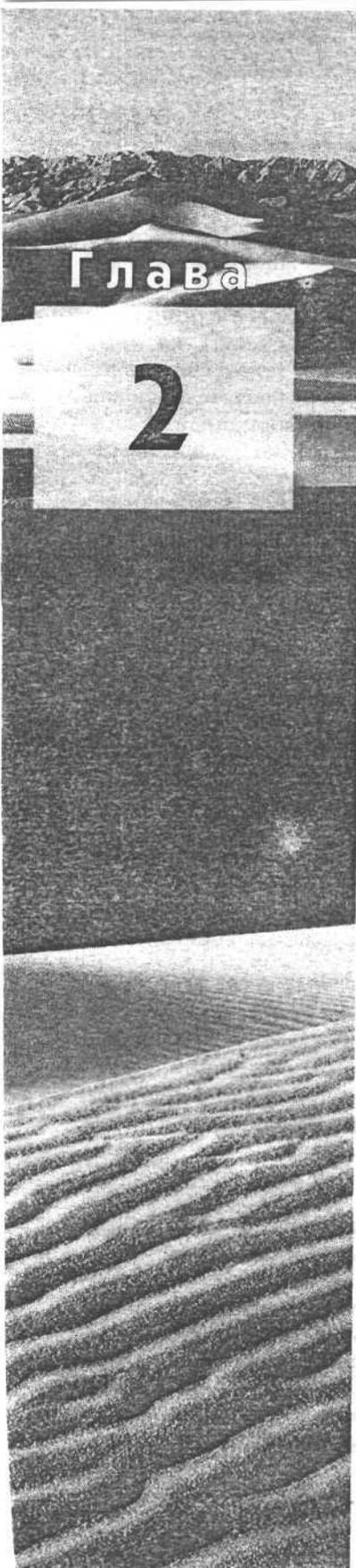
|                                    | A | B | C | D |
|------------------------------------|---|---|---|---|
| Домены конфликтов                  | 1 | 4 | 4 | 4 |
| Домены ширококвещательных рассылок | 1 | 1 | 1 | 4 |

---

**Ответы на проверочные вопросы**

---

- |         |                |
|---------|----------------|
| 1. B    | 11. C          |
| 2. C    | 12. A          |
| 3. D    | 13. D          |
| 4. A    | 14. B          |
| 5. D    | 15. A, B, C, D |
| 6. B, C | 16. E          |
| 7. C    | 17. D          |
| 8. C    | 18. C          |
| 9. D    | 19. B, C, D    |
| 10. A   | 20. B          |



Глава

2

## Технологии КОММУТАЦИИ

Коммутиция (лат. commutatio - изменение) - это процесс изменения состояния системы в зависимости от времени. В теории информации коммутиция является одним из основных понятий, характеризующих способность системы передавать и обрабатывать информацию. Коммутиция может быть реализована различными способами, в зависимости от типа системы и требований к ее работе. В настоящее время наиболее распространены коммутирующие устройства, основанные на полупроводниковых элементах, таких как транзисторы и диоды. Эти устройства позволяют эффективно управлять потоком информации, обеспечивая высокую скорость и надежность работы. Кроме того, в последнее время активно развиваются технологии оптической коммутиции, которые позволяют передавать информацию с помощью света, что значительно увеличивает скорость и емкость каналов связи. В заключение следует отметить, что коммутиция является фундаментальным процессом, лежащим в основе работы большинства современных информационных систем. Понимание принципов и технологий коммутиции необходимо для разработки эффективных и надежных систем передачи и обработки информации.

## Коммутация на уровне 2

Коммутация (переключение) на уровне 2 реализована аппаратно, т.е. для сетевой фильтрации используется MAC-адрес адаптера хоста. В переключателях установлены микросхемы ASIC (Application-Specific Integrated Circuits — специализированные интегральные микросхемы), которые формируют и обслуживают таблицы фильтрации. Допустимо считать переключатели уровня 2 многопортовыми мостами. Переключатели уровня 2 работают очень быстро, поскольку не пользуются информацией из заголовков сетевого уровня, а анализируют аппаратные адреса в кадре для решения о перенаправлении или об отбросе пакета.

Особенности коммутации на уровне 2:

- Аппаратная реализация мостов (MAC)
- Высокая скорость на линии
- Низкое запаздывание
- Низкая стоимость

Эффективность переключения на уровне 2 связана с тем, что нет изменений в пакетах данных, а все модификации связаны только с инкапсулирующими пакеты кадрами, следовательно, процесс коммутации выполняется быстрее и менее подвержен ошибкам, чем маршрутизация.

Переключение на уровне 2 используется в связях между рабочими группами и в сегментации сети (деление на домены конфликтов). Этот процесс позволяет создавать понятные сетевые проекты с гораздо большим количеством сегментов, чем в традиционных сетях ЮBaseT. Коммутация на уровне 2 увеличивает полосу пропускания для каждого пользователя, поскольку каждая связь (интерфейс) с переключателем образует собственный домен конфликтов, поэтому расширяются возможности подключения устройств к такому интерфейсу.

## Недостатки коммутации на уровне 2

Мы считаем коммутацию на уровне 2 аналогичной сети с мостами, поэтому должны столкнуться с теми же проблемами. Мосты эффективны только при правильном проектировании сети, т.е. при правильном делении на домены конфликтов. Правильным будет такой проект сети с мостами, где пользователи проводят не менее 80 % своего рабочего времени внутри собственных локальных сегментов.

Мосты делят сеть на домены конфликтов, но вся сеть остается одним большим доменом широковещательных рассылок. Переключатели уровня 2 (мосты) не способны разделить домен широковещательных рассылок, поскольку возникнут проблемы с производительностью и проявятся ограничения на размер сети. Широковещательные и многоадресные рассылки совместно с низким временем конвергенции алгоритма покрывающего дерева могут привести к серьезным проблемам при расширении размера сети. Учитывая эти проблемы, нельзя считать, что переключатели уровня 2 способны заменить маршрутизаторы (устройства уровня 3) в объединенной сети.

## Сравнение применения мостов с коммутацией в локальной сети

Переключатели уровня 2 реально являются мостами с большим числом портов. Однако между ними есть несколько важных отличий:

- Мосты реализованы программно, а переключатели — аппаратно, поскольку переключатели могут использовать микросхемы ASIC во время принятия решений о фильтрации данных.
- Мосты способны обслужить только один экземпляр покрывающего дерева на устройство, а переключатели — несколько покрывающих деревьев (см. ниже).
- Мосты содержат не более 16 портов, а переключатели могут иметь сотни портов.

## Три функции коммутации уровня 2

Во время переключения на уровне 2 выполняются три основные функции коммутации:

**Изучение адресов** Переключатели уровня 2 и мосты запоминают аппаратный адрес источника из каждого полученного интерфейсом кадра и хранят эту информацию в своей базе данных MAC-адресов.

**Решение о пересылке или фильтрации** Когда интерфейс получает кадр, переключатель анализирует аппаратный адрес назначения и ищет в своей базе данных MAC-адресов нужный интерфейс.

**Исключение заикливания** Если между переключателями для избыточности создано несколько путей, то могут появиться заикленные пути передачи информации. Протокол STP (Spanning-Tree Protocol — протокол покрывающего дерева) позволяет исключить заикливание пакетов в сети при сохранении избыточности.

Функции изучения адресов, решение о пересылке или фильтрации, а также исключение заикливания подробно рассмотрены ниже.

## Изучение адресов

После включения питания переключателя его таблица фильтрации MAC-адресов пуста. Когда устройство передает, а интерфейс получает кадр, переключатель помещает адрес источника в таблицу фильтрации MAC-адресов вместе с интерфейсом устройства. Переключатель не делает самостоятельных решений о перенаправлении кадров, поскольку не знает о местонахождении устройства назначения.

Если устройство отвечает и посылает кадр обратно, то переключатель извлекает адрес источника из возвращенного кадра и помещает MAC-адрес в свою базу данных, причем связывает этот адрес с интерфейсом, получившим кадр. Теперь переключатель имеет в таблице фильтрации два MAC-адреса и может установить соединение "точка-точка", а

кадры будут перемещаться только между двумя известными переключателем устройствами. Именно поэтому переключатель на уровне 2 работает эффективнее концентратора. В сетях с концентраторами кадры перенаправляются во все выходные порты устройства.

Рис. 2.1 показывает процедуру построения базы данных MAC-адресов.

На рисунке показаны четыре подключенные к переключателю хоста. После включения питания переключателя, его таблица MAC-адресов пуста.

1. Хост 1 посылает кадр хосту 3. MAC-адрес первого хоста равен 0000.8c01.1111, а MAC-адрес третьего хоста равен 0000.8c01.2222.
2. Переключатель принимает кадр в интерфейсе E0/1 (адресация интерфейсов рассмотрена в приложении В) и помещает в таблицу MAC-адресов адрес источника.
3. В базе данных MAC-адресов еще нет адреса назначения, поэтому кадр передается во все интерфейсы.
4. Хост 3 получает кадр и откликается на вызов хоста 1. Переключатель принимает этот ответный кадр в интерфейсе E2 и помещает аппаратный адрес источника второго кадра в базу данных MAC-адресов.
5. Хосты 1 и 3 могут установить соединение "точка-точка", причем кадры будут пересылаться только между этими двумя устройствами. Хосты 2 и 4 не будут "видеть" подобные кадры.

Если в течение определенного времени два устройства не будут откликаться во время передачи кадров через переключатель, то переключатель очистит соответствующие записи в своей базе данных, чтобы поддерживать корректность таблицы адресов.



Рис. 2.1. Изучение переключателем местоположения хостов в сети

## Решение о пересылке и фильтрации

Когда кадр попадает в интерфейс переключателя, аппаратный адрес назначения сравнивается с базой данных перенаправления/фильтрации MAC-адресов. Если аппаратный адрес назначения известен и присутствует в базе данных, то кадр направляется только в один выходной интерфейс, предписанный в таблице базы данных. Переключатель не транслирует кадр во все остальные интерфейсы, за исключением интерфейса, ведущего к точке назначения. Это сохраняет полосу пропускания в других сетевых сегментах, а сам процесс называется *фильтрацией кадров* (frame filtering).

Если же аппаратный адрес назначения не указан в базе данных MAC-адресов, то кадр отсылается в широковещательной рассылке по всем активным интерфейсам, за исключением интерфейса, в котором этот кадр был получен. Если одно из устройств откликается на широковещательную рассылку, происходит обновление базы данных MAC-адресов за счет добавления местоположения устройства (интерфейса).

## Исключение заикливания

Для связи между переключателями полезны избыточные соединения, которые помогают предотвратить отказ сети при выходе из строя отдельной связи. Несмотря на полезность избыточных соединений, они создают гораздо больше проблем, чем решают. Поскольку кадры одновременно передаются в широковещательных рассылках по всем дублирующим соединениям, могут возникать заикливания, а также другие проблемы. Наиболее серьезные негативные последствия перечислены в списке:

1. Если не реализована схема исключения заикливания, переключатель переполнит бесконечными широковещательными рассылками объединенную сеть. Это называется *штормом широковещательных рассылкок* (broadcast storm). Рис. 2.2 показывает распространение в сети такого шторма. Заметим, что согласно рисунку кадры будут бесконечно пересылаться в широковещательных рассылках на физическом уровне объединенной сети.

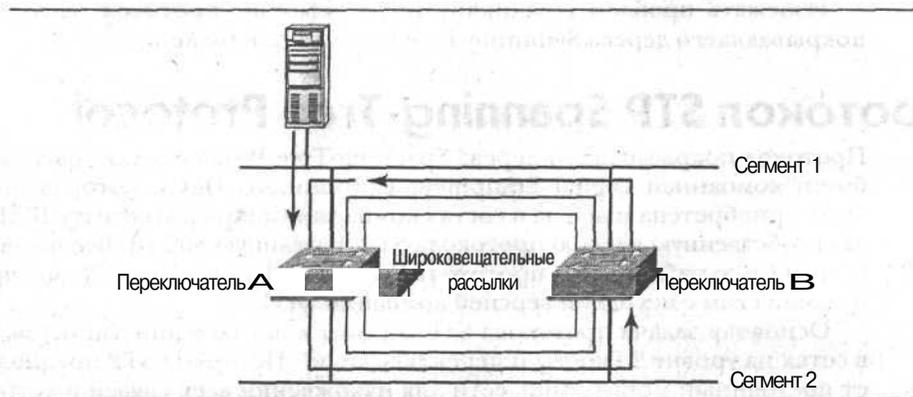


Рис. 2.2. Широковещательный шторм

2. Устройство может получить несколько копий одного кадра, поскольку кадры одновременно поступают из разных сегментов. Рис. 2.3 показывает одновременное поступление нескольких кадров из разных сегментов.

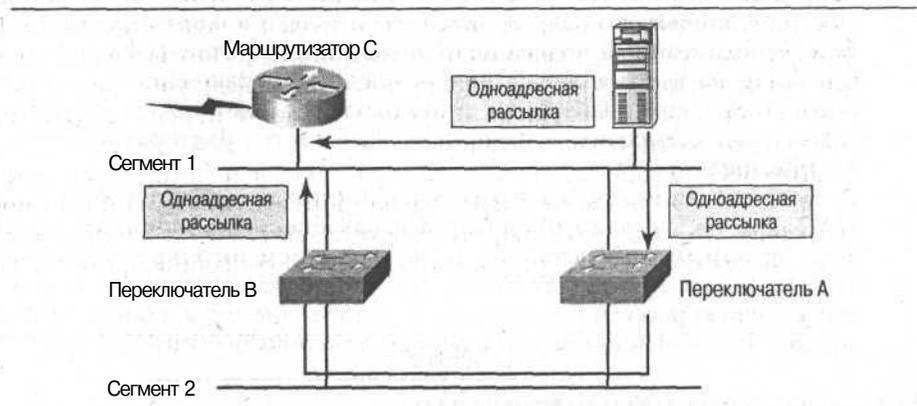


Рис. 2.3. Несколько копий кадра

3. Таблица фильтрации MAC-адресов не может быть заполнена корректно, поскольку переключатель получает ответы от одного устройства по нескольким связям. Вполне возможно, что переключатель не сможет переслать кадр, поскольку будет постоянно обновлять таблицу фильтрации MAC-адресов на основе постоянно меняющихся сведений о местоположении аппаратного адреса источника. Этот процесс называется "хлопаньем" (thrashing) MAC-таблицы.
4. Наиболее опасной проблемой является генерация нескольких замкнутых путей в объединенной сети. Замыкание одного пути порождает замыкание в других путях по сети, а шторм широковещательных рассылок будет усиливаться до такой степени, что произойдет полная остановка в работе сети.

Избежать проблем с замыканием помогает протокол (алгоритм) покрывающего дерева Spanning-Tree Protocol (см. ниже).

## Протокол STP Spanning-Tree Protocol

Протокол покрывающего дерева Spanning-Tree Protocol (STP) был разработан компанией Digital Equipment Corporation (DEC), которая позже была приобретена и вошла в состав компании Compaq. Институт IEEE создал собственную версию протокола STP, названную 802.1d. Все переключатели Cisco работают по протоколу IEEE 802.1d алгоритма STP, который не совместим с исходной версией компании DEC.

Основная задача протокола STP состоит в исключении замыкания в сетях на уровне 2 (мосты и переключатели). Протокол STP предполагает постоянный мониторинг сети для нахождения всех связей и устранения замыкания за счет отключения избыточных связей.

## Действие алгоритма покрывающего дерева

Протокол STP позволяет найти все связи в сети и выделить среди них избыточные, чтобы отключить избыточные связи и тем самым устранить любые заикливания в сети. Для этого производится выбор корневого моста (root bridge), который будет следить за сетевой топологией. В любой сети может быть только один корневой мост. Порты такого моста называются *назначенными* (designated port), поскольку работают в режиме состояния пересылки (forwarding-state). Порты пересылки состояния принимают и отправляют трафик.

Другие переключатели в сети называются некорневыми мостами (nonroot bridge) — см. рис. 2.4. Однако порты с небольшой стоимостью (которая определяется полосой пропускания связи) к корневому мосту называются корневыми портами (root port) и способны принимать и отправлять трафик.

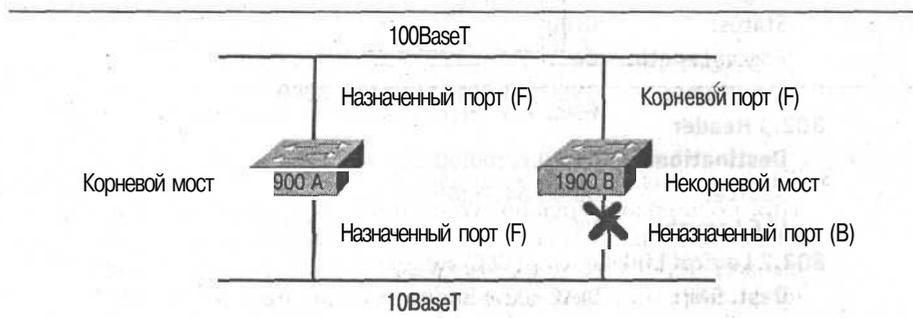


Рис. 2.4. Действие алгоритма покрывающего дерева

Назначенными называются также порты, ведущие к корневому мосту и имеющие наименьшую стоимость. Другие порты моста являются неназначенными (nondesignated) и не способны принимать и отправлять трафик — этот режим называется блокировкой (blocking mode).

## Выбор корневого моста

Исполняющие протокол STP переключатели и мосты обмениваются информацией о элементах данных протокола моста BPDU (Bridge Protocol Data Unit). Элементы BPDU передают сообщения о конфигурации в кадрах широковещательных рассылок. С помощью BPDU остальным устройствами пересылается идентификатор каждого моста.

Идентификатор моста служит для выявления в сети корневого моста и назначенных корневых портов. Идентификатор имеет длину 8 байтов и содержит сведения о приоритете и MAC-адресе устройства. Приоритет всех устройств, исполняющих протокол STP по версии IEEE, равен 32 768.

Чтобы определить корневой мост, анализируются идентификатор и MAC-адрес моста. Если два переключателя или моста имеют одинаковое

значение приоритета, то MAC-адрес служит для выявления устройства с наименьшим идентификатором. Например, если два переключателя с именами А и В имеют приоритет по умолчанию 32 768, то используются MAC-адреса. Если MAC-адрес переключателя А равен 0000.0c00.1111.1111, а MAC-адрес переключателя В - 0000.0c00.2222.2222, то корневым мостом станет переключатель А.

В показанном ниже листинге сетевого анализатора видна пересылка элементов BPDU от переключателя серии 1900. По умолчанию элементы BPDU отсылаются каждые две секунды. Может показаться, что это сильно нагружает сеть, но мы имеем дело только с кадрами уровня 2, а не с пакетами на уровне 3.

Основываясь на материале из главы 1 можно заключить, что в листинге показаны кадры 802.2, поскольку только кадры формата 802.3 имеют поля DSAP и SSAP в заголовке LLC.

```
Flags: 0x80 802.3
Status: 0x00
Packet Length: 64
Timestamp: 19:33:18.726314 02/28/2000
```

#### 802.3 Header

```
Destination: 01:80:c2:00:00:00
Source: 00:b0:64:75:6b:c3
LLC Length: 38
```

#### 802.2 Logical Link Control (LLC) Header

```
Dest. SAP: 0x42 802.1 Bridge Spanning Tree
Source SAP: 0x42 802.1 Bridge Spanning Tree
Command: 0x03 Unnumbered Information
```

#### 802.1 - Bridge Spanning Tree

(покрывающее дерево моста по спецификации 802.1)

```
ProtocolIdentifier: 0
Protocol Version ID: 0
Message Type: 0 Configuration Message
Flags: %00000000
Root Priority/ID: 0x8000 / 00:b0:64:75:6b:c0
Cost Of Path To Root: 0x00000000 (0)
Bridge Priority/ID: 0x8000 / 00:b0:64:75:6b:c0
Port Priority/ID: 0x80 / 0x03
Message Age: 0/256 seconds
(точно 0 с)
Maximum Age: 5120/256 seconds
(точно 20 с)
Hello Time: 512/256 seconds
(точно 2 с)
Forward Delay: 3840/256 seconds
(точно 15 с)
```

Extra bytes (Padding):  
 ..... 00 00 00 00 00 00 00 00  
**Frame Check Sequence:** 0x2e006400

Получив реальные данные BPDU, можно узнать стоимость пути к корню. В листинге это значение равно нулю, поскольку переключатель является корневым мостом. Стоимость пути мы рассмотрим ниже.

## Выбор назначенных портов

Чтобы выявить порт или порты, используемые для коммуникаций с корневым мостом, нужно сначала определить стоимость пути (path cost). Стоимость в протоколе STP подсчитывается на основе суммы стоимостей участков, которые определяются полосой пропускания связи. В таблице 2.2 показаны типичные стоимости для разных сетей Ethernet.

**Таблица 2.2.**  
**Типичные стоимости разных сетей Ethernet**

| Скорость   | Новая стоимость IEEE | Исходная стоимость IEEE |
|------------|----------------------|-------------------------|
| 10 Гбит/с  | 2                    | 1                       |
| 1 Гбит/с   | 4                    | 1                       |
| 100 Мбит/с | 19                   | 10                      |
| 10 Мбит/с  | 100                  | 100                     |

Спецификация IEEE 802.1d была пересмотрена для согласования с появившимися высокоскоростными связями. Переключатель серии 1900 использует исходную спецификацию IEEE 802.1d.

## Состояния портов в алгоритме покрывающего дерева

Порты моста или переключателя, исполняющего протокол STP, могут находиться в одном из четырех состояний:

**Blocking** (блокировка) Кадры не передаются, но принимаются элементы BPDU. После подачи напряжения на переключатель все его порты по умолчанию переходят в состояние блокировки.

**Listening** (слушание) Прием элементов BPDU для исключения появления в сети заикливания, еще до начала передачи кадров данных.

**Learning** (изучение) Обнаружение MAC-адресов и построение таблицы фильтрации, но без пересылки кадров.

**Forwarding** (перенаправление) Прием и передача всех данных на порту, исполняющем функции моста.

Обычно порты переключателя находятся в состоянии блокирования или перенаправления. Перенаправляющий порт выбран так, что имеет наименьшую стоимость пути к корневому мосту, однако если изменяется топология сети (например, вследствие отказа одной из связей или ввода администратором нового переключателя), то порты переключателя переходят в состояние слушания или изучения.

Блокированные порты предотвращают заикливание в сети. Когда переключатель выбрал наилучший путь к корневому мосту, все остальные порты переводятся в блокированное состояние, в котором эти порты способны принимать элементы BPDU.

Если переключатель выявит, что заблокированный порт должен стать назначенным, то этот порт переводится в состояние слушания. Порт будет прослушивать все элементы BPDU, чтобы не сформировать заикливаемых путей после перехода в состояние перенаправления.

### Конвергенция

Конвергенция (согласование) проявляется при переходе мостов и переключателей в состояние перенаправления или блокирования. Во время периода конвергенции не происходит перенаправление данных. Конвергенция необходима для согласования баз данных во всех устройствах.

Перед началом перенаправления данных все устройства должны обновить свои базы данных. Проблема в том, что для конвергенции нужно некоторое время, в течение которого происходит обновление информации в устройствах. Обычно требуется 50 секунд для перехода из состояния блокирования в состояние перенаправления. Не рекомендуется изменять установленные по умолчанию значения таймеров STP, но при необходимости эти таймеры допускают настройку. Задержка перенаправления — это время перехода порта из состояния слушания или изучения в состояние перенаправления.

## Пример использования алгоритма покрывающего дерева

Важно понять действие алгоритма покрывающего дерева в объединенной сети, чтобы предвидеть изменения в реальной сетевой среде. На рис. 2.5 показаны три переключателя с одинаковым приоритетом 32 768. Однако каждый переключатель имеет индивидуальный MAC-адрес. Анализируя приоритет и MAC-адрес каждого переключателя, можно выявить корневой мост.

Поскольку устройство 1900A имеет наименьший MAC-адрес и все три переключателя сохраняют приоритет по умолчанию, устройство 1900A станет корневым мостом.

Для определения корневых портов в переключателях 1900B и 1900C нужно выяснить стоимость связей подключения к корневому переключателю. Поскольку оба переключателя подключены к корневому переключателю из портов 0 по связи 100 Мбит/с (что является наилучшей стоимостью для данного случая), корневыми в обоих переключателях станут порты 0.



Рис. 2.5. Пример покрывающего дерева

Для выявления назначенных портов переключателей используется идентификатор моста. Все порты корневого моста назначены. Однако оба устройства 1900В и 1900С имеют одинаковую стоимость пути к корневому мосту, поэтому назначенным станет порт переключателя 1900В, поскольку это устройство имеет наименьший идентификатор моста. Учитывая, что назначенным выбран порт устройства 1900В, переключатель 1900С переведет свой порт 1 в заблокированное состояние и предохранит сеть от появления закливания.

## Типы переключателей локальных сетей

Задержка коммутации пакетов в переключателе зависит от выбранного режима работы. Существуют три режима работы переключателей:

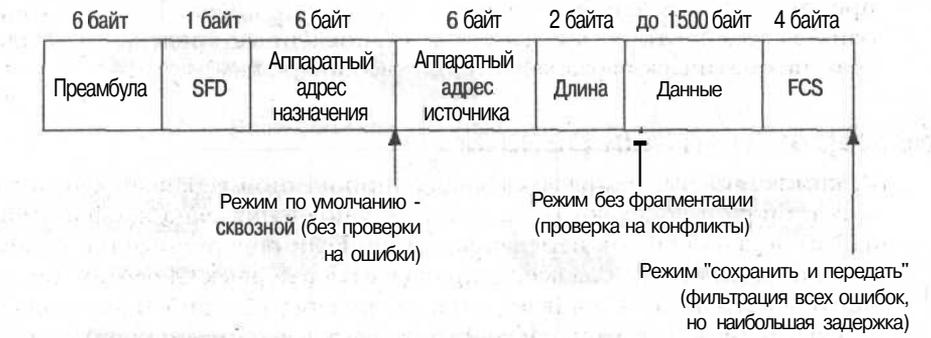
**Store and forward** (сохранить и передать) В буфер переключателя записывается весь кадр данных, проверяется CRC, а затем в таблице фильтрации MAC-адресов выбирается адрес назначения для полученного кадра.

**Cut-through** (сквозной) Переключатель только ожидает получения аппаратного адреса назначения, а затем производит по нему поиск в таблице фильтрации MAC-адресов.

**FragmentFree** (без фрагментации) Режим по умолчанию для переключателя Catalyst 1900, который иногда называют модифицированным сквозным режимом (modified cut-through). Производится проверка первых 64 байтов кадра для фрагментации (из-за возможных конфликтов в сегменте) перед перенаправлением кадра.

Рис. 2.6 показывает различные части кадра, связанные с режимами переключения.

Все режимы переключателей подробно рассматриваются ниже.



**Рис. 2.6.** Соотношение между режимами переключателя и частями кадра

## Режим "сохранить и передать"

Переключатель в режиме "сохранить и передать" является одним из трех основных типов переключателей локальных сетей. В таком режиме переключатель локальной сети полностью копирует кадр в собственный встроенный буфер и проверяет контрольную сумму CRC. Поскольку копируется весь кадр, задержка коммутации переключателя зависит от длины кадра.

При ошибке CRC кадр отбрасывается, а также отбрасываются слишком короткие (менее 64 байтов, включая CRC) или слишком длинные (более 1518 байтов, включая CRC) кадры. Если в кадре не обнаружено ошибок, переключатель локальной сети выполняет поиск по аппаратному адресу назначения в своей таблице коммутации или перенаправления и выявляет выходной интерфейс для кадра. Затем кадр отправляется через выбранный интерфейс в точку назначения. Этот режим используется в переключателях серии Catalyst 5000 и не может быть изменен в устройстве.

## Сквозной режим (реальное время)

Еще одним основным типом переключателей в локальных сетях являются устройства, работающие в *сквозном режиме*. В этом режиме переключатель копирует в собственный встроенный буфер только адрес назначения (первые шесть байтов после преамбулы). Затем ищется аппаратный адрес назначения в MAC-таблице переключателя, чтобы определить выходной интерфейс и направить в него кадр. Сквозные переключатели обеспечивают низкую задержку, поскольку начинают пересылку кадра сразу после чтения адреса назначения и выявления выходного интерфейса.

Некоторые переключатели могут настраиваться на сквозной режим для каждого отдельного порта. Причем этот режим действует до превышения установленной пользователем границы ошибок. Затем устройство автоматически переходит в режим "сохранить и передать", чтобы

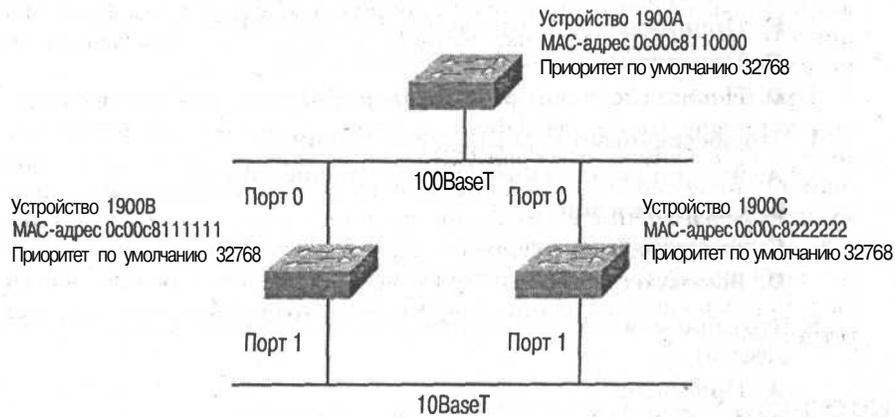
предотвратить дальнейшее распространение ошибок. Если же уровень ошибок для порта возвращается в установленные пределы, переключатель автоматически возвращается в сквозной режим.

## Бесфрагментный режим

Режим FragmentFree является модифицированной версией сквозного режима, причем переключатель ожидает заполнения окна конфликтов (64 байта) до выполнения перенаправления. Если обнаруживается ошибка в принятом пакете, то она всегда проявляется в первых 64 байтах. Бесфрагментный режим обеспечивает лучшую проверку на ошибки по сравнению со сквозным режимом (в частности, за счет того, что не происходит увеличения задержки на длинных кадрах). Этот режим установлен по умолчанию для переключателей серии 1900.

## Упражнение

Ответьте на вопросы по предложенному рисунку.



1. Укажите корневой мост?
2. Укажите назначенные порты?
3. Укажите неназначенные порты?
4. Какие порты заблокированы?

## Проверочные вопросы

---

1. В каком режиме переключатель локальной сети проверяет CRC в каждом кадре?
  - A. Сквозном
  - B. Сохранить и передать
  - C. Проверки фрагментов
  - D. Без фрагментов
2. В каком режиме переключатель локальной сети перед перенаправлением кадра проверяет только аппаратный адрес?
  - A. Сквозном
  - B. Сохранить и передать
  - C. Проверки фрагментов
  - D. Без фрагментов
3. Что справедливо для заблокированного состояния порта в протоколе STP? (Укажите все правильные ответы).
  - A. Не передаются и не принимаются кадры,
  - B. Принимаются и передаются элементы BPDU.
  - C. Продолжается прием элементов BPDU.
  - D. Передаются и не принимаются кадры.
4. Что обеспечивает переключатель уровня 2?
  - A. Функции моста на аппаратном уровне (MAC)
  - B. Скорость в линии
  - C. Высокую задержку
  - D. Высокую стоимость
5. Что определяет в сети корневой мост? (Укажите все правильные ответы)
  - A. Приоритет
  - B. Стоимость подключенных к переключателю связей
  - C. MAC-адрес
  - D. IP-адрес
6. Что определяет назначенный порт моста?
  - A. Приоритет
  - B. Стоимость подключенных к переключателю связей
  - C. MAC-адрес
  - D. IP-адрес
7. Каковы четыре состояния порта в переключателе STP?
  - A. Learning (изучение)
  - B. Learned (изученное)

- C. Listened (выслушанное)
  - D. Heard (услышанное)
  - E. Listening (слушание)
  - F. Forwarding (перенаправление)
  - G. Forwarded (перенаправленное)
  - H. Blocking (блокировка)
  - I. Gathering (сбор)
8. Каковы три разные функции переключателя уровня 2?
- A. Изучение адресов
  - B. Маршрутизация
  - C. Перенаправление и фильтрация
  - D. Создание сетевого зацикливания
  - E. Исключение зацикливания
  - F. Адресация по протоколу IP
9. Что справедливо для элементов BPDU?
- A. Используются для передачи конфигурационных сообщений с помощью пакетов IP
  - B. Используются для передачи конфигурационных сообщений с помощью кадров многоадресных рассылок
  - C. Используются для передачи сведений о стоимости связей STP
  - D. Используются для установки идентификатора моста в переключателе.
10. Если переключатель считает, что заблокированный порт должен стать назначенным, то в какое состояние должен быть переведен порт?
- A. Unblocked (разблокированное)
  - B. Forwarding (перенаправления)
  - C. Listening (слушания)
  - D. Listened (выслушанное)
  - E. Learning (изучения)
  - F. Learned (изученное)
11. Чем отличаются мосты и переключатели уровня 2? (Укажите все правильные ответы.)
- A. Мосты могут использовать только одно покрывающее дерево для одного устройства.
  - B. Переключатели могут иметь несколько покрывающих деревьев для одного устройства.
  - C. Мосты могут применять несколько покрывающих деревьев для одного устройства.
  - D. Переключатели могут иметь только одно покрывающее дерево для одного устройства.

12. Чем отличаются мосты и переключатели уровня 2? (Укажите все правильные ответы)
- A. Переключатели реализованы программно.
  - B. Мосты реализованы аппаратно.
  - C. Переключатели реализованы аппаратно.
  - D. Мосты реализованы программно.
13. Что делает переключатель после получения кадра в интерфейсе, когда неизвестен аппаратный адрес назначения или его нет в таблице фильтрации?
- A. Переслать переключателю по первой доступной связи
  - B. Отбросить кадр
  - C. Послать в сеть кадры поиска устройства
  - D. Возвратить сообщение исходной сетевой станции и запросить у нее разрешения имен
14. Какой тип переключателя локальной сети ожидает окно конфликтов до того, как начать поиск аппаратного адреса назначения в таблице фильтрации MAC-адресов и перенаправление этого кадра?
- A. Сквозной
  - B. Сохранить и передать
  - C. Проверки фрагментов
  - D. Без фрагментов
15. Каким по умолчанию является переключатель локальной сети серии 1900?
- A. Сквозным
  - B. Сохранить и передать
  - C. Проверки фрагментов
  - D. Без фрагментов
16. Как используется идентификатор моста переключателя, взаимодействующего с соседним переключателем?
- A. В процессе маршрутизации по протоколу IP
  - B. По протоколу STP
  - C. Во время перехода между четырьмя состояниями STP переключателя
  - D. В элементе Bridge Protocol Data Units
  - E. В широковещательных рассылках в процессе конвергенции
17. Как определяется корневой порт переключателя?
- A. Переключатель выявляет связь к корневому мосту с наибольшей стоимостью.
  - B. Переключатель выявляет связь к корневому мосту с наименьшей стоимостью.

- C.** Используется наибольшая скорость пересылки и приема BPDU между переключателями, на основе чего выявляется корневой порт.
- D.** Корневой мост отправляет в широковещательных рассылках собственный идентификатор моста, а принимающие устройства выявляют интерфейсы по полученным сообщениям и делают корневыми соответствующие порты.
- 18.** Сколько мостов допустимо иметь в сети?
- A.** 10
- B.** 1
- C.** Один для каждого переключателя
- D.** 20
- 19.** Что произойдет, если в сети не реализовано исключение заикливания?
- A.** Уменьшится время конвергенции
- B.** Шторм широковещательных пакетов
- C.** Несколько копий кадров \*
- D.** Маршрутизация IP приведет к неустойчивым связям по последовательным линиям
- 20.** Каков в протоколе STP приоритет по умолчанию для переключателя?
- A.** 32768
- B.** 3276
- C.** 100
- D.** 10
- E.** 1

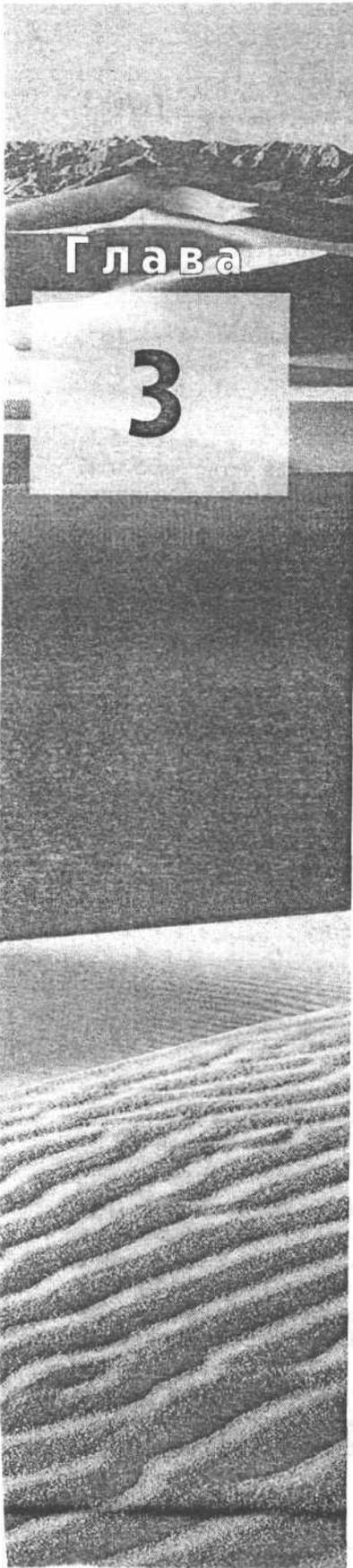
## Ответы к упражнению

---

1. 1900A
2. Порты 0 и 1 корневого моста, порт 0 переключателей 1900B и 1900C
3. Порт 1 устройства 1900C
4. Порт 1 устройства 1900C

## Ответы на проверочные вопросы

- |               |          |
|---------------|----------|
| 1. B          | 11. A, B |
| 2. A          | 12. C, D |
| 3. A, C       | 13. C    |
| 4. A, B       | 14. D    |
| 5. A, C       | 15. D    |
| 6. B          | 16. D    |
| 7. A, E, F, H | 17. B    |
| 8. A, C, E    | 18. B    |
| 9. B          | 19. B, C |
| 10. C         | 20. A    |



Глава

3

# Протокол Интернета

Модель OSI и TCP/IP

- Модель OSI
- Модель TCP/IP
- Сравнение OSI и TCP/IP
- Слои модели OSI
- Слои модели TCP/IP

Рис. 3.1. Сравнение моделей OSI и TCP/IP



Рис. 3.1. Сравнение моделей OSI и TCP/IP

Описание: В данной таблице сравниваются две модели сетевых коммуникаций: модель OSI (Open Systems Interconnection) и модель TCP/IP. Модель OSI состоит из семи слоев, в то время как модель TCP/IP состоит из четырех слоев. Соответствие между слоями показано стрелками.

| Модель OSI           | Модель TCP/IP     |
|----------------------|-------------------|
| 1. Физический        | Сетевой интерфейс |
| 2. Канальный         | Сетевой интерфейс |
| 3. Сетевой           | Сетевой           |
| 4. Транспортный      | Транспортный      |
| 5. Сессионный        | Сетевой интерфейс |
| 6. Представительский | Сетевой интерфейс |
| 7. Прикладной        | Прикладной        |

## Модели TCP/IP и DoD

Базовая модель DoD (Department of Defense — Министерство обороны США) является компактной версией базовой модели OSI. В DoD определены 4 (вместо семи) уровня:

- Уровень процессов/приложений (Process/Application)
- Уровень взаимодействия хостов (Host-to-Host)
- Уровень Интернета (Internet)
- Уровень доступа к сети (Network Access)

На рис. 3.1 сопоставляются две базовые модели. Как легко заметить, модели сходны по идее, но содержат разное число уровней с различными названиями.

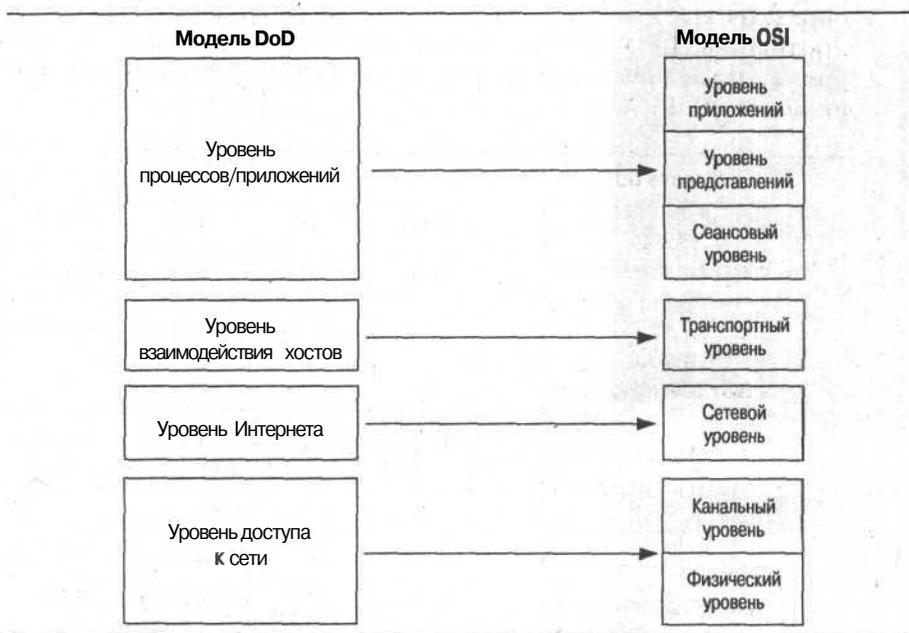


Рис. 3.1. Сопоставление базовой модели DoD и базовой модели OSI

Огромное множество протоколов объединено на *уровне процессов/приложений* модели DoD для решения задач, которые в модели OSI разложены на три верхних уровня (приложений, представлений и сеансовый). Подробно эти протоколы рассматриваются ниже. Уровень процессов/приложений определяет протоколы для взаимодействия приложений, выполняемых на разных узлах сети, и управляет спецификациями пользовательских интерфейсов.

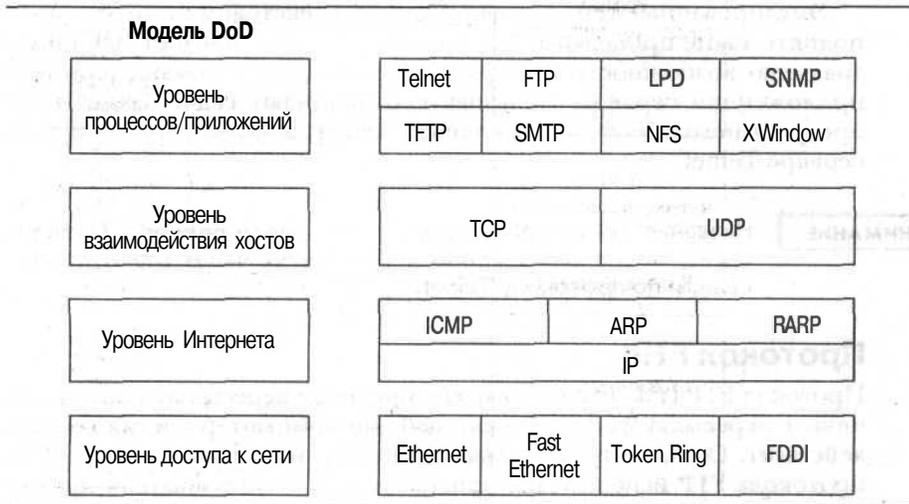
*Уровень взаимодействия хостов* соответствует транспортному уровню модели OSI и определяет протоколы, управляющие уровнем службы передачи данных приложениям. На этом уровне устанавливается надежная

связь между конечными хостами, обеспечивается доставка данных без ошибок, осуществляется упорядоченная передача пакетов и проверка целостности данных.

*Уровень Интернета* соответствует сетевому уровню модели OSI. Здесь определены протоколы логической передачи пакетов по всей сети. На этом уровне выполняются адресация хостов путем присваивания им IP-адресов, маршрутизация пакетов между сетями и управление потоками данных между хостами.

На нижнем уровне модели — *уровне доступа к сети* — производится управление обменом данными между хостом и сетью. Этот уровень, эквивалентный каналному и физическому уровням модели OSI, проверяет аппаратные адреса и определяет протоколы для физической передачи данных.

Модели DoD и OSI похожи по реализуемым идеям и структуре, но определенные в них функции выполняются по-разному. Поэтому наборы протоколов DoD и OSI существенно отличаются друг от друга. На рис. 3.2 представлен набор протоколов TCP/IP, отображаемый на уровне модели DoD.



**Рис. 3.2.** Набор протоколов TCP/IP

### Протоколы уровня процессов/приложений

В этом разделе мы обсудим типичные приложения и службы сетей IP. Среди рассматриваемых протоколов и приложений:

- Telnet
- FTP
- TFTP
- NFS

- SMTP
- LPD
- X Window
- SNMP
- DNS
- BootP
- DHCP

## Telnet

Основное назначение *Telnet* состоит в эмуляции терминала, благодаря чему пользователь, работающий на удаленном компьютере, называемом клиентом Telnet, получает доступ к ресурсам другой машины — сервера Telnet. Протокол проецирует клиентский компьютер на сервер Telnet так, что компьютер выглядит как терминал, непосредственно подключенный к локальной сети. В действительности, проекция является программным образом, виртуальным терминалом, способным взаимодействовать с удаленным хостом.

Эмулированные терминалы работают в текстовом режиме и могут выполнять такие процедуры, как просмотр меню с предоставлением пользователю возможности выбора в нем различных команд или доступ к приложениям сервера. Пользователи начинают сеанс Telnet с запуска программного обеспечения клиента Telnet, а затем регистрируются на сервере Telnet.

### ▼ ВНИМАНИЕ

1 Название Telnet происходит от "telephone network" (телефонные сети), поскольку именно в этих сетях чаще всего проводятся сеансы по протоколу Telnet.

## Протокол FTP

Протокол FTP (*File Transfer Protocol* — протокол пересылки файлов) обеспечивает пересылку файлов между любыми компьютерами, на которых он действует. Однако это не только протокол, но и программа. В качестве протокола FTP используется приложениями, а пользователи применяют его как программу для работы с файлами. Кроме того, FTP обеспечивает доступ ко всем каталогам и файлам и способен выполнять некоторые операции с каталогами, например их перемещение. Взаимодействие FTP с Telnet дает возможность пользователю зарегистрироваться на сервере FTP и выполнить затем пересылку файлов.

Доступ к хосту с помощью FTP является только первым шагом. Затем пользователи подвергаются регистрации с аутентификацией, которая, возможно, защищена паролями и именами пользователей, введенными администратором для ограничения доступа. Вы можете обойти защиту, выбрав имя пользователя "anonymous" (аноним), однако доступ к файлам сервера будет значительно ограничен.

Даже когда FTP применяется пользователями как программа, его функции ограничены просмотром каталогов и манипуляциями с ними, печатью содержимого файлов и копированием файлов между хостами. Он не может выполнять удаленные файлы как программы.

### Протокол TFTP

Протокол TFTP (*Trivial File Transfer Protocol* — простейший протокол пересылки файлов) является сокращенной версией FTP, которую следует применять лишь в тех случаях, когда вы точно знаете, что вы хотите и где это находится. Множество функций TFTP существенно беднее, по сравнению с FTP; в частности, среди них нет даже функции просмотра каталогов. TFTP позволяет всего лишь посылать и получать файлы, но и пересылаемые блоки данных значительно меньше, чем в протоколе FTP. Кроме того, TFTP не предполагает аутентификации. Не многие применяют этот протокол из-за высокого риска несанкционированного доступа.

#### ВНИМАНИЕ

Несколько позже мы воспользуемся протоколом TFTP для загрузки IOS (*Internetwork Operating System* — межсетевая операционная система) в маршрутизатор Cisco.

### Протокол NFS

Протокол NFS (*Network File System* — сетевая файловая система) создан специально для совместного использования файлов. Он обеспечивает взаимодействие двух разнотипных файловых систем. Предположим, что программное обеспечение сервера NFS работает на сервере Windows NT, а клиентское программное обеспечение — на хосте Unix. NFS позволяет прозрачно сохранить файлы Unix в оперативной памяти сервера Windows NT, которая в свою очередь доступна пользователям Unix. Хотя файловые системы Windows NT и Unix не похожи друг на друга (отличаясь по чувствительности к регистру, длине имен файлов, защите и т.д.), пользователи обеих систем могут получить доступ к одному и тому же файлу обычным для себя способом.

### Протокол SMTP

Протокол SMTP (*Simple Mail Transfer Protocol* — простой протокол пересылки почты) регулирует работу электронной почты, применяя для ее доставки метод буферизации. После отправки сообщения адресату оно записывается в буфер на некотором устройстве (обычно — на диске). Программное обеспечение сервера адресата регулярно проверяет наличие сообщений в буфере. Обнаруженное сообщение доставляется получателю.

### Протокол LPD

Протокол LPD (*Line Printer Daemon* — демон построчной печати) создан для совместного использования принтера. LPD вместе с программой LPR (*Line Printer*) позволяет буферизировать задания печати и посылать их на сетевые Принтеры.

## Протокол X Window

Разработанный для операций клиент/сервер протокол *X Window* применяется для создания приложений клиент/сервер, использующих графический пользовательский интерфейс. Идея состоит в том, чтобы позволить программе, называемой клиентом, работать на одном компьютере, а затем выводить информацию на экран другого компьютера, используя для этого программу, называемую оконным сервером.

## Протокол SNMP

Протокол SNMP (*Simple Network Management Protocol* — простой протокол управления сетью) создан для сбора и обработки информации о работе сети. Данные собираются путем опроса сетевых устройств со станции управления сетью через фиксированные или случайные интервалы времени. Если устройство функционирует нормально, создается так называемый *базовый отчет*, содержащий описание операционных свойств жизнеспособной сети. Протокол SNMP можно также использовать в качестве наблюдателя за сетью, быстро сообщающего администратору о любом непредвиденном изменении хода событий. Такие сетевые наблюдатели, называемые *агентами*, посылают предупреждения — *системные прерывания* (trap) — на станцию управления при возникновении каких-либо нарушений в сети.

## Служба доменных имен DNS

*Служба доменных имен* (Domain Name Service) выполняет разрешение (определение) имен хостов, в частности, имен Интернета, подобных `www.routersim.com`. Не обязательно пользоваться этой службой. Достаточно ввести *IP-адрес* любого устройства. IP-адрес определяет хост в сети или Интернете, однако служба DNS просто упрощает ввод данных. Что произойдет после переноса Web-страницы на сервер другого провайдера? Изменится IP-адрес и уже не будут действовать запросы по старому адресу страницы. Служба DNS позволяет использовать доменные имена для указания IP-адресов. Можно сколько угодно часто изменять IP-адрес, но посетители страницы не увидят никаких отличий в процедуре обращения к Web-странице.

Служба DNS использует для разрешения имен полностью квалифицированные доменные имена FQDN (Fully Qualified Domain Name), например `www.lammle.com` или `todd.lammle.com`. Имена FQDN обладают иерархией, что позволяет логически описать местоположение системы на основе ее доменного имени.

Чтобы разрешить имя "todd", следует ввести это имя в виде FQDN (т.е. `todd.lammle.com`), либо установить в устройстве или ПК режим добавления суффиксов. Например, в маршрутизаторе Cisco можно использовать команду `ip domain-name lammle.com` для добавления имени домена `lammle.com` к каждому запросу. Если не указывать добавляемый суффикс, то придется вводить полное имя FQDN, чтобы служба DNS выполнила разрешение имени.

## Bootstrap Protocol (BootP)

BootP означает *протокол перехвата загрузки* (Bootstrap Protocol). Когда включается питание на бездисковой рабочей станции, это устройство выполняет в сети широковещательную рассылку запроса по протоколу BootP. Сервер BootP откликается на запрос и ищет MAC-адрес клиентской станции в своем файле BootP. Если будет найдена соответствующая запись, то сервер отвечает на запрос, предоставляя клиентскому компьютеру свой IP-адрес и файл — обычно по протоколу TFTP — которые будут использоваться для загрузки рабочей станции.

Протокол BootP используется бездисковыми компьютерами в следующих целях:

- Получение собственного IP-адреса
- « Получение IP-адреса и имени хоста сервера
- » Получение имени файла загрузки, который будет помещен в память и выполнен при запуске устройства

Может показаться, что BootP — это старая и ненужная программа, но это неправильно. Протокол BootP используется до сих пор. Сегодня он называется DHCP (Dynamic Host Configuration Protocol).

## Протокол DHCP

*Протокол конфигурации динамических хостов* DHCP (Dynamic Host Configuration Protocol) предоставляет хостам IP-адреса. Протокол упрощает администрирование и используется для сетей любого размера (от небольших до очень крупных). В качестве сервера DHCP могут выступать разные устройства, в том числе и маршрутизаторы Cisco.

DHCP отличается от BootP тем, что BootP присваивает IP-адрес хосту, но аппаратный адрес хоста должен быть вручную внесен в таблицу BootP. Можно считать DHCP динамической версией BootP. Однако следует помнить, что BootP служит для пересылки хосту операционной системы, которая используется во время загрузки хоста. DHCP не способен выполнить эту функцию.

Сервер DHCP предоставляет разнообразную информацию хосту, который регистрирует на сервере свой IP-адрес. Вся эта информация предоставляется сервером DHCP:

- IP-адрес
- Маска подсети
- Доменное имя
- Шлюз по умолчанию (маршрутизатор)
- DNS
- Информация WINS

Сервер DHCP способен поставлять дополнительные сведения, но перечисленные в списке данные являются наиболее типичными.

## Протоколы уровня взаимодействия хостов

Основной задачей уровня взаимодействия хостов является защита приложений более высокого уровня от проблем, связанных с работой сети. Протоколы такого уровня принимают данные от приложений и готовят их к отправке. В следующих разделах подробно рассматриваются два основных протокола подобного уровня.

### Протокол TCP

*Протокол TCP* (Transmission Control Protocol — протокол управления передачей данных) получает большие блоки информации от приложений и разбивает их на более мелкие сегменты. Затем он нумерует и упорядочивает сегменты, чтобы протокол TCP получателя мог снова собрать их в исходный блок. По окончании передачи сегментов TCP ожидает подтверждений о доставке каждого из них и повторно отправляет те сегменты, получение которых не подтверждено.

Перед передачей сегментов вниз по модели протокол TCP отправителя связывается с протоколом TCP получателя для установки соединения. Созданное соединение именуется *виртуальной цепью*. Такой вид взаимодействия называется *ориентированным на установление соединения*. На начальном этапе два протокола TCP договариваются между собой о количестве информации, которое может быть отправлено до получения подтверждения. После окончания согласования соединение считается установленным и начинается процесс надежного взаимодействия между приложениями.

TCP является полнодуплексным, ориентированным на установление соединения, надежным и точным протоколом. Наличие таких свойств и возможности проверки ошибок передачи делают TCP очень сложным и дорогостоящим. Поэтому его следует использовать в ситуациях, когда особенно важна надежность взаимодействия. Часто в этом нет необходимости, поскольку современные сети стали гораздо надежнее, чем на заре своего развития.

### Формат сегментов TCP

Более высокие уровни посылают протоколам транспортного уровня поток данных, поэтому покажем, как TCP сегментирует его, подготавливая к передаче на сетевой уровень. На сетевом уровне происходит маршрутизация сегментов по объединенной сети. Такие пакеты управляются на транспортном уровне принимающего хоста. Там происходит воссоздание потока данных для последующей отправки в приложения или протоколы верхних уровней.

На рис. 3.3 приведен формат сегмента TCP и поля в заголовке элемента данных TCP.

Длина заголовка TCP равна 20 байт. Поясним назначение полей сегмента TCP:

- **Порт источника:** номер порта хоста, посылающего данные.

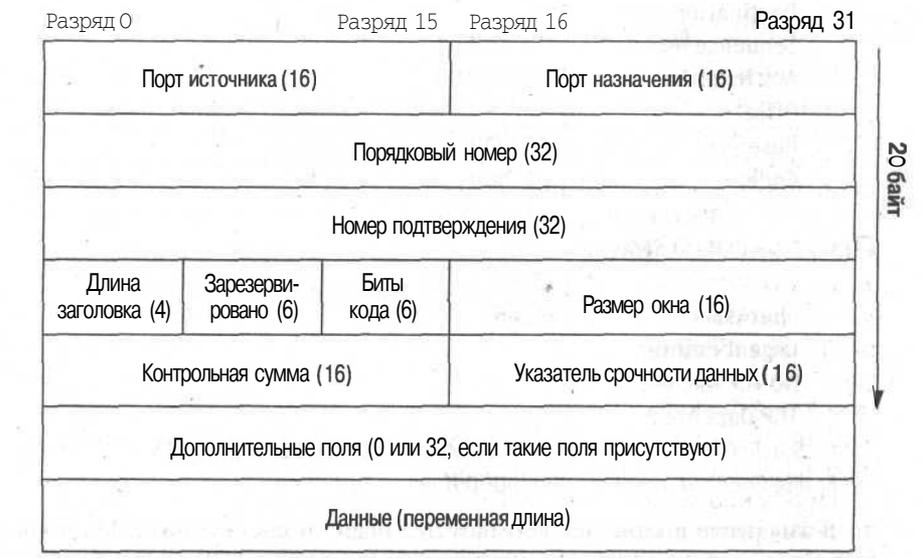


Рис. 3.3. Формат сегмента TCP

- **Порт назначения:** номер порта приложения, выставившего запрос к хосту назначения.
- **Порядковый номер:** используется для сборки сегментов в правильном порядке или для повторной передачи потерянных или поврежденных данных.
- **Номер подтверждения:** определяет номер ожидаемого октета данных.
- **Длина заголовка (HLEN):** равна числу 32-битовых слов в заголовке.
- **Зарезервировано:** всегда заполняется нулями.
- **Биты кода:** открывают или завершают сеанс связи.
- **Размер окна:** размер окна в октетах, согласованный с отправителем данных.
- **Контрольная сумма:** код CRC. TCP не доверяет более низким уровням и проверяет ошибки самостоятельно.
- **Указатель срочности данных:** указывает на конец времени срочности данных.
- » **Дополнительные поля:** здесь указывается максимальный размер сегмента TCP.
- **Данные:** данные, передаваемые на транспортный уровень протоколу TCP и содержащие заголовки более высоких уровней.

Рассмотрим сегмент TCP, перехваченный сетевым анализатором:

TCP — Transport Control Protocol

Source Port: 5973

```

Destination Port: 1223
Sequence Number: 1456389907
Ack Number: 1242056456
Offset: 5
Reserved: %000000
Code: %011000
 Ack is valid
 Push Request
Window: 61320
Checksum: 0x61ab
Urgent Pointer: 0
No TCP Options
TCP Data Area:
vL.5.+5.+5.+5 76 4c 19 35 11 2b 19 35 11 2b 19 35 11 2b 19 35 .+. 11 2b 19
Frame Check Sequence: 0x0d00000f

```

В листинге видны все упомянутые выше поля сегмента. По количеству этих полей не трудно заметить, что протокол TCP имеет большие накладные расходы. Разработчики приложений должны пользоваться протоколом TCP, когда необходима надежная доставка данных, но если нужно сократить накладные расходы, следует применять протокол UDP.

## Протокол UDP

*Протокол UDP* (User Datagram Protocol — протокол передачи пользовательских датаграмм) можно использовать вместо протокола TCP. UDP называют "тонким" протоколом, поскольку он более экономичен, занимает мало места и выполняет лишь часть функций, свойственных протоколу TCP.

Однако он вполне справляется с передачей информации, не требующей гарантированной доставки, и при этом использует значительно меньше сетевых ресурсов. (Протокол UDP описан в RFC 768.)

В некоторых ситуациях выгоднее применять протокол UDP, а не TCP. Вспомните протокол SNMP, наблюдающий за поведением сети, посылающий нерегулярные сообщения и создающий достаточно устойчивый поток предупреждений и сообщений об изменении состояния, особенно при работе в большой сети. Затраты на установление соединения, поддержку и закрытие соединения для каждого мелкого сообщения могли бы понизить производительность сети.

Кроме того, UDP имеет преимущество перед TCP в том случае, если надежность передачи обеспечивается на уровне приложений/процессов. Протокол NFS самостоятельно решает вопросы надежности, поэтому применение TCP непрактично и излишне. Однако решение об использовании протокола принимается разработчиком приложения, а не пользователем, который хотел бы ускорить передачу данных.

Протокол UDP получает блоки информации с более высоких уровней и разбивает их на сегменты. Каждому сегменту назначается порядковый

номер для последующей сборки в исходный блок у получателя. Однако UDP не упорядочивает сегменты и не заботится о последовательности их поступления к получателю. Он всего лишь нумерует и отправляет сегменты, сразу же забывая о них. UDP не проверяет, доставлены ли сегменты, и даже не допускает подтверждений, поэтому считается *ненадежным протоколом*. Это не означает, что протокол UDP неэффективен, просто он не имеет отношения к надежности.

Кроме того, протокол UDP не создает виртуальных цепей и не взаимодействует с получателем перед отправкой информации. Поэтому он называется *протоколом без установления соединения*. Поскольку UDP предполагает реализацию в приложении любого метода гарантированной (надежной) доставки, можно применять подобный метод. Разработчики приложений могут выбрать любой вариант из стека протоколов Интернета: TCP для надежной доставки или UDP для ускорения обмена.

### Формат сегмента UDP

Низкие затраты протокола UDP, не использующего окна и подтверждения, объясняются форматом его сегмента (см. рис. 3.4).

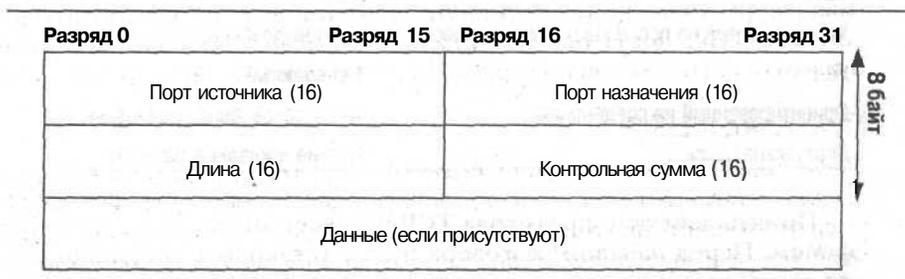


Рис. 3.4. Формат сегмента UDP

Сегмент UDP содержит следующие поля:

Порт источника определяет номер порта хоста, пославшего данные.

Порт назначения указывает номер порта приложения, запрошенного на хосте назначения.

Длина сегмента равна сумме длин заголовка и данных UDP.

Контрольную сумму формирует CRC для полей заголовка и данных UDP.

Данные — это информация с верхних уровней.

Как и TCP, протокол UDP не доверяет нижним уровням и создает контрольную сумму самостоятельно. Напомним, что поле контрольной последовательности кадра FCS содержит контрольную сумму.

Ниже приведен сегмент UDP, перехваченный сетевым анализатором:

UDP — User Datagram Protocol

Source Port: 1085

```

Destination Port: 5136
Length: 41
Checksum: 0x7a3c
UDP Data Area:
..Z.....00 01 5a 96 00 01 00 00 00 00 11 00 00 00
...C..2....C_C 2e 03 00 43 02 1e 32 0a 00 0a 00 80 43 00 80
Frame Check Sequence: 0x00000000

```

Обратите внимание на низкие затраты, а также попытайтесь найти порядковый номер, номер подтверждения и размер окна (все это отсутствует в сегменте UDP).

### Основные понятия, характеризующие протоколы уровня взаимодействия хостов

Приведем некоторые важные характеристики, которые помогут запомнить различия между протоколами TCP и UDP:

| TCP                                       | UDP                         |
|-------------------------------------------|-----------------------------|
| Упорядоченный по последовательным номерам | Неупорядоченный             |
| Надежный                                  | Ненадежный                  |
| Ориентированный на соединения             | Без установления соединения |
| Виртуальная цепь                          | Низкие накладные расходы    |

Понять действие протокола TCP поможет аналогия с обычным телефоном. Перед началом разговора нужно установить соединение с телефонным аппаратом нужного человека, что соответствует виртуальной цепи в протоколе TCP. Если в процессе разговора нужно срочно сообщить важную новость, то уместен вопрос: "Вы уже знаете об этом?". Такой вопрос похож на подтверждение (acknowledgment) протокола TCP. Периодически и по разным причинам люди спрашивают: "Слышите ли Вы меня?", а в конце разговора прощаются и кладут телефонную трубку. Аналогичные операции выполняются и в протоколе TCP.

Для протокола UDP уместна аналогия с почтовой открыткой. Для пересылки сообщения уже не нужно устанавливать соединение с другим человеком — достаточно написать послание на открытке и отнести ее на почту. Как и в протоколе UDP, почтовая служба не формирует соединение между отправителем и получателем. Сведения на открытках не очень важны (по крайней мере, речь не идет о жизни и смерти), поэтому не нужно подтверждать получение послания. Точно так же, в протоколе UDP не применяется подтверждение приема данных.

### Номера портов

Протоколы TCP и UDP должны использовать *номера портов* для взаимодействия с более высокими уровнями. Номера портов применяются для отслеживания различных взаимодействий, одновременно протекающих

в сети. Начальные номера портов динамически назначаются хостом-источником и обычно превышают 1023. В RFC 1700 перечислены номера так называемых общеизвестных портов.

Виртуальные цепи не используются приложениями с общеизвестными портами. Для них порты предоставляются случайным образом из определенного диапазона. Этим порты определяют хосты источника и назначения в сегменте TCP.

На рис. 3.5 показано применение номеров портов протоколами TCP и UDP.

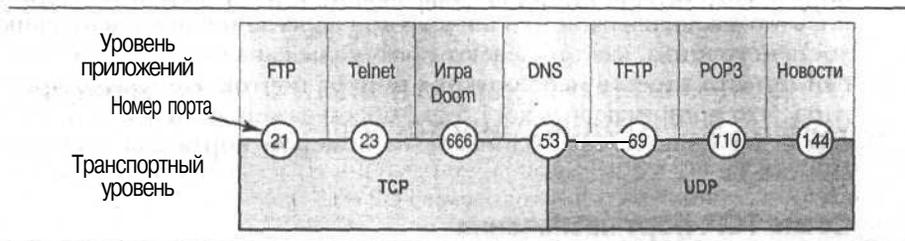


Рис. 3.5. Номера портов для протоколов TCP и UDP

Рассмотрим общепринятое назначение номеров портов:

- Номера ниже 1024 используются общеизвестными портами и определены в RFC 1700.
- Номера выше 1024 применяются более высокими уровнями для сеанса с другими хостами, а также протоколом TCP в качестве адресов источника и получателя в сегменте TCP.

**Сеанс TCP: порт источника**

Следующая информация получена с помощью анализатора протоколов Etherpeek, перехватившего сегмент TCP. Хост-источник установил в сегменте порт источника, равный 5973. Порт назначения равен 23, что указывает принимающему хосту на назначение устанавливаемого соединения (Telnet).

TCP - Transport Control Protocol

```

Source Port: 5973
Destination Port: 23
Sequence Number: 1456389907
Ack Number: 1242056456
Offset: 5
Reserved: %000000
Code: %011000
 Ack is valid
 Push Request
Window: 61320
Checksum: 0x61a6

```

```

Urgent Pointer: 0
No TCP Options
TCP Data Area:
VL.5+.5+.5+.5 76 4c 19 35 11 2b 19 35 11 2b 19 35 11 2b 19 35 +. 11 2b 19
Frame Check Sequence: 0x0d00000f

```

Из показанного листинга сеанса TCP видно, что номер порта источника сформирован хостом-источником. Это нужно для разделения сеансов с разными хостами-приемниками. Иначе сервер не будет знать, откуда поступила информация. Протокол TCP и верхние уровни не пользуются логической или аппаратной адресацией для идентификации хоста-источника, как это делают протоколы канального и сетевого уровней. Вместо адресов используются номера портов. Не трудно предположить, что принимающий хост будет обескуражен, если все остальные хосты будут пользоваться одинаковым номером порта для установления сеанса FTP.

### Сеанс TCP: порт назначения

В анализаторе протоколов мы видим только порты источника с номерами выше 1024 и порты назначения — общеизвестные номера. Покажем это в листинге, полученном в Etherpeek:

```

TCP - Transport Control Protocol
Source Port: 1144
Destination Port: 80 WorldWide Web HTTP
Sequence Number: 9356570
Ack Number: 0
Offset: 7
Reserved: %000000
Code: %000010
 Synch Sequence
Window: 8192
Checksum: 0x57E7
Urgent Pointer: 0
TCP Options:
 Option Type: 2 Maximum Segment Size
 Length: 4
 MSS: 536
 Option Type: 1 No Operation
 Option Type: 1 No Operation
 Option Type: 4
 Length: 2
 Opt Value:
No More HTTP Data
Frame Check Sequence: 0x43697363

```

Порт источника имеет номер выше 1024, но номер порта назначения равен 80 (т.е. служба HTTP). Сервер или принимающий хост могут при необходимости изменить порт назначения.

В листинге видно, что устройству назначения отправлен пакет синхронизации "syn". Последовательность пакетов syn указывает удаленному устройству назначения на необходимость создания сеанса.

### Сеанс TCP: подтверждение пакетов Syn

В следующем листинге показана процедура подтверждения пакета синхронизации. Фраза "Ack is valid" (запрос корректен) означает, что порт источника допустим и устройство соглашается создать виртуальную цепь с запросившим хостом.

```
TCP - Transport Control Protocol
Source Port: 80 World Wide Web HTTP
Destination Port: 1144
Sequence Number: 2873580788
Ack Number: 9356571
Offset: 6
Reserved: %000000
Code: %010010
 Ack is valid
 Synch Sequence
Window: 8576
Checksum: 0x5F85
Urgent Pointer: 0
TCPOptions:
 Option Type: 2 Maximum Segment Size
 Length: 4
 MSS: 1460
No More HTTP Data
Frame Check Sequence: 0x6E203132
```

В ответе сервера указан порт источника 80, а порт назначения 1144 был ранее установлен запросившим сеанс хостом.

## Протоколы уровня Интернета

Основной причиной существования уровня Интернета является необходимость маршрутизации и обеспечения единого сетевого интерфейса с протоколами более высоких уровней.

Ни один протокол более высоких и более низких уровней не занимается маршрутизацией. Эта сложная и важная процедура выполняется только на уровне Интернета. Второй функцией уровня Интернета является обеспечение единого сетевого интерфейса с протоколами более высоких уровней. При отсутствии этого уровня разработчики приложений были бы вынуждены включать в свои приложения собственные

средства взаимодействия с разными протоколами уровня доступа к сети, а это потребовало бы создания каждого приложения в нескольких версиях — для сетей Ethernet, Token Ring и т.д. С помощью протокола IP реализуется единый сетевой интерфейс с протоколами более высоких уровней, обеспечивающий совместную работу протокола IP и протоколов уровня доступа к сети.

Все другие протоколы этого и более высоких уровней используют протокол IP. Не забывайте о том, что все пути по модели проходят через протокол IP. Ниже рассматриваются протоколы уровня Интернета.

## Протокол IP

Уровень Интернета обеспечивается *протоколом IP* (Internet Protocol — протокол Интернета). Другие протоколы только помогают IP в создании "общей картины, где видно все", т.е. все устройства объединенной сети. Это возможно за счет присваивания всем компьютерам в сети программных (логических) адресов, называемых IP-адресами.

Протокол IP анализирует адрес каждого пакета. Затем по таблице маршрутизации принимается решение о направлении пакета в один из следующих участков, причем выбор основан на наилучшем пути достижения пакетом точки назначения. Протоколы сетевого уровня, находящиеся в модели ниже протокола IP, не могут просматривать всю сеть, поскольку действуют только на уровне физических связей (в локальных сетях).

Для идентификации сетевых устройств необходимо ответить на два вопроса. В какой сети находится устройство? И каков его идентификатор в этой сети? Ответом на первый вопрос является *программный*, или *логический*, *адрес* (в рамках аналогии с почтой — название улицы). Ответ на второй вопрос — *аппаратный адрес* (номер почтового ящика). Все хосты сети имеют логический идентификатор, который называется IP-адресом и который содержит важную закодированную информацию, значительно упрощающую маршрутизацию. (Протокол IP обсуждается в RFC 791.)

Протокол IP получает сегменты с уровня взаимодействия хостов и разбивает их на пакеты (датаграммы). На этом же уровне протокол IP получателя производит сборку сегментов из датаграмм. Каждая датаграмма содержит IP-адрес отправителя и IP-адрес получателя. Каждый маршрутизатор (устройство уровня 3), получивший датаграмму, принимает решение об ее перенаправлении с учетом IP-адреса получателя пакета.

На рис 3.6 представлен IP-заголовок, который показывает, что делает протокол во время передачи пользовательских данных с верхних уровней для отправки в удаленную сеть.

IP-заголовок состоит из следующих полей:

**Версия:** номер версии протокола IP

**Длина заголовка:** длина заголовка, выраженная в 32-разрядных словах

**Приоритет или тип обслуживания (ToS):** указывает способ обработки Датаграммы; первые три бита определяют приоритет.

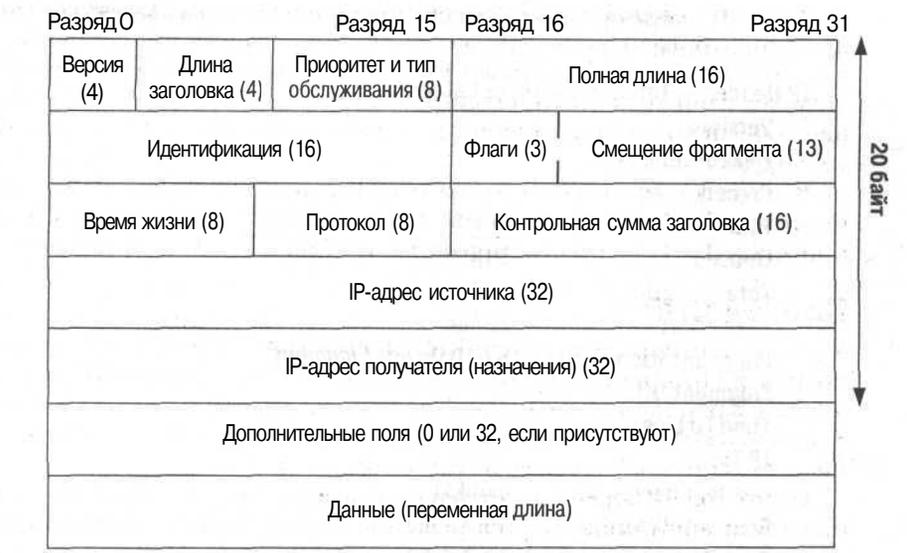


Рис. 3.6. IP-заголовок

**Полная длина:** длина всего пакета (с учетом заголовка и данных)

**Идентификация:** уникальное значение, идентифицирующее конкретный пакет IP

**Флаги:** определяют выполнение фрагментации

**Смещение фрагмента:** необходимо для фрагментации, когда пакет слишком велик для размещения в кадре. Дополнительно в Интернете обеспечивается значение максимального элемента передачи MTU (Maximum Transmission Unit)

**Время жизни TTL (Time to Live):** устанавливается во время исходной генерации пакета и определяет интервал существования этого пакета. Если пакет не достигает точки назначения за время TTL, то он отбрасывается (это сделано для предотвращения непрерывной циркуляции пакетов в сети).

**Протокол:** номер порта протокола более высокого уровня (порт TCP — 6, порт UDP — 17 в шестнадцатеричном виде)

**Контрольная сумма заголовка:** значение CRC только для заголовка

**IP-адрес источника:** 32-разрядный IP-адрес станции-отправителя

**IP-адрес получателя:** 32-разрядный IP-адрес станции, которой предназначен пакет

**Дополнительные поля:** используются для тестирования сети, отладки, обеспечения безопасности и т.д.

**Данные:** информация с верхних уровней

Пакет IP, перехваченный анализатором сети, показывает рассмотренные выше поля:

```

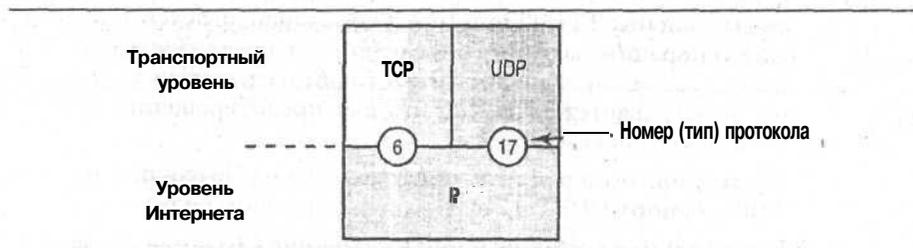
IP Header — Internet Protocol Datagram
Version: 4
Header Length: 5
Precedence: 0
Type of Service: %000
Unused: %00
Total Length: 187
Identifier: 22486
Fragmentation Flags: %010 Do not Fragment
FragmentOffset: 0
Time To Live: 60
IP Type: 0x06TCP
Header Checksum: 0xd031
Source IP Address: 10.7.1.30
Dest. IP Address: 10.7.1.10
No Internet Datagram Options

```

Обратите внимание, что в заголовке указаны логические адреса, т.е. IP-адреса.

Поле типа (обычно это поле протокола, но данный анализатор рассматривает его как поле типа) важно, поскольку, если заголовок не несет информации о протоколе для следующего уровня, протокол IP не поймет, что надо делать с данными.

На рис. 3.7 показано, как сетевой уровень взаимодействует с транспортным уровнем, когда требуется обработать данные с верхних уровней модели.



**Рис. 3.7.** Поле протокола в IP-заголовке

Поле протокола указывает IP на отправку данных либо в порт TCP с номером 6, либо в порт UDP с номером 17 (оба адреса в шестнадцатеричном виде). Однако указать можно только UDP или TCP, если информация является частью потока данных от службы или приложения верхнего уровня. В других случаях информация может предназначаться ICMP

(Internet Control Message Protocol), ARP (Address Resolution Protocol) или другому протоколу сетевого уровня.

В таблице 3.1 перечислены некоторые популярные протоколы, которые могут быть указаны в поле протокола.

**Таблица 3.1**

**Допустимые значения в поле протокола из заголовка IP**

| Протокол         | Номер протокола |
|------------------|-----------------|
| ICMP             | 1               |
| IGRP             | 9               |
| IPv6             | 41              |
| GRE              | 47              |
| IPX в IP         | 111             |
| Туннель уровня 2 | 115             |

### Протокол ICMP

*Протокол ICMP* (Internet Control Message Protocol — протокол управляющих сообщений Интернета) является управляющим протоколом, предоставляющим сообщения для протокола IP. Эти сообщения пересылаются в IP-датаграммах. Приложением к протоколу ICMP является RFC 1256 (*ICMP Router Discovery Messages* — сообщения ICMP об обнаружении маршрутизаторов), обеспечивающее хосты дополнительными средствами для обнаружения путей к шлюзам.

Маршрутизатор периодически рассылает оповещения о своем присутствии в сети, сообщая IP-адреса своих сетевых интерфейсов. Хосты прослушивают эти сообщения, чтобы получить информацию о маршрутизаторах. Требование маршрутизатора представляет собой запрос о немедленном оповещении, которое хосты могут расслать сразу же после загрузки. Ниже перечислены некоторые общие ситуации и сообщения протокола ICMP:

**Получатель недостижим** Если маршрутизатор не может послать IP-датаграмму дальше, он возвращает отправителю сообщение о недоступности получателя. Например, если маршрутизатор получил пакет, предназначенный сети, о которой маршрутизатор ничего не знает, он посылает ICMP-сообщение о недостижимости получателя на станцию-источник.

**Буфер заполнен** Это ICMP-сообщение маршрутизатор рассылает, если его буферная память, предназначенная для приема датаграмм, заполнилась.

**Число переходов** Для каждой IP-датаграммы определено число маршрутизаторов, которые она может пройти, или число *переходов*. Если лимит числа переходов исчерпан, но датаграмма еще не достигла получателя, последний маршрутизатор, принявший датаграмму, уничтожает ее. Затем этот маршрутизатор посылает отправителю ICMP-сообщение об уничтожении датаграммы.

**Пакет ping** Программа тестирования сети Packet Internet Groper использует эхо-сообщения протокола ICMP для проверки связи компьютеров в объединенной сети.

**Программа Traceroute** Использует тайм-аут сообщений ICMP для отслеживания путей пакетов в объединенной сети.

Следующие данные получены при расшифровке эхо-запроса ICMP, перехваченного сетевым анализатором. Заметьте, что хотя протокол ICMP работает на уровне Интернета, он использует IP для передачи запроса ping. Поле типа в IP-заголовке содержит 0x01h, указывая на протокол ICMP.

```

Flags: 0x00
Status: 0x00
Packet Length: 78
Timestamp: 14:04:25.967000 05/06/1998
Ethernet Header
Destination: 00:a0:24:6e:Of:a8
Source: 00:80:c7:a8:f0:3d
Protocol Type: 08-00 IP
IP Header - Internet Protocol Datagram
Version: 4
Header Length: 5
Precedence: 0
Type of Service: %000
Unused: %00
Total Length: 60
Identifier: 56325
Fragmentation Flags: %000
Fragment Offset: 0
Time To Live: 32
IP Type: 0x01 ICMP
Header Checksum: 0x2df0
Source IP Address: 100.100.100.2
Dest. IP Address: 100.100.100.1
No Internet Datagram Options
ICMP — Internet Control Messages Protocol
ICMP Type: 8 Echo Request
Code: 0
Checksum: 0x395c
Identifier: 0x0300
Sequence Number: 4352
ICMP Data Area:
abcdefghijklmnop 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d

```

qrstuvwabcdefghi 71 72 73 74 75 76 77 61 62 63 64 65 66  
 Frame Check Sequence: 0x00000000

В главе 1 мы говорили, что можно отслеживать типы кадров Ethernet. Доступны только поля аппаратного адреса назначения, аппаратного адреса источника и поле типа Ether-type. В кадрах в поле Ether-type можно указать тип Ethernet\_II (протокол SNAP тоже использует поле Ether-type, но только внутри поля 802.2 LLC, которое не присутствует в кадре).

### Протокол ARP

*Протокол АКР* (Address Resolution Protocol — протокол определения адреса) ищет аппаратный адрес хоста по известному IP-адресу. Когда протокол IP формирует датаграмму для отправки на другой компьютер, необходимо информировать протокол уровня доступа к сети (например, Ethernet или Token Ring) об аппаратном адресе точки назначения в локальной сети (а также информировать протокол верхнего уровня о IP-адресе назначения). Если IP не может найти аппаратный адрес хоста назначения в собственном кэше, для поиска этой информации используется протокол ARP.

Для выполнения заказа IP протокол ARP исследует локальную сеть за счет отправки широковещательной рассылки с запросом аппаратного адреса у компьютера с определенным IP-адресом, т.е. ARP транслирует программный адрес (IP) в аппаратный (например, в адрес сетевого адаптера Ethernet компьютера, получающего пакет). Этот аппаратный адрес называется физическим или адресом управления доступом к носителю MAC (media access control). На рис. 3.8 показана процедура обращения к локальной сети по протоколу ARP.

**ВНИМАНИЕ** ! ARP проводит разрешение IP-адресов в адреса Ethernet.

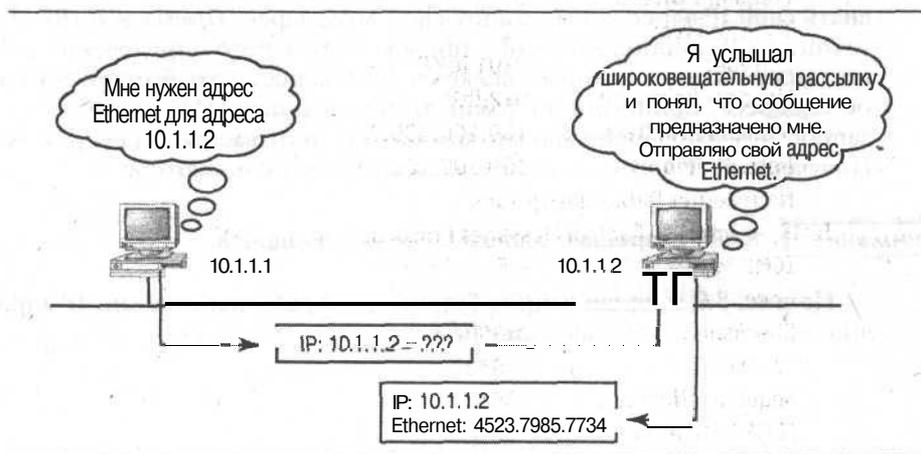


Рис. 3.8. Локальная широковещательная рассылка ARP



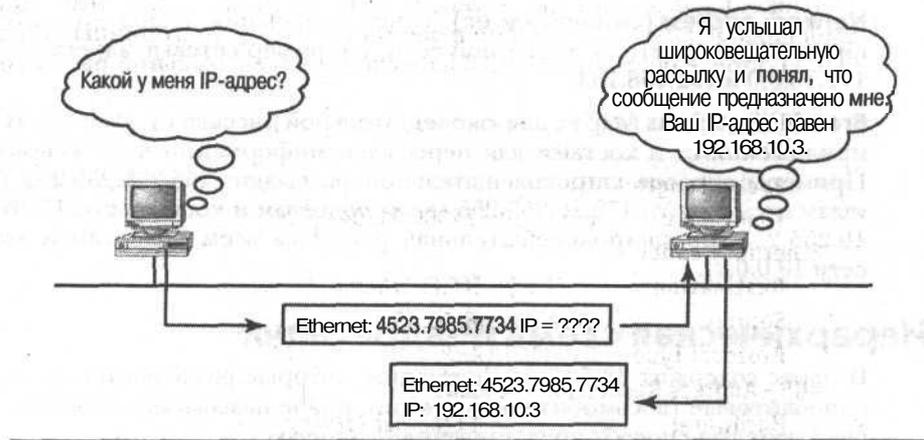


Рис. 3.9. Пример широковещательной рассылки RARP

## Адресация IP

Одной из наиболее важных тем при обсуждении стека TCP/IP является IP-адресация. *IP-адрес* представляет собой числовой идентификатор, присваиваемый каждому компьютеру сети IP. Он отражает расположение устройства в сети. Как говорилось ранее, IP-адрес является программным, а не аппаратным адресом — последний "зашит" в компьютере или плате сетевого интерфейса. IP-адреса позволяют хостам одной сети взаимодействовать с хостами другой сети вне зависимости от типов этих локальных сетей.

Перед подробным изучением IP-адресации нужно усвоить несколько базовых понятий и терминов.

**Т ВНИМАНИЕ** | Для понимания IP-адресации и выделения подсетей нужно знать правила преобразования десятичных чисел в двоичные, а также степени 2 (см. ниже).

## Термины IP-адресации

В этой главе мы будем постоянно пользоваться несколькими терминами, которые очень важны для понимания протокола Интернета (IP). Начнем с наиболее распространенных терминов:

**Bit (бит)** Один разряд, значение 1 или 0.

**Byte (байт)** 7 или 8 бит, в зависимости от использованной схемы проверки четности. В этой главе мы будем считать, что один байт всегда равен 8 бит.

**Octet (октет)** Всегда равен 8 бит (разрядам). Схема адресации Base-8.

**Network address** (сетевой адрес) Точка назначения, используемая в маршрутизации пакетов к удаленной сети, например сетевые адреса 10.0.0.0, 172.16.0.0 и 192.168.10.0.

**Broadcast address** (адрес широковещательной рассылки) Используется приложениями и хостами для пересылки информации всем узлам сети. Примеры адресов широковещательной рассылки: 255.255.255.255 (всем узлам всех сетей), 172.16.255.255 (всем подсетям и хостам сети 17.16.0.0), 10.255.255.255 (широковещательная рассылка всем подсетям и хостам сети 10.0.0.0).

## Иерархическая схема IP-адресации

IP-адрес содержит 32 бита информации, которые разделяются на четыре однобайтовые (восьмибитовые) секции, иначе называемые *октетами*. Существуют три способа представления IP-адресов:

- Представление десятичными числами, разделенными точками, например 172.16.30.56
- Двоичное представление, например 10101100.00010000.00011110.00111000
- Шестнадцатеричное представление, например AC 101E 38

Здесь показаны три формы представления одного и того же IP-адреса. Шестнадцатеричное представление используется реже, чем двоичное или десятичное, но все же применяется в некоторых программах, например, в реестре Windows IP-адреса компьютеров хранятся в шестнадцатеричном виде.

32-разрядный IP-адрес имеет иерархическую, а не плоскую (неиерархическую) структуру. Можно пользоваться любой схемой адресации, но иерархическая — более привлекательна. Достоинством плоской схемы является большое число возможных адресов, например, пространство 32-разрядных адресов, в каждой позиции которых может быть 0 или 1, содержит  $2^{32}$  или 4.2 миллиарда адресов. Неудобство такой схемы состоит в невозможности осуществления маршрутизации, именно по этой причине плоская схема не используется для IP-адресации. Если все адреса различны, маршрутизаторам Интернета придется запоминать адреса всех машин, подключенных к Интернету, что не позволит добиться эффективной маршрутизации, даже при использовании лишь части адресного пространства.

Поэтому для адресации выбрана иерархическая схема с тремя уровнями иерархии: сеть, подсеть и хост.

Для примера рассмотрим структуру телефонного номера. Первая его часть (код региона) описывает обширную географическую область. Вторая часть (префикс) сужает эту область до зоны действия локальной телефонной станции. Последний сегмент (собственно номер телефона) определяет конкретное соединение. При IP-адресации также используется схема с тремя уровнями. Вместо того чтобы рассматривать 32-разрядную комбинацию как единый идентификатор, в адресе выделяются части для адреса сети и для адреса узла.

|                |                                   |      |      |      |
|----------------|-----------------------------------|------|------|------|
| <b>Класс А</b> | Сеть                              | Хост | Хост | Хост |
| <b>Класс В</b> | Сеть                              | Сеть | Хост | Хост |
| <b>Класс С</b> | Сеть                              | Сеть | Сеть | Хост |
| <b>Класс D</b> | Многоадресная рассылка            |      |      |      |
| <b>Класс E</b> | Класс для исследовательских работ |      |      |      |

**Рис. 3.10.** Три класса сетей

### Адресация сетей

*Адрес сети* однозначно определяет сеть. В IP-адресах всех машин, подключенных к одной сети, указывается один и тот же адрес сети. Например, в IP-адресе 172.16.30.56 адресом сети может быть 172.16.

*Адрес узла* присваивается каждой машине сети. В отличие от адреса сети, описывающего группу устройств, адрес узла уникален и однозначно определяет конкретную машину сети. Адрес узла называют также *адресом хоста*. В приведенном примере адрес узла имеет вид 30.56.

Разработчики Интернета решили создать классы сетей, причем сеть относится к тому или иному классу в зависимости от своего размера. Для небольшого количества сетей со значительным числом узлов создан *класс А*. *Класс С* зарезервирован для многочисленных сетей с малым количеством узлов. К сетям *класса В* относятся сети промежуточного размера.

Способ разделения IP-адреса на поля адресов сети и узла определяется принадлежностью сети к тому или иному классу. На рис. 3.10 показаны особенности трех классов сетей.

Для эффективной маршрутизации разработчики Интернета определяют обязательную начальную часть адреса для каждого из классов. Например, зная, что адрес сети класса А всегда начинается с 0, маршрутизатор может ускорить передачу пакета по нужному маршруту после распознавания содержимого первого бита адреса. Рассмотрим схему адресов, позволяющую различать сети классов А, В и С.

### Диапазон сетевых адресов класса А

Создатели схемы IP-адресации установили, что первый бит первого байта сетевого адреса сети класса А всегда выключен (т.е. равен 0). Следовательно, адреса класса А находятся между 0 и 127.

Рассмотрим правила для этих чисел:

Охххххх: Если сначала выключить все остальные 7 бит, а затем включить их, то получится диапазон сетевых адресов класса А.

00000000=0

01111111=127

Итак, сеть класса А определяется тем, что первый октет имеет значение от 0 до 127. Иных значений не может быть (о незаконных адресах мы поговорим ниже).

**ВНИМАНИЕ** Для тех, кто неуверенно чувствует себя с операциями преобразования двоичных чисел в десятичные, предложим краткую справку об этом преобразовании.

### Преобразование из двоичного вида в десятичный

Перед изучением IP-адресации необходимо хорошо понимать правила преобразования чисел из двоичного вида в десятичный. Двоичные числа используют 8 разрядов для указания десятичного значения. Эти разряды (биты) располагаются справа налево, причем значение увеличивается вдвое в каждом разряде.

Пример значений битов 8-разрядного числа:

128 64 32 16 8 4 2 1

Пример преобразования из двоичного представления в десятичное:

|     |    |    |    |   |   |   |   |                   |
|-----|----|----|----|---|---|---|---|-------------------|
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | Двоичное значение |
| 0   | 0  | 1  | 0  | 0 | 1 | 1 | 0 | Двоичный байт     |

Сложим числа, разряды которых включены в двоичном представлении числа:

32  
4  
2  
=38

Для любого включенного разряда (значение 1) нужно добавить "вес" соответствующего бита. Рассмотрим еще один пример:

01010101=85  
64  
16  
4  
1  
=85

Другие примеры преобразования:

00001111=15  
10001100=140  
11001100=204

Можно запомнить значения согласно следующему списку, который пригодится в упражнениях по выделению подсетей:

00000000=0  
 10000000=128  
 11000000=192  
 11100000=224  
 11110000=240  
 11111000=248  
 11111100=252  
 11111110=254  
 11111111=255

### Диапазон сетевых адресов класса В

В сетях класса В спецификация RFC предписывает, что всегда должен быть включен первый бит первого байта, однако второй бит должен быть выключен. Если выключить, а затем включить остальные шесть разрядов, то мы получим диапазон для сетей В:

10000000=128  
 10111111=191

Следовательно, сети класса В имеют в первом байте значения от 128 до 191.

### Диапазон сетевых адресов класса С

В сетях класса С спецификация RFC предписывает, что всегда должны быть включены два первых бита первого октета. Найдем диапазон для сети класса С преобразованием из двоичного вида в десятичный:

11000000=192  
 11011111=223

Следовательно, если начало IP-адреса находится между 192 и 223, то это адрес сети класса С.

### Диапазоны сетевых адресов классов D и E

Адреса в диапазоне между 224 и 255 зарезервированы для сетей классов D и E. Класс D используется для многоадресных рассылок, а класс E — для исследовательских разработок. Далее мы не будем возвращаться к этим классам адресов.

### Диапазоны сетевых адресов для специального применения

Некоторые IP-адреса зарезервированы для специальных целей и сетевые администраторы не могут присвоить их узлам своих сетей. В таблице 3.2 перечислены некоторые специальные адреса и причины их попадания в список исключений.

**Таблица 3.2**  
**Зарезервированные IP-адреса**

| Адрес                                     | Функция                                                                                                                                        |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Сетевой адрес из всех нулей               | Означает "эта сеть или сегмент".                                                                                                               |
| Сетевой адрес из всех единиц              | Означает "все сети".                                                                                                                           |
| Сеть 127.0.0.1                            | Зарезервирована для кольцевого тестирования. Предназначена для сетевого узла, который может послать пакет себе без генерации сетевого трафика. |
| Адрес узла из всех нулей                  | Означает "этот узел".                                                                                                                          |
| Адрес узла из всех единиц                 | Означает "все узлы" определенной сети, например 128.2.255.255 показывает "все узлы сети 128.2 (адреса класса B)".                              |
| Весь IP-адрес из нулей                    | Используется маршрутизаторами Cisco для указания пути по умолчанию.                                                                            |
| Весь IP-адрес из единиц (255.255.255.255) | Широковещательная рассылка по всем узлам текущей сети, иногда называется "широковещательной рассылкой по всем единицам".                       |

### Адреса класса А

В IP-адресе сетей класса А первый байт занимает адрес сети, а в трех последующих байтах размещается адрес узла. Формат IP-адреса сети класса А:

Сеть.Узел.Узел.Узел

Например, в IP-адресе 49.22.102.70 адрес сети равен 49, а адрес узла — 22.102.70. Каждая машина этой сети должна иметь адрес сети, равный 49.

Адрес сети класса А имеет длину 1 байт, причем его первый бит зарезервирован, но доступны оставшиеся семь разрядов. Это означает, что можно создать не более 128 сетей класса А. Почему? Потому что каждый из семи оставшихся битов может принимать значение 0 или 1, т.е. существует  $2^7$  или 128 различных комбинаций.

Однако было решено, что нулевой адрес сети (0000 0000) резервируется для обозначения маршрута, выбранного по умолчанию (см. таблицу 3.2). Однако из-за того, что нулевой адрес зарезервирован, диапазон становится уже: от 1 до 127. В результате реальное число сетей класса А равно  $128 - 2$ , т.е. 126.

Под адрес узла в IP-адресе сетей класса А отведено 3 байта (24 разряда). В них можно разместить  $2^{24}$  или 16 777 216 различных двоичных комбинаций или адресов узлов. Поскольку адреса, состоящие только из нулей и только из единиц, зарезервированы, точное число узлов в сети класса А составляет  $2^{24} - 2 = 16\,777\,214$ .

### **Допустимые значения идентификаторов хостов в сети класса А**

Рассмотрим пример определения допустимого идентификатора хоста для сетевого адреса класса А:

10.0.0.0 В сетевом адресе выключены все разряды, определяющие идентификатор хоста.

10.255.255.255 Все разряды для хостов в широковещательном адресе.

Допустимое количество хостов находится в диапазоне между сетевым адресом и адресом широковещательной рассылки: от 10.0.0.1 до 10.255.255.254. Заметим, что допустимы идентификаторы хостов из всех нулей и 255. Для подсчета количества доступных адресов хостов нужно, помнить, что разряды хоста не могут быть все вместе включены или выключены.

### **Адреса класса В**

В IP-адресе сетей класса В первые два байта занимает адрес сети, а в двух последующих байтах размещается адрес узла. Формат IP-адреса сети класса В:

Сеть. Сеть.Узел.Узел

Например, в IP-адресе 172.16.30.56 адрес сети равен 172.16, а адрес узла — 30.56.

Для адреса сети, состоящего из 16 разрядов, имеется  $2^{16}$  возможных комбинаций. Однако разработчики Интернета решили, что адрес сети класса В должен начинаться с комбинации 10. Поэтому свободными для формирования адреса остаются лишь 14 бит; это означает, что может существовать  $2^{14}$  или 16 384 сетей класса В.

Под адрес узла в IP-адресе сетей класса В отведено 2 байта. Поскольку адреса, состоящие только из нулей и только из единиц, зарезервированы, точное число узлов в сети класса В равно  $2^{16} - 2 = 65\,534$ .

### **Допустимые значения идентификаторов хостов в сети класса В**

Рассмотрим пример определения допустимого идентификатора хоста для сетевого адреса класса В:

172.16.0.0 В сетевом адресе выключены все разряды, определяющие идентификатор хоста.

172.16.255.255 Все разряды для хостов в широковещательном адресе.

Допустимое количество хостов находится в диапазоне между сетевым адресом и адресом широковещательной рассылки: от 172.16.0.1 до 172.16.255.254.

### **Адреса класса С**

Первые три байта в IP-адресе сетей класса С занимает адрес сети, и всего один байт остается для адреса узла. Формат IP-адреса сети класса С:

Сеть.Сеть.Сеть.Узел

Например, в IP-адресе 192.168.100.102 адрес сети равен 192.168.100, а адрес узла – 102.

Первые три разряда адреса сети класса С занимает комбинация 110. Поэтому для формирования адреса остается лишь  $24 - 3 = 21$  разряд. Таким образом, может существовать  $2^{21}$  или 2 097 152 сетей класса С.

Под адрес узла в IP-адресе сетей класса С отведен 1 байт. Следовательно, в каждой сети класса С может быть  $2^8 - 2 = 254$  узла.

### **Допустимые значения идентификаторов хостов в сети класса С**

Рассмотрим пример определения допустимого идентификатора хоста для сетевого адреса класса С:

**192.168.100.0** В сетевом адресе выключены все разряды, определяющие идентификатор хоста.

**192.168.100.255** Все разряды для хостов в широковещательном адресе.

Допустимое количество хостов находится в диапазоне между сетевым адресом и адресом широковещательной рассылки: от 192.168.100.1 до 192.168.100.254.

## **Выделение подсетей**

Выше мы обсудили присвоение адресов и определение количества хостов в сетях класса А, В и С. Однако таким способом можно указать только одну сеть. Что делать, если получен один сетевой адрес, но нужно создать на его основе шесть сетей? Следует использовать *выделение подсетей* (subnetting), т.е. деление одной большой сети на несколько маленьких.

Существуют разные причины для выделения подсетей, наиболее важными являются:

**Сокращенный сетевой трафик** Все ощутят снижение трафика любого типа. При этом сети остаются однотипными. Без маршрутизаторов трафик грозит почти полностью затормозить работу сети. А при их использовании большая часть трафика остается в локальной сети; через маршрутизатор будут передаваться лишь пакеты, предназначенные потребителям из других сетей. Кроме того, маршрутизаторы формируют домены широковещательных рассылок, которые сокращают распространение таких рассылок по сетевым сегментам.

**Оптимизация производительности сети** Это премия за сокращение сетевого трафика.

**Упрощенное управление** В группе небольших сетей, связанных друг с другом, гораздо легче выявить и решить возникающие проблемы, чем в одной большой сети.

**Упрощенный охват больших географических пространств** Связи региональных сетей намного медленнее и более дорогостоящие по сравнению со связями локальных сетей. Объединение многочисленных мелких сетей делает всю систему более эффективной.

Для создания подсетей используются разряды IP-адреса. Они предназначены для хостов, которые резервируются для определения адреса подсети. Сокращается число разрядов для хостов, поэтому чем больше будет подсетей, тем меньше разрядов доступно для указания идентификаторов хостов.

Мы рассмотрим выделение подсетей в пространстве адресов класса С, однако сначала нужно установить требования и выработать план этого процесса. Следует выяснить следующее:

1. Определите требуемое число сетевых идентификаторов:
  - A. Один для каждой подсети
  - B. Один для каждого соединения с региональной сетью
2. Определите требуемое число идентификаторов хостов для подсети:
  - A. Один для каждого TSP/IP-хоста
  - B. Один для каждого интерфейса маршрутизатора
3. С учетом предыдущих ответов, создайте:
  - A. Одну маску подсети для всей сети
  - B. Единственный идентификатор подсети для каждого физического сегмента
  - C. Диапазон идентификаторов хостов для каждой подсети

#### Степени числа 2

Степени числа 2 широко используются в процессе выделения подсетей IP. Ниже приведен список часто используемых степеней, который рекомендуется запомнить:

$$2^1=2$$

$$2^2=4$$

$$2^3=8$$

$$2^4=16$$

$$2^5=32$$

$$2^6=64$$

$$2^7=128$$

$$2^8=256$$

### Маска подсети

При применении схемы адресации с подсетями каждая машина сети должна знать, какая часть адреса хоста занята адресом подсети. Для этого на каждом компьютере создается *маска подсети*. Это 32-разрядное **число**, которое позволяет получателю пакета IP отделить идентификатор сети в IP-адресе от идентификатора хоста.

Администратор сети создает 32-разрядную маску подсети, состоящую из 0 и 1. Единицы в маске подсети помечают позиции, относящиеся к адресам сети и подсети.

Не во всех сетях нужны подсети, т.е. иногда используются маски подсети по умолчанию (иными словами, в такой сети нет адресов подсетей). В таблице 3.3 показаны маски подсетей по умолчанию для классов А, В и С. Их нельзя изменить. Например, в классе В недопустима маска 255.0.0.0. Хосты будут считать этот адрес неправильным и даже не позволят ввести его. В сети класса А нельзя изменить первый байт маски подсети — как минимум, маска должна быть 255.0.0.0. Аналогично, недопустимо присваивание значения 255.255.255.255, поскольку это широко-вещательный адрес "все единицы". Адрес в классе В обязан начинаться с 255.255.0.0, а в классе С - с 255.255.255.0.

**Таблица 3.3.**  
**Маски подсетей по умолчанию**

| Класс | Формат              | Маска по умолчанию |
|-------|---------------------|--------------------|
| А     | Узел.Узел.Узел.Узел | 255.0.0.0          |
| В     | Сеть.Сеть.Узел.Узел | 255.255.0.0        |
| С     | Сеть.Сеть.Сеть.Узел | 255.255.255.0      |

### Выделение подсетей в классе С

Существуют разные способы выделения подсетей, среди которых можно выбрать наиболее подходящий для себя. Сначала мы обсудим двоичный метод, а затем познакомимся с другим способом выделения подсетей.

В адресном пространстве класса С для определения хостов доступны только 8 разрядов. Биты подсети отсчитываются слева направо без пропусков разрядов. Масками подсетей могут быть:

10000000=128  
 11000000=192  
 11100000=224  
 11110000=240  
 11111000=248  
 11111100=252  
 11111110=254

Спецификация RFC не разрешает использовать для подсетей только один разряд, поскольку он всегда будет либо включен, либо выключен, а это недопустимо. Следовательно, первой правильной маской подсети будет 192, а последней — 252, поскольку нужно не менее двух разрядов для указания хостов.

#### Двоичный метод: Выделение подсетей в классе С

Рассмотрим выделение подсетей в адресном пространстве класса С с помощью двоичного метода. Сначала следует выявить первую доступную маску подсети, которая заимствует два разряда. Например, можно использовать 255.255.255.192.

192=11000000 Два разряда применяются для выделения подсетей, 6 разрядов определяют хосты в каждой подсети. Какими будут подсети? Поскольку разряды подсети не могут быть одновременно включены или выключены, допустимы только две подсети:

01000000=64 (все разряды хостов выключены)

или

10000000=128 (все разряды хостов выключены)

Корректные адреса хостов находятся между подсетями, за исключением вариантов, когда одновременно включены или выключены все разряды хостов.

Для выявления адресов хостов нужно сначала выключить все разряды хостов в адресе, а затем включить их, чтобы найти широковещательный адрес подсети. Допустимые адреса хостов располагаются между двумя полученными адресами. В таблице 3.4 показана подсеть 64, диапазон хостов и адрес широковещательной рассылки.

**Таблица 3.4.**  
Подсеть 64

| Подсеть | Хост       | Описание                                  |
|---------|------------|-------------------------------------------|
| 01      | 000000=64  | Сеть (первая операция)                    |
| 01      | 000001=65  | Первый допустимый хост                    |
| 01      | 111110=126 | Последний допустимый хост                 |
| 01      | 111111=127 | Широковещательный адрес (вторая операция) |

В таблице 3.5 показана подсеть 128, диапазон хостов и адрес широковещательной рассылки.

**Таблица 3.5.**  
Подсеть 128

| Подсеть | Хост       | Описание                  |
|---------|------------|---------------------------|
| 10      | 000000=128 | Адрес подсети             |
| 10      | 000001=129 | Первый допустимый хост    |
| 10      | 111110=190 | Последний допустимый хост |
| 10      | 111111=191 | Широковещательный адрес   |

Операция проста, но в наших примерах рассмотрен только случай с двумя разрядами для подсети. Что делать, когда нужно 9, 10 или даже 20 разрядов? Рассмотрим альтернативный метод, пригодный для выделения большого количества подсетей.

## Альтернативный метод: Выделение подсетей в классе С

Установив маску подсети, следует определить количество подсетей, хостов и широковещательные адреса. Для этого нужно ответить на несколько простых вопросов:

1. Сколько подсетей формирует данная маска?
2. Сколько хостов будет в каждой подсети?
3. Каковы правильные подсети?
4. Каковы правильные хосты в каждой подсети?
5. Какие широковещательные адреса в подсетях?

Для ответов на эти вопросы нужно помнить степени числа 2 (см. выше). Приведем примеры ответов на поставленные вопросы:

1. Сколько подсетей?  $2^x - 2 =$  количество\_подсетей, где  $X$  равно количеству маскируемых разрядов (т.е. единиц). Например, для 11000000 мы имеем  $2^2 - 2$ , т.е. 2 подсети.
2. Сколько хостов в подсетях?  $2^x - 2 =$  количество\_хостов\_в\_подсети, где  $X$  равно количеству немаскируемых разрядов (т.е. нулей). Например, для 11000000 мы имеем  $2^6 - 2$ , т.е. 62 хоста в подсети.
3. Каковы корректные подсети?  $256\text{-маска\_подсети} =$  базовое\_количество. Например,  $256 - 192 = 64$ .
4. Каковы корректные хосты? Количество хостов равно разности между подсетями, минус "все нули" и "все единицы".
5. Каков широковещательный адрес в каждой подсети? Адрес широковещательной рассылки получается после включения всех разрядов хостов, поэтому легко вычисляется для любой подсети.

Чтобы лучше понять рассмотренные выше расчеты, приведем несколько примеров.

### Примеры выделения подсетей в классе С

Рассмотрим несколько примеров выделения подсетей в классе С с помощью рассмотренных выше методов. Мы будем исходить из первой маски подсети для класса С и вычислим все характеристики подсетей. Далее мы приведем примеры для классов А и В.

#### Пример 1: 255.255.255.192

Начнем с адреса подсети в классе С, который использовался в предыдущем примере (255.255.255.192), чтобы показать преимущество альтернативного метода над двоичным. В этом примере мы используем сетевой адрес 192.168.10.0 и маску подсети 255.255.255.192.

192.168.10.0=Сетевой адрес

255.255.255.192=Маска подсети

Не трудно получить ответы на пять основных вопросов:

1. Сколько подсетей? В 192 включены два разряда (11000000), поэтому  $2^2 - 2 = 2$ . (вычитание 2 связано с некорректными по определению адресами, в которых включены или выключены все разряды подсети).
2. Сколько хостов в подсети? Выключено 6 разрядов хоста (11000000), следовательно,  $2^6 - 2 = 62$  хоста.
3. Какова правильная подсеть?  $256 - 192 = 64$  и мы получаем первую подсеть, а также базовое количество (переменную). Далее следует складывать эту переменную до тех пор, пока не будет достигнута маска подсети.  $64 + 64 = 128$ .  $128 + 64 = 192$ , но это уже некорректная маска, поскольку в ней включены все разряды подсети. Итак, получаем две подсети: 64 и 128.
4. Каковы правильные хосты? Они находятся между подсетями. Проще всего выявить их адреса, записав адреса подсетей и адреса широковещательных рассылок.
5. Какие широковещательные адреса в подсетях? Это число находится перед следующей подсетью и имеет включенными все биты хостов. В таблице 3.6 показаны подсети 64 и 128, диапазон хостов в каждой из них и широковещательные адреса в каждой подсети.

**Таблица 3.6.**  
**Диапазоны подсетей 64 и 128**

| Первая подсеть | Вторая подсеть | Описание                                      |
|----------------|----------------|-----------------------------------------------|
| 64             | 128            | Подсеть (первая операция)                     |
| 65             | 129            | Первый хост (адреса хостов вычисляются позже) |
| 126            | 190            | Последний хост                                |
| 127            | 191            | Широковещательный адрес (вторая операция)     |

Мы получили те же ответы, что и в двоичном методе, но нам уже не пришлось прибегать к преобразованию числа из двоичного вида в десятичный. Однако этот метод не всегда будет проще двоичного. Для первой подсети, где только два разряда подсети, двоичный метод будет удобнее. Возможно, следует хорошо изучить оба метода, поскольку часто приходится выполнять вычисления о подсетях в уме.

**Пример 2: 255.255.255.224**

Рассмотри сетевой адрес 192.168.10.0 и маску подсети 255.255.255.224.

192.168.10.0=Сетевой адрес

255.255.255.224=Маска подсети

1. Сколько подсетей? 224 равно 11100000, следовательно,  $2^3 - 2 = 6$ .
2. Сколько хостов?  $2^5 - 2 = 30$ .

3. Сколько корректных подсетей?  $256-224=32$ .  $32+32=64$ .  $64+32=96$ .  $96+32=128$ .  $128+32=160$ .  $160+32=192$ .  $192+32=224$ , но это уже недопустимая подсеть для нашей маски (включены все разряды подсети). Следовательно, мы имеем подсети 32, 64, 96, 128, 160 и 192.

#### 4. Каковы правильные хосты?

- 5: Широковещательные адреса имеются в каждой подсети?

Для ответов на четвертый и пятый вопросы нужно сначала записать подсети и широковещательные адреса (это будет число, стоящее перед следующей подсетью). Затем можно указать адреса хостов. В таблице 3.7 показаны все подсети для маски 255.255.255.224 в классе C.

**Таблица 3.7.**

**Маска подсети 255.255.255.224 в классе C**

| Подсеть 1 | Подсеть 2 | Подсеть 3 | Подсеть 4 | Подсеть 5 | Подсеть 6 | Описание                |
|-----------|-----------|-----------|-----------|-----------|-----------|-------------------------|
| 32        | 64        | 96        | 128       | 160       | 192       | Адрес подсети           |
| 33        | 65        | 97        | 129       | 161       | 193       | Первый хост             |
| 62        | 94        | 126       | 158       | 190       | 222       | Последний хост          |
| 63        | 95        | 127       | 159       | 191       | 223       | Широковещательный адрес |

#### **Пример 3: 255.255.255.240**

Рассмотрим еще один пример:

192.168.10.0=Номер сети

255.255.255.240=Маска подсети

- 240 равно 11110000 в двоичном виде.  $2^4 - 2 = 14$  подсетей.
- Первые разряды хостов или  $2^4 - 2 = 14$ .
- $256-240=16$ .  $16+16=32$ .  $32+16=48$ .  $48+16=64$ .  $64+16=80$ .  $80+16=96$ .  $96+16=112$ .  $112+16=128$ .  $128+16=144$ .  $144+16=160$ .  $160+16=176$ .  $176+16=192$ .  $192+16=208$ .  $208+16=224$ .  $224+16=240$  является нашей маской подсети, поэтому данный вариант некорректен. Следовательно, мы имеем подсети 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208 и 224.
- Каковы правильные хосты?
- Каковы широковещательные адреса в подсетях?

Для ответа на вопросы 4 и 5 заполним таблицу, где отмечены подсети, хосты и широковещательные адреса. Сначала найдем широковещательные адреса в каждой подсети, а затем выясним адреса хостов.

|                         |    |    |    |    |    |     |     |     |     |            |     |     |     |     |
|-------------------------|----|----|----|----|----|-----|-----|-----|-----|------------|-----|-----|-----|-----|
| Подсеть                 | 16 | 32 | 48 | 64 | 80 | 96  | 112 | 128 | 144 | 160        | 176 | 192 | 208 | 224 |
| Первый хост             | 17 | 33 | 49 | 65 | 81 | 97  | 113 | 129 | 145 | 161        | 177 | 193 | 209 | 225 |
| Последний хост          | 30 | 46 | 62 | 78 | 94 | 110 | 126 | 142 | 158 | <b>174</b> | 190 | 206 | 222 | 238 |
| Широковещательный адрес | 31 | 47 | 63 | 79 | 95 | 111 | 127 | 143 | 159 | 175        | 191 | 207 | 223 | 239 |

**Пример 4: 255.255.255.248**

Продолжим серию наших примеров:

192.168.10.0=Сетевой адрес

255.255.255.248=Маска подсети

1. 248 в двоичном виде равно 11111000.  $2^5 - 2 = 30$  подсетей.
2.  $2^3 - 2 = 6$  хостов.
3. 256 - 248 = 8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232 и 240.
4. Сначала найдем в п.5 широковещательные адреса, а затем вернемся к п. 4 и вычислим адреса хостов.
5. Как и раньше, адрес широковещательной рассылки в подсети мы вычисляем как число, стоящее перед адресом следующей подсети.

В таблице показаны подсети (только три первые и три последние), хосты и широковещательные адреса в подсетях для маски 255.255.255.248 в классе С.

|                         |    |    |    |     |     |     |
|-------------------------|----|----|----|-----|-----|-----|
| Подсеть                 | 8  | 16 | 24 | 224 | 232 | 240 |
| Первый хост             | 9  | 17 | 25 | 225 | 233 | 241 |
| Последний хост          | 14 | 22 | 30 | 230 | 238 | 246 |
| Широковещательный адрес | 15 | 23 | 31 | 231 | 239 | 247 |

**Пример 5: 255.255.255.252**

192.168.10.0=Сетевой номер

255.255.255.252=Маска подсети

1. 62.
2. 2.
3. 4, 8, 12 и т.д. до 248.
4. Сначала найдем в п.5 широковещательные адреса, а затем вернемся к п. 4 и вычислим адреса хостов.
5. Как и раньше, адрес широковещательной рассылки в подсети мы вычисляем как число, стоящее перед адресом следующей подсети.

В таблице показаны подсети (только три первые и три последние), хосты и широковещательные адреса в подсетях для маски 255.255.255.252 в классе С.

|                         |   |    |    |     |     |     |
|-------------------------|---|----|----|-----|-----|-----|
| Подсеть                 | 4 | 8  | 12 | 240 | 244 | 248 |
| Первый хост             | 5 | 9  | 13 | 241 | 245 | 249 |
| Последний хост          | 6 | 10 | 14 | 242 | 246 | 250 |
| Широковещательный адрес | 7 | 11 | 15 | 243 | 247 | 251 |

### Пример 6: 255.255.255.128

В предыдущих примерах мы не пользовались только одним разрядом для подсети, поскольку считали этот вариант незаконным. Однако нет правил без исключений. Такая маска вполне допустима, когда нужны две подсети с 126 хостами в каждой. Наши стандартные пять вопросов уже не помогут вычислить характеристики подсетей, поэтому нужен другой способ. Сначала следует ввести глобальную конфигурационную команду `ip subnet-zero`, чтобы узнать, какие маршрутизаторы нарушают правило и используют одноразрядную маску.

Поскольку 128 равно 1000000 в двоичном виде, для выделения подсетей доступен только один разряд. Соответствующий бит может быть включен или выключен, поэтому присутствуют две подсети: 0 и 128. Можно выяснить количество подсетей, проанализировав десятичное значение в четвертом октете. Ниже показана таблица для двух подсетей, диапазонов хостов и широковещательных адресов при маске 255.255.255.128 для класса С.

|                         |     |     |
|-------------------------|-----|-----|
| Подсеть                 | 0   | 128 |
| Первый хост             | 1   | 129 |
| Последний хост          | 126 | 254 |
| Широковещательный адрес | 127 | 255 |

Итак, если мы получаем IP-адрес 192.168.10.5 при маске подсети 255.255.255.128, значит это подсеть 0 и разряд с весом 128 должен быть выключен. Если же IP-адрес равен 192.168.10.189, то разряд с весом 128 должен быть включен, а хост будет находиться в подсети 128. Мы еще вернемся к исключению из общего правила.

### Выделение подсетей класса С в уме

Можно выполнить расчеты при выделении подсетей в уме, причем сделать это несложно. Покажем эти расчеты на примере:

192.168.10.33=Сетевой адрес  
255.255.255.224=Маска подсети

Сначала определим подсеть и адрес широковещательной рассылки для указанного IP-адреса. Для этого нужно ответить на третий вопрос нашей анкеты с пятью вопросами.  $256-224=32$ .  $32+32=64$ . Готово! Адрес подсети падает между двумя подсетями и обязан быть частью подсети 192.168.10.32. Следующей подсетью станет 64, поэтому адрес широковещательной рассылки равен 63 (широковещательный адрес подсети всегда стоит перед адресом следующей подсети). Диапазон хостов: 10.33 — 10.62.

Рассмотрим еще один пример устного вычисления. Для сети класса C мы имеем:

192.168.10.33=Сетевой адрес  
255.255.255.240=Маска подсети

Членом какой сети будет указанный IP-адрес и каким будет адрес широковещательной рассылки?  $256-240=16$ .  $16+16=32$ .  $32+16=48$ . Адрес хоста находится между подсетями 32 и 48. Следовательно, подсеть — 192.168.10.32, а широковещательный адрес — 47. Допустимый диапазон хостов равен 33 — 46.

Завершив обсуждение выделения подсетей в классе C, можно перейти к классу B.

## Выделение подсетей в классе B

Сначала рассмотрим все допустимые маски подсети в классе B. Заметим, что вариантов будет больше, чем для адресного пространства класса C.

255.255.128.0  
255.255.192.0  
255.255.224.0  
255.255.240.0  
255.255.248.0  
255.255.252.0  
255.255.254.0  
255.255.255.0  
255.255.255.128  
255.255.255.192  
255.255.255.224  
255.255.255.240  
255.255.255.248  
255.255.255.252

В сетях класса B для адреса хоста доступны 16 разрядов, т.е. можно использовать для подсетей 14 разрядов, оставив два разряда для адресации хостов.

Обратите внимание на шаблон в значениях подсетей. Для работы с шаблоном следует запомнить правила преобразования их из двоичного вида в десятичный. Поскольку биты маски подсети отсчитываются слева

направо без пропусков, числа будут одинаковыми. Это следует запомнить.

Процесс выделения подсетей в классе В похож на выделение в классе С, но доступно больше разрядов для хостов. Можно пользоваться теми же числами, что и для класса С, но добавить в четвертом октете к сетевой части адреса или 255 к части ширококвещательного адреса. Ниже показаны диапазоны хостов для двух подсетей в классе В.

16.0            32.0  
16.255        32.255

Добавьте между этими числами корректные хосты и все будет готово.

### Примеры выделения подсетей в классе В

Рассмотрим несколько примеров выделения подсетей в адресном пространстве класса В.

#### Пример 1: 255.255.192.0

172.16.0.0=Сетевой адрес

255.255.192.0=Маска подсети

1.  $2^2 - 2 = 2$ .
2.  $2^{14} - 2 = 16\ 382$ .
3.  $256 - 192 = 64$ .  $64 + 64 = 128$ .
4. Сначала определим ширококвещательный адрес в п. 5, а затем выполним п. 4 для выявления адресов хостов.
5. **Ширококвещательный** адрес в каждой подсети всегда равен числу, стоящему перед адресом следующей подсети.

В таблице показаны две доступные подсети, а также диапазоны хостов и ширококвещательные адреса для них.

|                          |         |         |
|--------------------------|---------|---------|
| Подсеть                  | 64.0    | 128.0   |
| Первый хост              | 64.1    | 128.1   |
| Последний хост           | 127.254 | 191.254 |
| Ширококвещательный адрес | 127.255 | 191.255 |

Мы добавили наибольшее и наименьшее значения в четвертом октете и сразу получили ответ. Процедура похожа на вычисления для класса С, но нужно добавлять четвертый октет.

#### Пример 2: 255.255.240.0

172.16.0.0=Сетевой адрес

255.255.240.0=Маска подсети

1.  $2^4 - 2 = 14$ .

2.  $2^{12} - 2 = 4094$ .
3. 256 - 240 = 16, 32, 48 и т.д. до 224. Заметим, что это число равно подсетям в классе С с маской 240.
4. Сначала определим широковещательный адрес в п. 5, а затем выполним п. 4 для выявления адресов хостов.
5. Широковещательный адрес в каждой подсети всегда равен числу, стоящему перед адресом следующей подсети.

В таблице показаны три первые подсети, корректные хосты и широковещательные адреса для класса В с маской 255.255.240.0.

|                         |        |        |        |
|-------------------------|--------|--------|--------|
| Подсеть                 | 16.0   | 32.0   | 48.0   |
| Первый хост             | 16.1   | 32.1   | 48.1   |
| Последний хост          | 31.254 | 47.254 | 63.254 |
| Широковещательный адрес | 31.255 | 47.255 | 63.255 |

**Пример 3: 255.255.254.0**

1.  $2^7 - 2 = 126$ .
2.  $2^9 - 2 = 510$ .
3. 256 - 254 = 2, 4, 6, 8 и т.д. до 252.
4. Сначала определим широковещательный адрес в п. 5, а затем выполним п. 4 для выявления адресов хостов.
5. Широковещательный адрес в каждой подсети всегда равен числу, стоящему перед адресом следующей подсети.

В таблице показаны четыре первые подсети, хосты и широковещательные адреса для класса В с маской 255.255.254.0.

|                         |       |       |       |       |
|-------------------------|-------|-------|-------|-------|
| Подсеть                 | 2.0   | 4.0   | 6.0   | 8.0   |
| Первый хост             | 2.1   | 4.1   | 6.1   | 8.1   |
| Последний хост          | 3.254 | 5.254 | 7.254 | 9.254 |
| Широковещательный адрес | 3.255 | 5.255 | 7.255 | 9.255 |

**Пример 4: 255.255.255.0**

Согласно популярному заблуждению, 255.255.255.0 является маской подсети в классе С. Очень многие люди пользуются этой маской сетей класса В, считая ее маской подсети в классе С. Однако это маска подсети класса В с 8-ю разрядами для выделения подсетей — т.е. отнюдь не маска из класса С. Выделение подсетей для этого случая:

1.  $2^8 - 2 = 254$ .
2.  $2^8 - 2 = 254$ .

3.  $256-255=1$ , 2, 3 и т.д. до 254.
4. Сначала определим широковещательный адрес в п. 5, а затем выполним п. 4 для выявления адресов хостов.
5. Широковещательный адрес в каждой подсети всегда равен числу, стоящему перед адресом следующей подсети.

Таблица для первых трех и одной последней подсети, а также диапазона хостов вместе с широковещательным адресом для маски 255.255.255.0 в классе В.

|                         |       |       |       |         |
|-------------------------|-------|-------|-------|---------|
| Подсеть                 | 1.0   | 2.0   | 3.0   | 254.0   |
| Первый хост             | 1.1   | 2.1   | 3.1   | 254.1   |
| Последний хост          | 1.254 | 2.254 | 3.254 | 254.254 |
| Широковещательный адрес | 1.255 | 2.255 | 3.255 | 254.255 |

### Пример 5: 255.255.255.128

На первый взгляд данная маска является незаконной! Действительно, это одна из самых трудных масок подсетей для расчетов. Ее можно успешно использовать на практике, поскольку мы получаем более 500 подсетей с 126 хостами в каждой.

1.  $2^9 - 2=510$ .
2.  $2^7 - 2=126$ .
3. Ответ на третий вопрос не так прост.  $256-255=1$ , 2, 3 и т.д. для третьего октета. Однако нельзя забывать один разряд подсетей в четвертом октете. Помните о примере с одним разрядом подсетей для класса С? Аналогичная ситуация возникает и в нашем случае (именно поэтому мы и привели пример с 1-разрядной маской подсети для класса С). Реально мы получаем две подсети для каждого значения в третьем октете, т.е. 510 подсетей. Например, если третий октет определяет подсеть 3, то подсетями станут 3.0 и 3.128.
4. Сначала определим широковещательный адрес в п. 5, а затем выполним п. 4 для выявления адресов хостов.
5. Широковещательный адрес в каждой подсети всегда равен числу, стоящему перед адресом следующей подсети.

В таблице показаны характеристики подсетей, хостов и широковещательных адресов для маски 255.255.255.128 в классе В.

|                         |       |       |       |       |       |       |       |
|-------------------------|-------|-------|-------|-------|-------|-------|-------|
| Подсеть                 | 0.128 | 1.0   | 1.128 | 2.0   | 2.128 | 3.0   | 3.128 |
| Первый хост             | 0.129 | 1.1   | 1.129 | 2.1   | 2.129 | 3.1   | 3.129 |
| Последний хост          | 0.254 | 1.126 | 1.254 | 2.126 | 2.254 | 3.126 | 3.254 |
| Широковещательный адрес | 0.255 | 1.127 | 1.255 | 2.127 | 2.255 | 3.127 | 3.255 |

**Пример 6: 255.255.255.192**

Этот пример тоже непрост. Подсети 0 и 192 допустимы в четвертом октете. Поэтому вычисления зависят от значений в третьем октете.

1.  $2^{10} - 2 = 1022$  подсетей.
2.  $2^6 - 2 = 62$  хостов.
3.  $256 - 192 = 64$  и 128. Однако когда выключены все разряды подсети в третьем октете, то допустима подсеть 0 в четвертом октете. Кроме того, когда включены не все разряды подсети в третьем октете, то 192 будет допустимым значением для подсети в четвертом октете.
4. Сначала определим ширококвещательный адрес в п. 5, а затем выполним п. 4 для выявления адресов хостов.
5. Широковещательный адрес в каждой подсети всегда равен числу, стоящему перед адресом следующей подсети.

Таблица для первых двух диапазонов подсетей, хостов и ширококвещательных адресов:

|                         |       |       |       |      |       |       |       |
|-------------------------|-------|-------|-------|------|-------|-------|-------|
| Подсеть                 | 0.64  | 0.128 | 0.192 | 1.0  | 1.64  | 1.128 | 1.192 |
| Первый хост             | 0.65  | 0.129 | 0.193 | 1.1  | 1.65  | 1.129 | 1.193 |
| Последний хост          | 0.126 | 0.190 | 0.254 | 1.62 | 1.126 | 1.190 | 1.254 |
| Широковещательный адрес | 0.127 | 0.191 | 0.255 | 1.63 | 1.127 | 1.191 | 1.255 |

Обратите внимание, что для каждого значения в третьем октете мы получаем подсети 0, 64, 128 и 192 в четвертом октете. Это справедливо для всех подсетей в третьем октете за исключением 0 и 255. Для подсети 0 в третьем октете мы уже показывали варианты, однако для подсети 1 в третьем октете мы получим четыре подсети: 0, 64, 128 и 192.

**Пример 7: 255.255.255.224**

Вычисления аналогичны предыдущему примеру, но получится больше подсетей и меньше хостов в каждой из них.

1.  $2^{11} - 2 = 2046$  подсетей.
2.  $2^5 - 2 = 30$  хостов.
3.  $256 - 224 = 32, 64, 96, 128, 160, 192$ . Однако как показано выше, подсети 0 и 224 могут использоваться тогда, когда в третьем октете нет значений 0 или 255. Это пример варианта, когда в третьем октете нет разрядов подсетей.
4. Сначала определим ширококвещательный адрес в п. 5, а затем выполним п. 4 для выявления адресов хостов.
5. Широковещательный адрес в каждой подсети всегда равен числу, стоящему перед адресом следующей подсети.

Таблица первого диапазона подсетей:

|                         |      |      |       |       |       |       |       |
|-------------------------|------|------|-------|-------|-------|-------|-------|
| Подсеть                 | 0.32 | 0.64 | 0.96  | 0.128 | 0.160 | 0.192 | 0.224 |
| Первый хост             | 0.33 | 0.65 | 0.97  | 0.129 | 0.161 | 0.193 | 0.225 |
| Последний хост          | 0.62 | 0.94 | 0.126 | 0.158 | 0.190 | 0.222 | 0.254 |
| Широковещательный адрес | 0.63 | 0.95 | 0.127 | 0.159 | 0.191 | 0.223 | 0.255 |

Рассмотрим ситуацию, когда в третьем октете включен разряд подсети. Представлена таблица для полного диапазона подсетей, доступных в четвертом октете.

|                         |      |      |      |       |       |       |       |       |
|-------------------------|------|------|------|-------|-------|-------|-------|-------|
| Подсеть                 | 1.0  | 1.32 | 1.64 | 1.96  | 1.128 | 1.160 | 1.192 | 1.224 |
| Первый хост             | 1.1  | 1.33 | 1.65 | 1.97  | 1.129 | 1.161 | 1.193 | 1.225 |
| Последний хост          | 1.30 | 1.62 | 1.94 | 1.126 | 1.158 | 1.190 | 1.222 | 1.254 |
| Широковещательный адрес | 1.31 | 1.63 | 1.95 | 1.127 | 1.159 | 1.191 | 1.223 | 1.255 |

В следующей таблице показана последняя подсеть:

|                         |               |        |        |         |         |         |         |
|-------------------------|---------------|--------|--------|---------|---------|---------|---------|
| Подсеть                 | 255.0         | 255.32 | 255.64 | 255.96  | 255.128 | 255.160 | 255.192 |
| Первый хост             | 255.1         | 255.33 | 255.65 | 255.97  | 255.129 | 255.161 | 255.193 |
| Последний хост          | 255.62        | 255.62 | 255.94 | 255.126 | 255.158 | 255.190 | 255.222 |
| Широковещательный адрес | <b>255.63</b> | 255.63 | 255.95 | 255.127 | 255.159 | 255.191 | 255.223 |

### Выделение подсетей в уме для класса В

Можно ли устно выполнить выделение подсетей для класса В? Для этого существует простой способ, который лучше всего показать на примере:

**Вопрос:** Каковы подсети и широковещательный адрес для IP-адреса 172.16.10.33 из сети 255.255.255.224?

**Ответ:**  $256-224=32$ .  $32+32=64$ . Подсказка - 33 находится между 32 и 64. Однако вспомним, что третий октет считается частью подсети, поэтому ответ: подсеть 10.32. Широковещательный адрес равен 10.63, поскольку 10.64 является следующей подсетью.

Рассмотрим еще четыре примера:

**Вопрос:** Каковы подсети и широковещательный адрес для IP-адреса 172.16.90.66 из 255.255.255.192?

**Ответ:**  $256-192=64$ .  $64+64=128$ . Подсеть - 172.16.90.64. Широковещательный адрес — 172.16.90.127, поскольку следующей подсетью будет 90.128.

**Вопрос:** Каковы подсети и широковещательный адрес для IP-адреса 172.16.50.97 из 255.255.255.224?

**Ответ:**  $256-224=32$ , 64, 96, 128. Подсеть - 172.16.50.96, а широковещательный адрес — 172.16.50.127, поскольку следующей подсетью будет 50.128.

Вопрос: Каковы подсети и широковещательный адрес для IP-адреса 172.16.10.10 из 255.255.255.192?

Ответ:  $256-192=64$ . Подсеть — 172.16.10.0, а широковещательный адрес — 172.16.10.63.

Вопрос: Каковы подсети и широковещательный адрес для IP-адреса 172.16.10.10 из 255.255.255.224?

Ответ:  $256-224=32$ . Подсеть — 172.16.10.0, а широковещательный адрес — 172.16.10.31.

## Выделение подсетей в классе А

Выделение подсетей в классе А ничем не отличается от аналогичной операции для классов В и С, хотя можно использовать 24 разряда вместо 16 разрядов в классе В и восьми разрядов в классе С.

Перечислим все подсети в классе А:

255.128.0.0

255.192.0.0

255.224.0.0

255.240.0.0

255.248.0.0

255.252.0.0

255.254.0.0

255.255.0.0

255.255.128.0

255.255.192.0

255.255.224.0

255.255.240.0

255.255.248.0

255.255.252.0

255.255.254.0

255.255.255.0

255.255.255.128

255.255.255.192

255.255.255.224

255.255.255.240

255.255.255.248

255.255.255.252

Необходимо оставить два разряда для определения хостов. Это не трудно сделать, основываясь на примерах для классов В и С, хотя в данном случае мы получаем больше разрядов для хостов.

### Примеры выделения подсетей в классе Л

Проводя вычисления с IP-адресами и масками подсетей нужно выяснить разряды, используемые для подсети, и разряды для хостов. Это обязательная операция, во время которой следует понимать различия между разрядами подсетей и хостов (см. выше).

#### Пример 1: 255.255.0.0

В классе А используется маска по умолчанию 255.0.0.0, что оставляет 22 для подсетей, поскольку нужны два разряда для адресации хостов. Маска 255.255.0.0 в классе А применяет восемь разрядов для подсетей.

1.  $2^8 - 2 = 254$ .
2.  $2^{16} - 2 = 65, 534$ .
3.  $256 - 255 = 1, 2, 3$  и т.д. (все во втором октете). Подсетями будут 10.1.0.0, 10.2.0.0, 10.3.0.0 и т.д. до 10.254.0.0.
4. Сначала определим широковещательный адрес в п. 5, а затем выполним п. 4 для выявления адресов хостов.
5. Широковещательный адрес в каждой подсети всегда равен числу, стоящему перед адресом следующей подсети.

В таблице 3.8 показаны первая и последняя подсети, диапазон хостов и адрес широковещательной рассылки.

Таблица 3.8.

Первая и последняя подсети

|                         | Первая подсеть | Последняя подсеть |
|-------------------------|----------------|-------------------|
| Подсеть                 | 10.1.0.0       | 10.254.0.0        |
| Первый хост             | 10.1.0.1       | 10.254.0.1        |
| Последний хост          | 10.1.255.254   | 10.254.255.254    |
| Широковещательный адрес | 10.1.255.255   | 10.254.255.255    |

#### Пример 2: 255.255.240.0

255.255.240.0 дает нам 12 разрядов для подсетей, оставляя 12 разрядов для адресов хостов.

1.  $2^{12} - 2 = 4094$ .
2.  $2^{12} - 2 = 4094$ .
3.  $256 - 240 = 16$ . Однако второй октет равен 255 (все разряды подсети включены), поэтому можно начать третий октет с 0, поскольку включены разряды подсетей во втором октете. Следовательно, подсетями будут 10.1.0.0, 10.1.16.0, 10.1.32.0, 10.1.48.0 и т.д. до 10.1.240.0. Второй набор подсетей: 10.2.0.0, 10.2.16.0, 10.2.32.0, 10.2.48.0 и т.д. до 10.2.240.0. Заметим, что можно использовать 240 в третьем октете, поскольку включены не все разряды подсетей во втором октете.

Другими словами, 10.255.240.0 является допустимой, ведь включены все разряды подсетей. Последней корректной подсетью станет 10.255.224.0.

4. Сначала определим широковещательный адрес в п. 5, а затем выполним п. 4 для выявления адресов хостов.
  5. Широковещательный адрес в каждой подсети всегда равен числу, стоящему перед адресом следующей подсети.
- В таблице 3.9 показаны несколько примеров диапазонов хостов.

**Таблица 3.9.**  
**Допустимые диапазоны хостов для маски 255.255.240.0 в классе А**

|                         | Первая подсеть | Вторая подсеть | Последняя подсеть |
|-------------------------|----------------|----------------|-------------------|
| Подсеть                 | 10.1.0.0       | 10.1.16.0      | 10.255.224.0      |
| Первый хост             | 10.1.0.1       | 10.1.16.1      | 10.255.224.1      |
| Последний хост          | 10.1.15.254    | 10.1.31.254    | 10.255.239.254    |
| Широковещательный адрес | 10.1.15.255    | 10.1.31.255    | 10.255.239.255    |

**Пример 3: 255.255.255.192**

Рассмотрим еще один пример, где для выделения подсетей использованы второй, третий и четвертый октеты.

1.  $2^{18} - 2 = 262\ 142$  подсетей.
2.  $2^6 - 2 = 62$  хостов.
3. Необходимо добавить количество подсетей для второго, третьего и четвертого октетов. Во втором и третьем октете мы можем использовать диапазон от 1 до 255, поскольку одновременно не могут быть включены все разряды подсетей во втором, третьем и четвертом октетах. Для четвертого октета это количество равно  $256 - 192 = 64$ . Однако допустимо и значение 0, поскольку во втором и третьем октетах будет включен хотя бы один другой разряд подсетей. Кроме того, 192 тоже допустима, ведь включены все разряды во втором и третьем октетах.
4. Сначала определим широковещательный адрес в п. 5, а затем выполним п. 4 для выявления адресов хостов.
5. Широковещательный адрес в каждой подсети всегда равен числу, стоящему перед адресом следующей подсети.

В таблице показаны несколько первых подсетей и первых допустимых хостов, а также широковещательные адреса для маски 255.255.255.192 в классе А.

---

|                         |           |            |            |            |
|-------------------------|-----------|------------|------------|------------|
| Подсеть                 | 10.1.0.0  | 10.1.0.64  | 10.1.0.128 | 10.1.0.192 |
| Первый хост             | 10.1.0.1  | 10.1.0.65  | 10.1.0.129 | 10.1.0.193 |
| Последний хост          | 10.1.0.62 | 10.1.0.126 | 10.1.0.190 | 10.1.0.254 |
| Широковещательный адрес | 10.1.0.63 | 10.1.0.127 | 10.1.0.191 | 10.1.0.255 |

---

В следующей таблице показаны последние три подсети и хосты для маски 255.255.255.192 в классе А.

---

|                         |               |                |                |
|-------------------------|---------------|----------------|----------------|
| Подсеть                 | 10.255.255.0  | 10.255.255.64  | 10.255.255.128 |
| Первый хост             | 10.255.255.1  | 10.255.255.65  | 10.255.255.129 |
| Последний хост          | 10.255.255.62 | 10.255.255.126 | 10.255.255.190 |
| Широковещательный адрес | 10.255.255.63 | 10.255.255.127 | 10.255.255.191 |

---

## Упражнение

---

Напишите подсеть, широковещательный адрес и диапазон допустимых хостов для:

- 172.16.10.5 255.255.255.128
- 172.16.10.33 255.255.255.224
- 172.16.10.65 255.255.255.192
- 172.16.10.172 255.255.255.252
- 172.16.10.33 255.255.255.240
- 192.168.100.25 255.255.255.252
- 192.168.100.17 при 4 разрядах на выделение подсетей
- 192.168.100.66 при 3 разрядах на выделение подсетей
- 192.168.100.17 255.255.255.248
- 10.10.10.5 255.255.255.252

## Проверочные вопросы

---

- Какой протокол транспортного уровня обеспечивает службу без установления соединения для взаимодействия хостов?
  - IP
  - ARP
  - TCP
  - UDP

2. Какой протокол транспортного уровня формирует виртуальные цепи между хостами?
  - A. IP
  - B. ARP**
  - C. TCP
  - D. UDP
3. Какой протокол уровня Интернета обеспечивает службу с установлением соединения для взаимодействия хостов?
  - A. IP
  - B. ARP**
  - C. TCP
  - D. UDP
4. Если хост посылает в широковещательной рассылке кадр, содержащий аппаратный адрес источника и назначения, причем целью является присваивание себе IP-адреса, то какой используется протокол сетевого уровня?
  - A. RARP
  - B. ARPA**
  - C. ICMP
  - D. TCP
  - E. IPX**
5. Если перегружен интерфейс маршрутизатора, то какой протокол стека TCP/IP служит для сообщения о перегрузке соседним маршрутизаторам?
  - A. RARP
  - B. ARP**
  - C. ICMP
  - D. IP
  - E. TCP**
6. Каков допустимый диапазон хостов для IP-адреса 172.16.10.22 и маски 255.255.255.240?
  - A. 172.16.10.20 до 172.16.10.22**
  - B. 172.16.10.1 до 172.16.10.255**
  - C. 172.16.10.16 до 172.16.10.23**
  - D. 172.16.10.17 до 172.16.10.31**
  - E. 172.16.10.17 до 172.16.10.30**
7. Какой диапазон адресов можно использовать в первом октете сетевого адреса класса B?
  - A. 1 – 126**
  - B. 1 – 127**

- C. 128 – 190
  - D. 128 – 191
  - E. 129 – 192
  - F. 192-220
8. Какой диапазон адресов можно использовать в первом октете сетевого адреса класса C?
- A. 1 – 127
  - B. 129 – 192
  - C. 203 – 234
  - D. 192-223
9. Сколько байтов в адресе Ethernet?
- A. 3
  - B. 4
  - C. 5
  - D. 6
  - E. 7
  - F. 8
  - G. 16
10. Какой протокол служит для поиска аппаратного адреса локального устройства?
- A. RARP
  - B. ARP
  - C. IP
  - D. ICMP
  - E. BootP
11. Что из перечисленного ниже является адресом широковещательной рассылки в сети класса B с маской подсети по умолчанию?
- A. 172.16.10.255
  - B. 172.16.255.255
  - C. 172.255.255.255
  - D. 255.255.255.255
12. Какой класс IP-адресов предоставляет не более 254 адресов хостов для идентификатора сети?
- A. A
  - B. B
  - C. C
  - D. D
  - E. E
13. Каков широковещательный адрес для подсети 10.254.255.19 из 255.255.255.248?

- A. 10.254.255.23
  - B. 10.254.255.24
  - C. 10.254.255.255
  - D. 10.255.255.255
14. Каков широковещательный адрес для подсети 172.16.99.99 из 255.255.192.0?
- A. 172.16.99.255
  - B. 172.16.127.255
  - C. 172.16.255.255
  - D. 172.16.64.127
15. Если нужно 12 подсетей в классе C, то какую следует использовать маску подсети?
- A. 255.255.255.252
  - B. 255.255.255.248
  - C. 255.255.255.240
  - D. 255.255.255.255
16. Каков диапазон номеров портов, которым пользуется передающий хост для установки сеанса с другим хостом?
- A. 1 – 1023
  - B. 1024 и выше
  - C. 1 – 256
  - D. 1 – 65534
17. Какой диапазон является диапазоном общеизвестных портов?
- A. 1 – 1023
  - B. 1024 и выше
  - C. 1 – 256
  - D. 1 – 65534
18. Каков адрес широковещательной рассылки для хостов в подсети 10.10.10.10 из 255.255.254.0?
- A. 10.10.10.255
  - B. 10.10.11.255
  - C. 10.10.255.255
  - D. 10.255.255.255
19. Какой широковещательный адрес использует хост 192.168.210.5 из 255.255.255.252?
- A. 192.168.210.255
  - B. 192.168.210.254
  - C. 192.168.210.7
  - D. 192.168.210.15

20. Если сеть класса В разделена строго на 510 подсетей, то какую маску подсети нужно присвоить в этой сети?
- A. 255.255.255.252
  - B. 255.255.255.128
  - C. 255.255.0.0
  - D. 255.255.255.192

### Ответы к упражнению

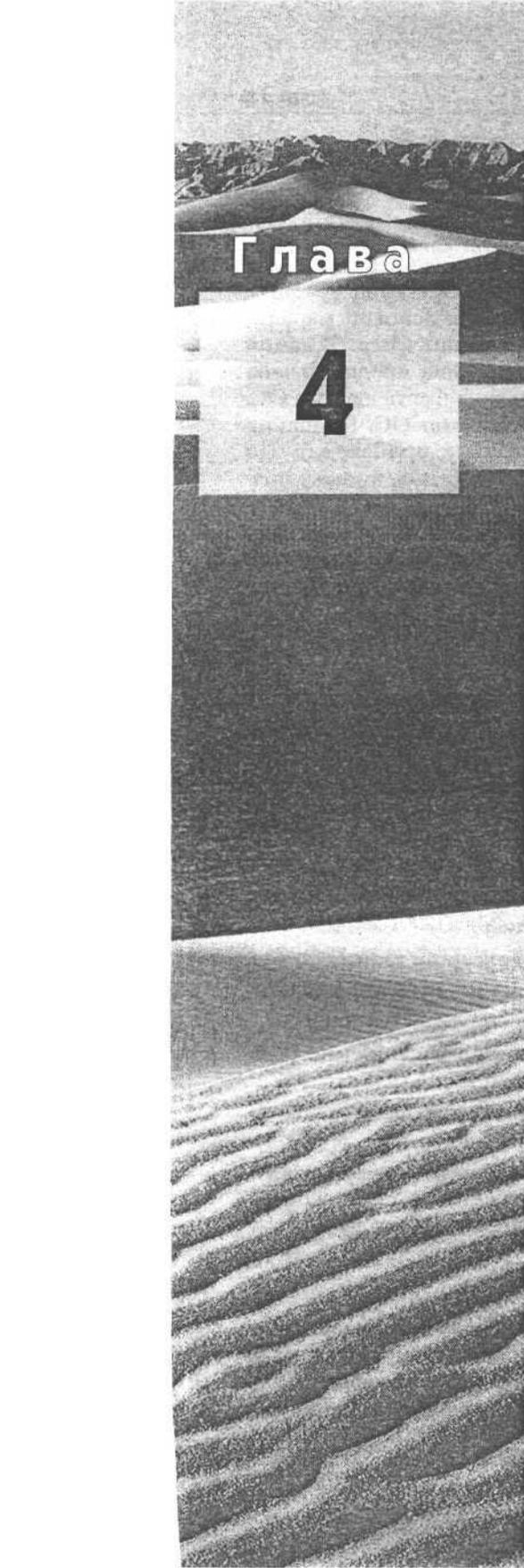
---

1. Подсеть 172.16.10.0, широковещательный адрес 172.16.10.127, а диапазон хостов от 172.16.10.1 до 126.
2. Подсеть 172.16.10.32, широковещательный адрес 172.16.10.63, а диапазон хостов от 172.16.10.33 до 10.62
3. Подсеть 172.16.10.64, широковещательный адрес 172.16.10.127, а диапазон хостов от 172.16.10.65 до 172.16.10.126
4. Сеть 172.16.10.16, широковещательный адрес 172.16.10.19, а диапазон хостов от 172.16.10.17 до 18
5. Сеть 172.16.10.32, широковещательный адрес 172.16.10.47, а диапазон хостов от 172.16.10.33 до 46
6. Подсеть 192.168.100.24, широковещательный адрес 192.168.100.27, а диапазон хостов от 192.168.100.25 до 26
7. Подсеть 192.168.100.16, широковещательный адрес 192.168.100.31, а диапазон хостов от 192.168.100.17 до 30
8. Подсеть 192.168.100.64, широковещательный адрес 192.168.100.95, а диапазон хостов от 192.168.100.65 до 94
9. Подсеть 192.168.100.16, широковещательный адрес 192.168.100.23, а диапазон хостов от 192.168.100.17 до 22
10. Подсеть 10.10.10.4, широковещательный адрес 10.10.10.7, а диапазон хостов от 10.10.10.5 до 6

### Ответы на проверочные вопросы

---

- |      |       |       |
|------|-------|-------|
| 1. D | 8. D  | 15. C |
| 2. C | 9. D  | 16. B |
| 3. A | 10. B | 17. A |
| 4. A | 11. B | 18. B |
| 5. C | 12. C | 19. C |
| 6. E | 13. A | 20. B |
| 7. D | 14. B |       |



Глава

4

## Конфигурация и команды управления /OS

## Пользовательский интерфейс маршрутизатора Cisco

Операционная система (ОС) *Cisco IOS* (Internetwork Operating System — операционная система объединенных сетей) является основой маршрутизаторов и большей части переключателей компании Cisco. В самой компании эту ОС называют *Cisco Fusion*, поскольку она предназначена для поддержки всех устройств Cisco, которые должны иметь единую ОС. Однако не все устройства Cisco выполняют одинаковую ОС. Компания приобретает больше устройств, чем разрабатывает и производит. Но почти все маршрутизаторы Cisco работают в одной ОС IOS, а также почти половина переключателей этой компании.

В этом разделе книги мы познакомимся с ОС Cisco IOS, а также процессом последовательной настройки маршрутизатора Cisco, сначала в режиме установки, а затем через интерфейс CLI (Command-Line Interface — интерфейс командной строки).

### Операционная система IOS в маршрутизаторах Cisco

ОС IOS была создана для доставки сетевых служб и поддержки сетевых приложений. Cisco IOS действует в большинстве маршрутизаторов Cisco и некоторых переключателях Cisco Catalyst, например Catalyst 1900 (см. приложение В).

Программное обеспечение IOS в маршрутизаторе Cisco служит для следующих целей, дополняя функции аппаратного обеспечения Cisco:

- Обслуживание сетевых протоколов и функций
- Передача высокоскоростного трафика между устройствами
- Защита управления доступом и предотвращение неавторизованного использования сети
- Обеспечение масштабируемости для упрощения расширения сети и создания избыточности (резервирования)
- Поддержка должного уровня надежности при подключениях к сетевым ресурсам

К Cisco IOS можно обратиться через консольный порт маршрутизатора, по модемному соединению или по протоколу Telnet. Доступ к командной строке IOS называется сеансом EXEC (исполнения команды).

### Подключение к маршрутизатору Cisco

К маршрутизатору Cisco подключаются для его настройки (конфигурация), проверки параметров настройки или получения статических данных о работе устройства. Существуют разные способы подключения к маршрутизатору Cisco, но в первый раз такое подключение обычно выполняется через консольный порт.

*Консольный порт* имеет разъем RJ-45 на задней стенке маршрутизатора. Этот разъем служит для подключения к маршрутизатору и его настройки. По умолчанию для доступа к консольному порту не установлен пароль.

Другим способом доступа к маршрутизатору Cisco является *вспомогательный порт* (auxiliary port). Он подобен консольному порту и используется с теми же целями. Однако вспомогательный порт допускает настройку на модемные команды для подключения к маршрутизатору через модем. Т.е. можно вызвать удаленный маршрутизатор по коммутируемой (телефонной) линии и подключиться к нему через вспомогательный порт, если маршрутизатор выключен и необходимо настроить его параметры.

Третий способ подключения к маршрутизатору Cisco предполагает использование программы *Telnet*. Это программа эмуляции терминала, которая поддерживает режим неинтеллектуального терминала (dumb-terminal). Можно использовать Telnet для подключения к любому активному интерфейсу маршрутизатора, например к порту Ethernet или последовательному порту.

На рис. 4.1 показаны разъемы маршрутизатора Cisco серии 2501. Обратите внимание на разные интерфейсы для разных способов подключения.

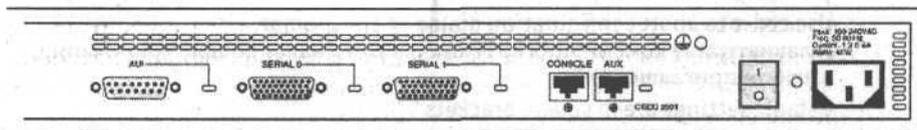


Рис. 4.1. Маршрутизатор серии 2501

Маршрутизатор серии 2501 имеет два последовательных интерфейса для соединений по региональным сетям (WAN) и один интерфейс AUI (Attachment Unit Interface, интерфейс подключения модуля) для сетевых соединений 10 Мбит/с Ethernet. Кроме того, маршрутизатор 2501 имеет один консольный и один вспомогательный порты с разъемами RJ-45.

## Включение маршрутизатора

Во время первого включения маршрутизатора Cisco, он запускает проверочный тест по включению питания POST (power-on self test). Если тестирование пройдет успешно, то ищет и загружает Cisco IOS из флэш-памяти, если в ней находится соответствующий файл. Флэш-память — это электрически стираемая программируемая память "только чтение" EEPROM (electronically erasable programmable read-only memory). ОС IOS будет загружена и начнет поиск корректной конфигурации, называемой конфигурацией запуска (startup-config), которая по умолчанию хранится в энергонезависимой оперативной памяти NVRAM (nonvolatile RAM).

Если в NVRAM нет конфигурации для загрузки, маршрутизатор переходит в режим настройки (setup mode). В нем выполняется последовательный ввод конфигурационных данных маршрутизатора. Можно в

любой момент перейти в режим настройки, введя в командной строке `setup`, находясь в режиме глобального конфигурирования (`global configuration mode`). В режиме настройки доступны только несколько глобальных команд. Однако подобный режим помогает установить даже малопонятные конфигурационные параметры, например режим моста или работу в сети DECnet.

## Режим настройки

В режиме настройки реально существуют два варианта действий: *Basic Management* (базовое управление) и *Extended Setup* (расширенная настройка). Режим *Basic Management* обеспечивает только основные возможности для установки подключения к маршрутизатору, но режим *Extended Setup* поддерживает установку некоторых глобальных параметров, например параметров конфигурации интерфейсов.

— System Configuration Dialog —  
(диалог системной конфигурации)

Would you like to enter the initial configuration dialog? [yes/no]:y  
(войти в диалог начального конфигурирования?)

At any point you may enter a question mark '?' for help.  
(в любой момент можно ввести вопросительный знак для вывода справки)

Use **ctrl-c** to abort configuration dialog at any prompt.  
(клавиатурная комбинация `ctrl-c` прерывает диалог конфигурирования в любом приглашении)

Default settings are in square brackets '['].  
(значения по умолчанию показаны в квадратных скобках)

Режим настройки *Basic Management* служит только для установки подключений для управления системой, а режим *Extended Setup* выводит запросы для конфигурации каждого интерфейса системы.

Would you like to enter basic management setup? [yes/no]:n  
(войти в режим настройки базового управления)

First would you like to see the current interface summary? [yes]:return  
(сначала можно вывести сведения о текущем интерфейсе)

Any interface listed with OK? value "NO" does not have a valid configuration  
(любой интерфейс, для которого после OK? выведено "NO", не имеет правильной конфигурации)

| Interface             | IP-Address  | OK? | Method | Status        | Protocol  |
|-----------------------|-------------|-----|--------|---------------|-----------|
| (IP-адрес интерфейса) |             |     | Метод  | Статус        | Протокол) |
| FastEthernet0/0       | unassigned  | NO  |        | unset up      | up        |
| (FastEthernet0/0      | не присвоен | NO  |        | не установлен | включен)  |
| FastEthernet0/1       | unassigned  | NO  |        | unset up      | up        |

Configuring global parameters:  
(конфигурирование глобальных параметров)

Enter hostname [Router]:Todd  
(введите имя хоста)

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted

in the configuration.

(разрешенный секрет является паролем для доступа к привилегированному режиму EXEC и режимам конфигурирования. После ввода этот пароль будет зашифрован в конфигурации.)

Enter enable secret: **todd**

(введите разрешенный секрет)

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

(разрешенный пароль используется, когда не указан допускаемый секрет, и в устаревших версиях программного обеспечения или некоторых образах загрузки)

Enter enable password: **todd**

(введите разрешенный пароль)

% Please choose a password that is different from the enable secret

(пожалуйста, укажите иной пароль, чем разрешенный секрет)

Enter enable password: **todd1**

Остановимся, чтобы обсудить два введенных пароля. Мы подробно рассмотрим пароли ниже, а пока нужно понять только назначение пароля "разрешенный пароль". Этот пароль применяется для маршрутизаторов с IOS версий до 10.3, однако в режиме настройки необходимо ввести два разных пароля. Далее этот пароль не будет использоваться, если сконфигурирован разрешенный секрет.

Следующий пароль служит для защиты сеансов по Telnet с маршрутизатором. Причина ввода пароля для Telnet (VTY) в режиме настройки в том, что если не установлен пароль для линии VTY, то нельзя будет по умолчанию обратиться по Telnet к маршрутизатору.

The virtual terminal password is used to protect access to the router over a network interface.

(пароль виртуального терминала защищает доступ к маршрутизатору через сетевой интерфейс)

Enter virtual terminal password: **todd**

(введите пароль виртуального терминала)

Configure SNMP Network Management? [yes]:enter **or no**

(настроить сетевое управление по протоколу SNMP?)

Community string [public]:enter

(строка сообщества)

Configure DECnet? [no]:enter

(настроить DECnet?)

Configure AppleTalk? [no]:enter

(настроить AppleTalk?)

Configure IP? [yes]:enter

(настроить IP?)

Configure IGRP routing? [yes]: n

(настроить маршрутизацию IGRP?)

Configure RIP routing? [no]:enter

(настроить маршрутизацию RIP?)

Configure bridging? [no]:enter  
(настроить выполнение функции моста?)

Configure IPX? [no]:enter  
(настроить IPX?)

Представленные выше команды помогают настроить протокол, когда не вполне понятно назначение каждой команды. Однако ввод через интерфейс командной строки CLI, а не в режиме **настройки**, обеспечивает большую гибкость.

Если в маршрутизаторе установлена карта асинхронного модема, в режиме **настройки** придется установить параметры модема.

Async lines accept incoming modems calls. If you will have users dialing in via modems, configure these lines.

(асинхронная линия принимает входящие модемные звонки.

Если пользователи обращаются к устройству по модемной связи, следует сконфигурировать эту линию)

Configure Async lines? [yes]: n  
(настроить асинхронные линии?)

Если маршрутизатор имеет интерфейс **ISDN BRI**, появится приглашение для установки типа коммутации **ISDN**. Маршрутизатор выведет:

BRI interface needs isdn switch-type to be configured  
(необходимо настроить тип коммутации **ISDN** для интерфейса **BRI**)

Valid switch types are:

(доступны следующие типы коммутации)

[0] none .....Only if you don't want to configure BRI.  
(только, когда не требуется настраивать **BRI**)

[1] basic-ltr6 .....1TR6 switch type for Germany  
(тип коммутации **1TR6** для Германии)

[2] basic-5ess ..... AT&T 5ESS switch type for the US/Canada  
(тип коммутации **AT&T 5ESS** для США и Канады)

[3] basic-dms100... Northern DMS-100 switch type for US/Canada  
(тип коммутации **Northern DMS-100** для США и Канады)

[4] basic-net3 ..... NET3 switch type for UK and Europe  
(тип коммутации **NET3** для Великобритании и Европы)

[5] basic-ni ..... National ISDN switch type  
(национальный тип коммутации **ISDN**)

[6] basic-ts013 ..... TS013 switch type for Australia  
(тип коммутации **TS013** для Австралии)

[7] ntt ..... NTT switch type for Japan  
(тип коммутации **NTT** для Японии)

[8] vn3 ..... VN3 and VN4 switch types for France  
(тип коммутации **VN3** и **VN4** для Франции)

Choose ISDN BRI Switch Type [2]: 2

(укажите тип коммутации **ISDN BRI**)

После настройки типа коммутации появится приглашение для конфигурирования интерфейса, включая IP-адрес.

В следующей секции режима Extended Setup производится настройка интерфейсов. В нашем маршрутизаторе только два интерфейса FastEthernet: FastEthernet 0/0 и FastEthernet 0/1. Интерфейсы маршрутизаторов будут рассмотрены ниже.

Configuring interface parameters:  
(настройка параметров интерфейса)

Do you want to configure FastEthernet0/0 interface? [yes]:return

(настроить интерфейс FastEthernet0/0?)

Use the 100 Base-TX (RJ-45) connector? [yes]:return

(используется разъем RJ-45 для 100 Base-TX?)

Operate in full-duplex mode? [no]:y and return

(полнодуплексный режим?)

Configure IP on this interface? [yes]:return

(настроить в этом интерфейсе протокол IP?)

IP address for this interface: 1.1.1.1

(IP-адрес этого интерфейса)

Subnet mask for this interface [255.0.0.0] : 255.255.0.0

(маска подсети этого интерфейса)

Class A network is 1.0.0.0, 16 subnet bits; mask is /16

(сеть 1.0.0.0 класса А, 16 разрядов для подсетей, маска /16)

Do you want to configure FastEthernet0/1 interface? [yes]:return

Use the 100 Base-TX (RJ-45) connector? [yes]:return

Operate in full-duplex mode? [no]:y and return

Configure IP on this interface? [yes]:return

IP address for this interface: 2.2.2.2

Subnet mask for this interface [255.0.0.0] : 255.255.0.0

Class A network is 2.0.0.0, 16 subnet bits; mask is /16

Эта конфигурация с базовыми параметрами, но она позволяет быстро установить и запустить маршрутизатор. Маска показана в виде /16, что означает использование 16-ти из 32-х разрядов (см. главу 3).

Далее в режиме Extended Setup выполняется создание исполняемой конфигурации (running configuration):

The following configuration command script was created:

(был создан следующий конфигурационный сценарий команд)

```
hostname Todd
```

```
enable secret 5 1B0wu$5F0m/EDdtRkQ4vy4a8qwC/
```

```
enable password todd1
```

```
line vty 0 4
```

```
password todd
```

```
snmp-server community public
```

```
|
```

```
no decnet routing
```

```
no appletalk routing
```

```
ip routing
```

```

no bridge 1
no ipx routing
!
interface FastEthernet0/0
media-type IOBaseX
full-duplex
ipaddress 1.1.1.1 255.255.0.0
no mop enabled
!
interface FastEthernet0/1
media-type IOBaseX
full-duplex
ip address 2.2.2.2 255.255.0.0
no mop enabled
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
end

```

[0] Go to the IOS command prompt without saving this config.  
(перейти в командную строку IOS без сохранения этой конфигурации)

[1] Return back to the setup without saving this config.  
(вернуться в режим настройки без сохранения этой конфигурации)

[2] Save this configuration to nvram and exit.  
(выйти с сохранением этой конфигурации в NVRAM)

Enter your selection [2]:0  
(введите значение)

Интересные возможности Extended Setup появляются в конце процесса настройки. Можно перейти в режим CLI и отменить исполняемую конфигурацию `running-config` [0], вернуться в режим настройки для повторного ввода данных [1] или сохранить введенную информацию в NVRAM, причем с созданием исполняемой конфигурации `startup-config`. Полученный в последнем случае файл будет загружаться при каждом перезапуске маршрутизатора.

В примере выбран вариант "0", т.е. возврат в IOS без сохранения файла исполняемой конфигурации. Это можно сделать и в режиме командной строки CLI.

## Интерфейс командной строки

*Интерфейс командной строки CLI (Command-Line Interface) является наилучшим для конфигурации маршрутизатора, поскольку он обеспечивает максимальную гибкость. Для перехода в интерфейс CLI следует ввести по в диалоге начального конфигурирования Initial Configuration Dialog. После этого маршрутизатор выведет сообщение о состоянии всех своих интерфейсов.*

```
Would you like to enter the initial configuration dialog? [yes]: n
(войти в диалог начального конфигурирования?)
Would you like to terminate autoinstall? [yes]:return
(отменить автоматическую установку?)

Press RETURN to get started!
(для начала работы нажмите RETURN)

00:00:42: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
(интерфейс Ethernet0 изменил состояние на включенное)
00:00:42: %LINK-3-UPDOWN: Interface Serial0, changed state to down
(интерфейс Serial0 изменил состояние на выключенное)
00:00:42: %LINK-3-UPDOWN: Interface Serial1, changed state to down
00:00:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0,
changed state to up
00:00:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0, changed >
state to down
00:00:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1, changed
state to down
00:01:30: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0,
changed state to down
00:01:31: %LINK-5-CHANGED: Interface Serial0, changed state
to administrativelydown
(интерфейс Serial0 изменил состояние на выключенное административно)
00:01:31: %LINK-5-CHANGED: Interface Ethernet0, changed state to
administratively down
00:01:31: %LINK-5-CHANGED: Interface Serial1, changed state to
administratively down
00:01:32: %IP-5-WEBINST_KILL: Terminating DNS process
(завершен процесс DNS)
00:01:38: %SYS-5-RESTART: System restarted --
(система перезапущена)
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-DS-L), Version 11.3(9),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 06-Apr-99 19:23 by dschwart
```

## Регистрация (вход) в маршрутизатор

После вывода сообщения о статусе интерфейсов и нажатия клавиши Return появится приглашение Router>. Это приглашение пользовательского режима (user mode), которое часто используется для просмотра статистики, хотя из него можно перейти в привилегированный режим (privileged mode). В пользовательском режиме допускается только просмотр, а изменение конфигурации маршрутизатора Cisco выполняется в привилегированном режиме, переход в который выполняется командой enable.

```
Router>
Router>enable
Router#
```

Теперь приглашение имеет вид **Router#**, что отмечает привилегированный режим. В нем можно просматривать и изменять конфигурацию. Для выхода из привилегированного режима в пользовательский используйте команду `disable`.

```
Router#disable
Router>
```

Теперь можно ввести `logout`, чтобы выйти из режима консоли.

```
Router>logout
```

```
Router con0 is now available
(маршрутизатор con0 доступен)
Press RETURN to get started.
(для начала работы нажмите RETURN)
```

Либо разрешен ввод `logout` или `exit` в привилегированном режиме для вывода приглашения на выход.

```
Router>en
Router#logout
```

```
Router con0 is now available
Press RETURN to get started.
```

## Обзор режимов маршрутизатора

Для настройки из интерфейса CLI необходимо глобально изменить состояние маршрутизатора, указав команду `config terminal` (краткая форма: `config t`), которая переводит устройство в режим глобального конфигурирования и изменяет исполняемую конфигурацию `running-config`. Можно ввести `config` в приглашении привилегированного режима, а затем нажать `Return` для возвращения режима терминала по умолчанию.

```
Router#config
Configuring from terminal, memory, or network [terminal]?return
(настройка с терминала, из памяти или по сети)
Enter configuration commands, one per line. End with CNTL/Z.
(введите команды конфигурирования, по одной в строке.
Закончите ввод клавиатурной комбинацией CNTL/Z)
Router(config)#
```

После этого можно внести изменения, которые действуют на маршрутизатор в целом.

Для изменения конфигурации `running-config`, которая является текущей исполняемой конфигурацией в динамической оперативной памяти DRAM (Dynamic RAM) следует использовать команду `config terminal`

(`config t`). Для изменения конфигурации из NVRAM (конфигурации запуска `startup-config`) следует ввести команду `config memory` (`config mem`). Если необходимо изменить конфигурацию маршрутизатора, хранящуюся на хосте TFTP (см. главу 7), применяйте команду `config network` (`config net`).

Однако для точного и реального изменения конфигурации маршрутизатора, ее следует поместить в оперативную память RAM. Т.е. ввод `config mem` или `config net` приводит к замене текущей исполняемой конфигурации `running-config` на конфигурацию, хранящуюся в памяти NVRAM или на хосте TFTP.

## Приглашения интерфейса CLI

Важно научиться различать приглашения во время конфигурации маршрутизатора, чтобы точно знать текущий конфигурационный режим. В следующем разделе книги мы рассмотрим приглашения, выводимые маршрутизатором Cisco. Рекомендуется обращать внимание на выведенное приглашение перед любым изменением конфигурации маршрутизатора.

Мы не стремимся сразу показать все доступные команды, но хотим на их примерах продемонстрировать различные приглашения, которые будут появляться и в других листингах этой книги.

## Интерфейсы

Для изменения в интерфейсе служит команда `interface` в режиме глобального конфигурирования:

```
Router(config)#interface?
```

|                   |                                |
|-------------------|--------------------------------|
| Async             | Async interface                |
| BVI               | Bridge-Group Virtual Interface |
| Dialer            | Dialer interface               |
| FastEthernet      | FastEthernet IEEE 802.3        |
| Group-Async       | Async Group interface          |
| Lex               | Lex interface                  |
| Loopback          | Loopback interface             |
| Multilink         | Multilink-group interface      |
| Null              | Null interface                 |
| Port-channel      | Ethernet Channel of interfaces |
| Tunnel            | Tunnel interface               |
| Virtual-Template  | Virtual Template interface     |
| Virtual-TokenRing | Virtual TokenRing              |

```
Router(config)#interface fastethernet 0/0
```

```
Router(config-if)#
```

Заметьте, что приглашение изменилось на `Router(config-if)#`, что указывает на режим конфигурирования интерфейса. Было бы неплохо показать и настраиваемый интерфейс, но этого не сделано (наверное, поэтому администраторы Cisco зарабатывают больше, чем администраторы Windows).

## Подинтерфейсы

Подинтерфейсы позволяют создавать в маршрутизаторе виртуальные интерфейсы. Приглашение меняется на Router(config-subif)# (см. главу 10 и приложение В)

```
Router(config)#intf0/0?
<0-4294967295> FastEthernet interface number
Router(config)#intf0/0.1
Router(config-subif)#
```

## Команда Line

Для настройки пароля пользовательского режима служит команда line. Приглашение становится Router (config-line)#.

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line?
<0-70> First Line number
aux Auxiliary line
console Primary terminal line
tty Terminal controller
vty Virtual terminal

Router(config)#lineconsole 0
Router(config-line)#
```

Команда line console 0 считается основной (глобальной) и любая введенная после нее команда называется подкомандой (иногда говорят, что подкоманды вводятся в приглашении config-line).

## Настройка протокола маршрутизации

Для конфигурации протокола маршрутизации (например, RIP и IGRP) используется приглашение (config-router)# (протоколы маршрутизации рассмотрены в главе 5).

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router rip
Router(config-router)#
```

**▼ ВНИМАНИЕ** | Важно понять, что делает каждая из команд в данное время. Об этом мы поговорим позже, а пока разберемся с другими доступными приглашениями.

## Возможности редактирования и вывода справки

Расширенные возможности редактирования позволят упростить настройку маршрутизатора Cisco. Ввод вопросительного знака (?) в любом приглашении всегда выводит список доступных в этом приглашении команд (назначения каждой из показанных ниже команд см. в приложении С).

```
Router#?
```

```
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
bfe For manual emergency modes setting
clear Reset functions
clock Manage the system clock
configure Enter configuration mode
connect Open a terminal connection
copy Copy configuration or image data
debug Debugging functions (see also 'undebug')
disable Turn off privileged commands
disconnect Disconnect an existing network connection
enable Turn on privileged commands
erase Erase flash or configuration memory
exit Exit from the EXEC
help Description of the interactive help system
lock Lock the terminal
login Log in as a particular user
logout Exit from the EXEC
mrinfo Request neighbor and version information from a multicast router
—More—
```

В этот момент можно нажать клавишу пробела для получения следующей страницы информации, либо нажать Return для перехода к единственной команде. Нажатие любой другой клавиши приведет к выходу из экрана справки и возвращению в приглашение ввода команд.

Для поиска сведений о команде, начинающейся на определенную букву, можно ввести эту букву, а затем вопросительный знак (?), без разделения их пробелом.

```
Router#c?
```

```
clear clock configure connect copy
```

```
Router#c
```

После ввода "c?" мы получили справку о всех командах, начинающихся на "c". Заметьте, что сохраняется приглашение Router#. Это помогает

работать с длинными командами и тогда, когда шаблон поиска выводит слишком много результатов. Было бы неправильным повторно вводить всю команду каждый раз, когда вводится вопросительный знак!

Для поиска следующей в строке команды сначала введите ее название, а затем вопросительный знак.

```
Router#clock?
 set Set the time and date

Router#clockset ?
 hh:mm:ss Current Time

Router#clock set 10:30:10 ?
 <1-31> Day of the month
 MONTH Month of the year

Router#clock set 10:30:10 28 ?
 MONTH Month of the year

Router#clock set 10:30:10 28 may ?
 <1993-2035> Year

Router#clock set 10:30:10 28 may 2000 ?
 <cr>

Router#
```

После ввода команды clock, пробела и вопросительного знака мы получили список всех возможных вариантов и их описания. Заметьте, что ввод команды, пробела и вопросительного знака нужно обязательно сделать до нажатия клавиши <cr> (carriage return, возврат каретки).

Если вести команду иначе, то мы получим сообщение об ошибке:

```
Router#clock set 10:30:10
% Incomplete command.
(незавершенная команда)
```

Командная строка не закончена. Нажмите клавишу "стрелка вверх" для получения последней введенной команды, а затем закончите командную строку вопросительным знаком.

Если же будет такое сообщение об ошибке:

```
Router(config)#access-list 110 permit host 1.1.1.1
```

```
% Invalid input detected at '^' marker.
(неправильно введенная позиция отмечена символом '^')
```

то маркер "^" будет указывать на ту часть команды, которая введена неправильно. Это помогает при вводе команд.

Если же будет получено сообщение об ошибке:

```
Router#sh te
% Ambiguous command: "sh te"
(двусмысленная команда "sh te")
```

значит не введены все ключевые слова или значения, которые обязательны для этой команды. Введите вопросительный знак, чтобы получить описание команды.

```
Router#sh?te?
```

```
WORD tech-support terminal
```

В таблице 4.1 перечислены команды редактирования, доступные в маршрутизаторе Cisco.

**Таблица 4.1.**

**Улучшенные команды редактирования**

| Команда   | Описание                                                |
|-----------|---------------------------------------------------------|
| Ctrl+A    | Перемещение курсора в начало строки                     |
| Ctrl+E    | Перемещение курсора в конец строки                      |
| Esc+B     | Перемещение курсора на одно слово назад                 |
| Ctrl+F    | Перемещение курсора вперед на один символ               |
| Esc+F     | Перемещение вперед на одно слово                        |
| Ctrl+D    | Удаление одного символа                                 |
| Backspace | Удаление одного символа                                 |
| Ctrl+R    | Повторный вывод строки                                  |
| Ctrl+U    | Стирание строки                                         |
| Ctrl+W    | Стирание слова                                          |
| Ctrl+Z    | Завершение режима конфигурирования и возвращение в EXEC |
| Tab       | Завершение ввода команды маршрутизатором                |

Следует отметить еще одну возможность редактирования — автоматическую прокрутку (перенос на другую строку) длинной команды. В следующем примере вводимая команда достигла правой границы строки и была автоматически перенесена на следующую строку с добавлением слева десяти пробелов. Символ доллара (\$) указывает на прокрутку команды влево.

```
Router#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# $ 110 permit host 171.10.10.10 0.0.0.0 host
```

Для просмотра журнала (history) введенных в маршрутизатор команд служат клавиатурные комбинации и команды, перечисленные в таблице 4.2.

**Таблица 4.2.**  
**Журнал команд маршрутизатора**

| Команда                    | Описание                                                         |
|----------------------------|------------------------------------------------------------------|
| Ctrl+P или "стрелка вверх" | Показывает последнюю введенную команду                           |
| Ctrl+N или "стрелка вниз"  | Демонстрирует предыдущую введенную команду                       |
| Show history               | По умолчанию показывает 10 последних введенных команд            |
| Show terminal              | Показывает конфигурацию терминала и размер буфера журнала команд |
| Terminal history size      | Изменяет размер буфера (максимум 256)                            |

Покажем пример команды `show history` и изменения размера журнала, а также процедуру проверки журнала командой `show terminal`.

Командой `show history` выведем 10 последних введенных в маршрутизатор команд.

```
Router#sh history
```

```
en
sh history
show terminal
sh cdp neig
sh ver
sh flash
sh int e0
sh history
sh int s0
sh int s1
```

Теперь используем `show terminal` для проверки размера журнала для терминала.

```
Router#sh terminal
```

```
Line 0, Location: "", Type: ""
```

```
[листинг сокращен]
```

```
History is enabled, history size is 10.
```

```
(журнал разрешен, его размер равен 10)
```

```
Full user help is disabled
```

```
(запрещена полная пользовательская справка)
```

```
Allowed transports are lat pad v120 telnet mop rlogin nasi. Preferred is lat.
```

```
(разрешенные транспорты: lat pad v120 telnet mop rlogin nasi.
```

```
Рекомендуется lat)
```

```
No output characters are padded
```

```
(выходные символы не дополняются)
```

```
No special data dispatching characters
```

```
(не используются специальные символы управления данными)
```

```
Group codes: 0
```

```
(код группы)
```

Команда `terminal history size` используется в привилегированном режиме и допускает изменение размера буфера журнала.

```
Router#terminal history size ?
<0-256> Size of history buffer
Router#terminal history size 25
```

Проверим изменение буфера командой `show terminal`.

```
Router#sh terminal
Line 0, Location: "", Type: ""
[листинг сокращен]
Editing is enabled.
(редактирование допустимо)
History is enabled, history size is 25.
(журнал разрешен, его размер равен 25)
Full user help is disabled
(запрещена полная пользовательская справка)
Allowed transports are lat pad v120 telnet mop rlogin nasi. Preferred is lat.
(разрешенные транспорты: lat pad v120 telnet mop rlogin nasi.
Рекомендуется lat)
No output characters are padded
(выходные символы не дополняются)
No special data dispatching characters
(не используются специальные символы управления данными)
Group codes: 0
(код группы)
```

## Сбор основной информации о маршрутизации

Команда `show version` предоставляет сведения о базовой аппаратной конфигурации системы, а также номер версии программного обеспечения, имена и источники конфигурационных файлов вместе с образом загрузки.

```
Router#sh version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(8), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by Cisco Systems, Inc.
Compiled Mon 29-Nov-99 14:52 by kpm
Image text-base: 0x03051C3C, data-base: 0x00001000
ROM: System Bootstrap, Version 11.0(10c), SOFTWARE
BOOTFLASH: 3000 Bootstrap Software (IGS-BOOT-R), Version 11.0(10c),
RELEASE SOFTWARE (fc1)

RouterA uptime is 5 minutes
(маршрутизатор А работает 5 минут)
System restarted by power-on
(система перезапущена по включению питания)
```

System image file is "flash:c2500-js-l\_120-8.bin"  
 (файл образа системы)

cisco 2522 (68030) processor (revision N) with 14336K/2048Kbytes of memory.  
 (процессор cisco 2522 (68030) обновление N с 14336К/2048К байтами памяти)

Processorboard ID 15662842, with hardware revision 00000003  
 (идентификатор процессорной платы 15662842 при аппаратном обновлении 00000003)

Bridging software.  
 (программное обеспечение для функций моста)

X.25 software, Version 3.0.0.

SuperLAT software (copyright 1990 by Meridian Technology Corp).

TN3270 Emulation software.  
 (программное обеспечение эмуляции TN3270)

Basic Rate ISDN software, Version 1.1.  
 (программное обеспечение базового уровня ISDN версии 1.1)

1 Ethernet/IEEE 802.3 interface(s)

2 Serial network interface(s)

8 Low-speed serial(sync/async) network interface(s)

1 ISDN Basic Rate interface(s)

32K bytes of non-volatile configuration memory.  
 (32 Кбайта в энергонезависимой памяти конфигурации)

16384K bytes of processor board System flash (Read ONLY)  
 (16384 Кбайта в системной памяти флэш процессорной платы для режима "только чтение")

Configuration register is 0x2102  
 (конфигурационный регистр 0x2102)

С помощью команды `show version` можно узнать, как долго работает маршрутизатор, как он был перезапущен, имя исполняемого файла IOS, версии процессора и аппаратного обеспечения, а также размер памяти DRAM. Кроме того, указано значение в конфигурационном регистре (см. главу 7).

## Установка паролей

Для защиты маршрутизатора Cisco используются пять паролей. Первые два пароля служат для установки разрешенного пароля, который защищает привилегированный режим. Пароль запрашивается у пользователя после ввода команды `enable`. Остальные три пароля служат для настройки паролей для доступа пользователя через консольный порт, вспомогательный порт и по протоколу Telnet.

### Разрешенные пароли

Для установки разрешенного пароля необходимо находиться в режиме глобального конфигурирования.

```
Router(config)#enable ?
last-resort Define enable action if no TACACS servers respond
```

|            |                                      |
|------------|--------------------------------------|
| password   | Assign the privileged level password |
| secret     | Assign the privileged level secret   |
| use-tacacs | Use TACACS to check enable passwords |

**Last-resort** (крайний случай) Используется после установки аутентификации через сервер tacacs, который недоступен. Этот режим позволяет администратору даже в этом случае войти в систему маршрутизатора. Однако подобный режим недоступен при работающем сервере tacacs.

**Password** (пароль) Служит для установки разрешенного пароля (enable password) в устаревших системах с версиями до 10.3. Не используется, если установлен разрешенный секрет (enable secret).

**Secret** (секрет) Новый зашифрованный пароль. После установки перекрывает действие разрешенного пароля.

**Use-tacacs** (использовать tacacs) Указывает маршрутизатору на аутентификацию через сервер tacacs. Это удобно, когда приходится обслуживать десятки и сотни маршрутизаторов. Как иначе изменить пароль на 200 маршрутизаторах? Сервер tacacs позволяет однократно изменить пароль, который будет действовать на все устройства.

```
Router(config)#enablesecret todd
```

```
Router(config)#enablepassword todd
```

The enable password you have chosen is the same as your enable secret.

This is **not** recommended. Re-enter the enable password.

(выбранный разрешенный пароль совпадает с разрешенным секретом.

Это не рекомендуется. Введите другой разрешенный пароль)

При попытке ввода одинакового разрешенного пароля и разрешенного секрета выводится вежливое предупреждение о недопустимости такого выбора. Однако при повторном вводе того же самого пароля, он будет установлен в маршрутизаторе даже при совпадении с разрешенным секретом. Между тем, пароли не работают одновременно. В новых маршрутизаторах (а не в старых унаследованных) можно не беспокоиться об использовании разрешенного пароля.

Пароли пользовательского режима присваиваются командой line.

```
Router(config)#line ?
```

```
<0-4> First Line number
```

```
aux Auxiliary line
```

```
console Primary terminal line
```

```
vty Virtual terminal
```

**Aux** (вспомогательный) Служит для установки пароля пользовательского режима для вспомогательного порта. Обычно применяется для настройки в маршрутизаторе параметров модема, но может служить и для доступа к консоли.

**Console** (консоль) Служит для установки пароля консоли пользовательского режима.

Vty (виртуальный терминал) Служит для установки в маршрутизаторе пароля Telnet. Если такой пароль не установлен, то по умолчанию использование Telnet запрещено.

Для настройки паролей пользовательского режима сначала конфигурируется нужная линия (line), а затем вводится команда login или no login для вывода из маршрутизатора приглашения аутентификации.

### Вспомогательный пароль

Для настройки вспомогательного пароля следует перейти в режим глобального конфигурирования и ввести line aux ?. Список выбора содержит только строку 0-0, поскольку существует один вспомогательный порт.

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line aux ?
<0-0> First Line number
Router(config)#line aux 0
Router(config-line)#login
Router(config-line)#password todd
```

Важно помнить о команде login, иначе вспомогательный порт не выведет приглашения для аутентификации.

### Пароль консоли

Для установки пароля консоли служит команда line console 0. Однако если подобно настройке вспомогательного порта ввести line console 0 ?, то вы получите ошибку. Необходимо ввести команду line console 0, причем после этого недоступен экран справки. Для возвращения на один уровень вверх следует задать "exit".

```
Router(config-line)#line console ?
% Unrecognized command
(нераспознанная команда)
Router(config-line)#exit
Router(config)#line console ?
<0-0> First Line number
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password todd1
```

Поскольку существует только один консольный порт, доступен вариант line console 0.

### Другие команды консольного порта

Существует еще несколько важных команд для консольного порта, которые следует запомнить.

Команда `exec-timeout 0 0` устанавливает в ноль время тайм-аута консольного сеанса EXEC (т.е. тайм-аут запрещен). Можно разыграть своих коллег по работе, установив тайм-аут в значение `0 1`, что приведет к прерыванию терминального сеанса через каждую секунду! Избежать прерывания сеанса в этом случае позволит постоянное нажатие клавиши "стрелка вниз" при вводе изменения времени тайм-аута другой рукой.

Команда `logging synchronous` должна была бы быть установлена по умолчанию, но этого не сделано. Команда запрещает вывод консольных сообщений, которые прерывают ввод команд в консольном режиме. Это упростит чтение и ввод сообщений в маршрутизатор.

Примеры упомянутых команд:

```
Router(config)#line con 0
Router(config-line)#exec-timeout ?
 <0-35791> Timeout in minutes
 (тайм-аут в минутах)
Router(config-line)#exec-timeout 0 ?
 <0-2147483> Timeout in seconds
 (тайм-аут в секундах)
 <cr>
Router(config-line)#exec-timeout 0 0
Router(config-line)#logging synchronous
```

## Пароль Telnet

Для установки пароля пользовательского режима при доступе по Telnet к маршрутизатору служит команда `line vty`. Маршрутизаторы, которые не исполняют версию Enterprise операционной системы Cisco IOS, по умолчанию имеют пять линий VTY (от 0 до 4). Однако в версии Enterprise таких линий намного больше — 198 (0 — 197). Проще всего узнать количество линий с помощью вопросительного знака.

```
Router(config-line)#line vty 0 ?
 <1-197> Last Line Number
 <cr>
Router(config-line)#line vty 0 197
Router(config-line)#login
Router(config-line)#password todd2
```

Если попытаться установить сеанс Telnet с маршрутизатором, не имеющим заданных паролей для линий VTY, то будет получено сообщение об ошибке "подключение прервано, поскольку не установлен пароль". Можно указать маршрутизатору на разрешение подключений по Telnet без пароля, использовав команду `no login`.

```
Router(config-line)#line vty 0 197
Router(config-line)#no login
```

После настройки IP-адреса маршрутизатора можно использовать программу Telnet для конфигурирования и проверки устройства вместо выполнения этих операций через консольный порт. Для запуска программы Telnet следует ввести в командной строке telnet (в DOS или Cisco). Протокол Telnet подробно рассмотрен в главе 7.

### Шифрование паролей

По умолчанию шифруется только пароль разрешенного секрета. Можно вручную установить режим- шифрования для пользовательского режима и разрешенного пароля.

Заметим, что выполнение в маршрутизаторе команды show running-config позволяет увидеть все пароли за исключением разрешенного секрета.

```
Router#sh run
[листинг сокращен]
!
enable secret 5 1rFbM$8.aXocHg6yHrM/zzeNkAT.
enable password todd1
[
[листинг сокращен]
line con 0
password todd1
login
line aux 0
password todd
login
line vty 0 4
password todd2
login
line vty 5 197
password todd2
login
!
end
Router#
```

Для шифрования паролей вручную следует выполнить команду service password-encryption. Пример шифрования пароля вручную:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#service password-encryption
Router(config)#enable password todd
Router(config)#line vty 0 197
```

```
Router(config-line)#login
Router(config-line)#password todd2
Router(config-line)#line con 0
Router(config-line)#login
Router(config-line)#password todd1
Router(config-line)#line aux 0
Router(config-line)#login
Router(config-line)#password todd
Router(config-line)#exit
Router(config)#no service password-encryption
Router(config)#^Z
```

После ввода команды `show running-config` мы увидим, что зашифрованы разрешенный пароль и пароли линий.

```
Router#sh run
Building configuration...
(построение конфигурации)
[листинг сокращен]
!
enable secret 5 1rFbM$8.aXocHgbyHrM/zzeNkAT.
enablepassword70835434AOD
!
[листинг сокращен]
!
line con 0
 password 7 111D160113
 login
line aux 0
 password 7 071B2E484A
 login
line vty 0 4
 password 7 0835434AOD
 login
line vty 5 197
 password 7 09463724B
 login
!
end
Router#
```

## Баннеры

В маршрутизаторе Cisco допускается установка баннера (banner — приветственное сообщение), чтобы выводить его во время регистрации (входа) пользователя в систему маршрутизатора или администрирования этого устройства во время сеанса Telnet, например, баннер может выводить дополнительную справочную информацию (обычно баннеры изменяют для того, чтобы вид баннера по умолчанию не позволил злоумышленнику определить тип и модель обнаруженного в сети устройства, — Прим. пер.). Еще одной причиной изменения баннера является добавление предупреждения о защите для пользователей, обращающихся к устройству удаленно по объединенной сети. Доступны четыре разных баннера (в переводе на русский язык):

```
Router(config)#banner?
```

```
LINE c текст_баннера c, где 'c' является символом-разделителем
exec Установка баннера для EXEC-процесса
incoming Установка входного баннера для терминальной линии
Login Установка баннера входа в систему (регистрации)
motd Установка баннера Message of the Day (ежедневного сообщения)
```

Чаще всего используется баннер Message of the Day, который выводится всем людям, подключающимся (в том числе по коммутируемым линиям) к маршрутизатору по Telnet, вспомогательному порту или консольному порту.

```
Router(config)#banner motd ?
```

```
LINE c banner-text c, where 'c' is a delimiting character
```

```
Router(config)#banner motd #
```

```
Enter TEXT message. End with the character '#'.

```

```
$ized to be in Acme.com network, then you must disconnect immediately.

```

```
ft

```

```
Router(config)#^Z
```

```
Router#
```

```
00:25:12: %SYS-5-CONFIG_I: Configured from console by console

```

```
Router#exit

```

```
Router con0 is now available

```

```
Press RETURN to get started.

```

```
If you are not authorized to be in Acme.com network, then you must disconnect immediately.

```

```
(если вы не авторизованы в сети Acme.com, то будете немедленно отключены)

```

```
Router>

```

Показанный баннер MOTD сообщает, что для подключения к маршрутизатору нужно пройти авторизацию. В противном случае произойдет отключение. Следует отметить использование разделителя. Можно поменять любой символ, который укажет маршрутизатору на завершение

сообщения. Следовательно, разделитель нельзя использовать в тексте баннера. Кроме того, для указания на завершение сообщения следует сначала нажать Return, затем ввести разделитель, а далее снова нажать Return. Если сделать иначе, то баннер тоже будет создан, но когда используются несколько баннеров, то они будут объединены в одно однострочное сообщение.

Другие типы баннеров:

**Баннер Eexec** Можно настроить баннер активизации линии (line-activation, eexec) для вывода при создании процесса EEXEC (например, для активизации линии или для входного подключения к линии VTU).

**Входной баннер** (incoming banner) Можно настроить баннер для вывода на терминале, подключенном по обратной линии Telnet. Этот баннер полезен для сообщения пользователю инструкций по использованию обратной процедуры Telnet.

**Баннер регистрации** (login banner) Можно настроить баннер регистрации для вывода на всех подключенных терминалах. Этот баннер появляется после баннера MOTD, но перед приглашением регистрации (входа в систему). Баннер регистрации нельзя отменить для отдельной линии. Для полного отказа от баннера регистрации следует удалить его командой по banner login.

## Интерфейсы маршрутизатора

Конфигурация интерфейсов является важнейшей процедурой маршрутизатора. Без интерфейсов маршрутизатор бесполезен. Конфигурация интерфейсов должна взаимодействовать с другими устройствами. Среди конфигурационных параметров интерфейса: адрес сетевого уровня, тип носителя, полоса пропускания и другие административные характеристики.

Разные маршрутизаторы используют различные методы выбора интерфейсов. Например, ниже показана команда для маршрутизатора серии 2522 с 10-ю последовательными интерфейсами (от 0 до 9):

```
Router(config)#intserial?
```

```
<0-9> Serial interface number
```

После этого следует выбрать конфигурируемый интерфейс, затем мы попадаем в конфигурацию этого интерфейса. Например, команда выбора последовательного порта 5:

```
Router(config)#intserial 5
```

```
Router(config)-if)#
```

Маршрутизатор 2522 имеет один порт Ethernet IOBaseT. Ввод interface ethernet 0 начнет настройку этого интерфейса.

```
Router(config)#intethernet?
```

```
<0-0> Ethernet interface number
```

```
Router(config)#int ethernet 0
Router(config-if)#
```

Маршрутизатор серии 2500 имеет фиксированную конфигурацию, т.е. после покупки нельзя изменить состав этого устройства. Для настройки интерфейса нужно всегда использовать присвоенный интерфейсу порядковый номер. Однако маршрутизаторы серий 2600, 3600, 4000 и 7000 применяют физические слоты и номера портов для вставки в слоты съемных модулей. Например, в маршрутизаторе 2600 для конфигурирования нужно ввести interface type slot/port:

```
Router(config)#int fastethernet ?
<0-1> FastEthernet interface number
Router(config)#int fastethernet 0
% Incomplete command.
Router(config)#int fastethernet 0?
/
Router(config)#int fastethernet 0/?
<0-1> FastEthernet interface number
```

Заметим, что недопустим ввод int fastethernet 0. Следует ввести полную команду с фрагментом type slot/port или int fastethernet 0/0. Кроме того, разрешено указать type int fa 0/0.

Для установки типа подключения служит команда media-type. Однако обычно этот тип определяется автоматически.

```
Router(config)#int fa 0/0
Router(config-if)#media-type?
IOBaseX Use RJ45 for -TX; SC FO for -FX
MII Use MII connector
```

## Включение интерфейса

Выключить интерфейс позволяет команда shutdown, а включить — no shutdown. Выключенные интерфейсы показаны с признаком "административно выключен" (administratively down) в выводе команды show interface. Однако команда show running-config продемонстрирует такие интерфейсы с признаком "выключено" (shut down). Все интерфейсы по умолчанию выключены.

```
Router#sh int e0
Ethernet0 is administratively down, line protocol is down
[листинг сокращен]
```

Включение интерфейса командой no shutdown:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int e0
Router(config-if)#no shutdown
Router(config-if)#^Z
```

```
00:57:08: %LINK-3-UPDOWN: Interface Ethernet0, changed state to up
00:57:09: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0,
changed state to up
```

```
Router#sh inte0
Ethernet0 is up, line protocol is up
```

## Настройка IP-адреса интерфейса

Не обязательно использовать протокол IP в маршрутизаторе, однако он применяется во всех маршрутизаторах. Для настройки IP-адреса интерфейса служит команда `ip address` в режиме конфигурирования интерфейса.

```
Router(config)#inte0
Router(config-if)#ip address 172.16.10.2 255.255.255.0
Router(config-if)#no shut
```

Не забудьте включить интерфейс командой `no shut`. Например, проверить включение можно с помощью команды `show interface e0`. Она покажет состояние данного интерфейса (выключен или включен административно). Команда `show running-config` тоже покажет выключенные интерфейсы.

Если требуется добавить интерфейсу второй адрес подсети, следует применить команду `secondary`. Если ввести другой IP-адрес и нажать `Enter`, то будет заменен существующий IP-адрес и маска подсети. Для добавления второго IP-адреса используйте команду `secondary`.

```
Router(config-if)#ip address 172.16.20.2 255.255.255.0 secondary
Router(config-if)#^Z
```

Проверить конфигурирование обоих адресов интерфейса можно с помощью команды `show running-config` (сокращенная форма: `sh run`).

```
Router#sh run
Building configuration...
Current configuration:
[листинг сокращен]
!
interface Ethernet0
 ip address 172.16.20.2 255.255.255.0 secondary
 ip address 172.16.10.2 255.255.255.0
```

## Карты VIP

В маршрутизаторах серий 7000 и 7500 с картами VIP (Versatile Interface Processor — многоцелевой интерфейсный процессор) определение интерфейса выполняется командой `interface type slot/port adapter/port number`, например:

```
7000(config)#interface ethernet 2/0/0
```

## Команды последовательного интерфейса

Для настройки последовательного интерфейса нужно знать его особенности. Интерфейс подключается к устройству типа CSU/DSU, которое обеспечивает тактовую частоту в линии. Однако если в лабораторной среде используется конфигурации "один к одному", то только один участник соединения должен предоставлять тактовую частоту. Это может быть окончное кабельное устройство DCE. Маршрутизатор Cisco по умолчанию является устройством DTE, поэтому необходимо явно указать интерфейсу на предоставление тактовой частоты, если этот интерфейс работает в режиме DCE. Настройка последовательного интерфейса на режим DCE выполняется командой `clock rate` (уровень тактовой частоты).

```
Router#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#ints0
```

```
Router(config-if)#clockrate ?
```

```
Speed (bits per second)
```

```
1200
```

```
2400
```

```
4800
```

```
9600
```

```
19200
```

```
38400
```

```
56000
```

```
64000
```

```
72000
```

```
125000
```

```
148000
```

```
250000
```

```
500000
```

```
800000
```

```
1000000
```

```
1300000
```

```
2000000
```

```
4000000
```

```
<300-4000000> Choose clockrate from list above
```

```
Router(config-if)#clock rate 64000
```

```
%Error: This command applies only to DCE interfaces
```

```
(ошибка: эта команда применима только для интерфейса DCE)
```

```
Router(config-if)#ints1
```

```
Router(config-if)#clock rate64000
```

Установка тактовой частоты в интерфейсе не приведет ни к каким поломкам, но нужно знать, что команда `clock rate` предполагает значение в битах в секунду.

Кроме того, следует знать о команде `bandwidth`. Любой маршрутизатор Cisco поставляется с установленной в последовательных интерфейсах полосой пропускания для линии T1 (т.е. скорости 1.544 Мбит/с). Однако это никак не влияет на скорость пересылки данных по линии. Значение полосы пропускания используется в протоколах маршрутизации IGRP, EIGRP и OSPF для вычисления наилучшей стоимости пути к удаленной сети. Если применяется маршрутизация RIP, то значение полосы пропускания не учитывается.

```
Router(config-if)#bandwidth?
<1-10000000> Bandwidth in kilobits
Router(config-if)#bandwidth 64
```

В отличие от команды `clock rate`, команда `bandwidth` устанавливает значение в килобитах.

## Имена хостов

Для установки имени хоста в маршрутизаторе служит команда `hostname`. Это имя действует локально, т.е. не учитывается во время просмотра маршрутизатором имен в объединенной сети.

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname todd
todd(config)#hostname Atlanta
Atlanta(config)#
```

Хотя кажется, что лучше выбрать для имени хоста собственное имя, рекомендуется именовать маршрутизаторы по географическому признаку.

## Описание

Установка описания интерфейса поможет администратору, но, как и имя хоста, описание действует только локально. В нем можно указать дополнительные характеристики интерфейса, например номер цепи.

```
Atlanta(config)#inteO
Atlanta(config-if)#descriptionSales Lan
Atlanta(config-if)#intsO
Atlanta(config-if)#descWan to Miami circuit:6fdda4321
```

Для просмотра описания интерфейса служат команды `show running-config` и `show interface`.

```
Atlanta#sh run
[листинг сокращен]
interface Ethernet0
```

```

description Sales Lan
ip address 172.16.10.30 255.255.255.0
no ip directed-broadcast
[
interface Serial0
description Wan to Miami circuit:6fdda4321
no ip address
no ip directed-broadcast
no ip mroute-cache

Atlanta#sh inteO
EthernetO is up, line protocol is up
Hardware is Lance, address is 0010.7be8.25db (bia 0010.7be8.25db)
Description: Sales Lan
[листинг сокращен]

Atlanta#sh int sO
SerialO is up, line protocol is up
Hardware is HD64570
Description: Wan to Miami circuit:6fdda4321
[листинг сокращен]
Atlanta#

```

## Просмотр и сохранение конфигурации

Пройдя все операции процедуры установки, мы получим приглашение на сохранение созданной конфигурации. Если ответить yes, то конфигурация будет записана в память DRAM (т.е. станет исполняемой конфигурацией), в память NVRAM или в файл с именем `startup-config`.

Можно вручную скопировать файл из DRAM в NVRAM командой `copy running-config startup-config`. Краткая форма данной команды: `copy run start also`.

```

Router#copy run start
Destination filename [startup-config]?return
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
(предупреждение: попытка перезаписать в NVRAM конфигурацию,
записанную из другой версии образа системы)
Overwrite the previous NVRAM configuration?[confirm]return
(перезаписать предыдущую конфигурацию в NVRAM)
Building configuration...
(построение конфигурации)

```

Обратите внимание, что сообщение говорит о попытке записи поверх старой конфигурации `startup-config`. Операционная система IOS была обновлена до версии 12.8, но при последнем сохранении файла использовалась версия 11.3.

Для просмотра файла используйте команду `show running-config` или `show startup-config` в привилегированном режиме. Команда `sh run` (краткая форма `show running-config`) укажет на просмотр текущей конфигурации.

```
Router#sh run
Building configuration...

Current configuration:
!
```

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router
ip subnet-zero
frame-relay switching
```

[листинг сокращен]

Команда `sh start` (краткая форма `show startup-config`) покажет конфигурацию, которая будет использоваться при следующей перезагрузке маршрутизатора, а также выведет объем памяти NVRAM для хранения файла `startup-config`.

```
Router#sh start
Using 4850 out of 32762 bytes
```

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router
```

```
!
!
ip subnet-zero
frame-relay switching
```

[листинг сокращен]

Можно удалить файл `startup-config` командой `erase startup-config`. После этого выводится ошибка при попытке просмотра файла конфигурации запуска (`startup-config`).

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

```
[OK]
Erase of nvram: complete
Router#sh start
%% Non-volatile configuration memory is not present
(нет энергонезависимой памяти конфигурации)
Router#
```

## Проверка конфигурации

Разумеется, лучше всего проверить конфигурацию во время просмотра командой `show running-config`. С помощью команды `show startup-config` можно проверить конфигурацию, установленную для загрузки при следующем перезапуске маршрутизатора.

Однако после проверки исполняемой конфигурации `running-config`, когда все будет в порядке, можно дополнительно проверить конфигурацию утилитами `Ping` и `Telnet`.

Проверить по `Ping` другой протокол позволит ввод `ping ?` в пользовательском или привилегированном режиме маршрутизатора.

```
Router#ping?
WORD Ping destination address or hostname
appletalk Appletalk echo
decnet DECnet echo
ip IP echo
ipx Novell/IPX echo
srb srb echo
<cr>
```

Для поиска адреса сетевого уровня соседнего устройства следует переместиться к маршрутизатору или переключателю, либо ввести `show cdp nei detail` для получения сведений об адресе сетевого уровня, по которому будет обращаться утилита `Ping`.

Можно использовать программу `Trace` для поиска пути, по которому движутся пакеты в объединенной сети. Допускается трассировка по нескольким протоколам.

```
Router#trace?
WORD Trace route to destination address or hostname
appletalk AppleTalk Trace
clns ISO CLNS Trace
ip IP Trace
oldvines Vines Trace (Cisco)
vines Vines Trace (Banyan)
<cr>
```

Большие возможности имеет Telnet. Эта утилита использует протокол IP на сетевом уровне и TCP на транспортном уровне для создания сеанса с удаленным хостом. Если можно обратиться к устройству по Telnet, следовательно, корректно подключение по IP. По Telnet можно обращаться только к IP-адресам, но допустимо использование хостов Windows или приглашения маршрутизаторов для применения утилиты Telnet.

```
Router#telnet?
WORDIP-адрес or hostname of a remote system
<cr>
```

В приглашении маршрутизатора не обязательно вводить команду telnet. Если ввести имя хоста или IP-адрес, то по умолчанию предполагается использование Telnet.

### Проверка командой Show Interface

Еще один способ проверки конфигурации связан с использованием команды show interface. Сначала рекомендуется ввести show interface ?, чтобы увидеть все доступные для конфигурации интерфейсы. Единственные интерфейсы, которые не подчиняются общим правилам, — это Ethernet и Serial (последовательный).

```
Router#sh int ?
Ethernet IEEE 802.3
Null Null interface
Serial Serial
accounting Show interface accounting
crb Show interface маршрутизация/bridging info
irb Show interface маршрутизация/bridging info
<cr>
```

Следующая команда show interface ethernet 0 покажет аппаратный адрес, логический адрес и метод инкапсуляции, а также статистические данные о конфликтах.

```
Router#sh int e0
Ethernet0 is up, line protocol is up
Hardware is Lance, address is 0010.7b7f.c26c (bia 0010.7b7f.c26c)
Internet address is 172.16.10.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:08:23, output 00:08:20, 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
25 packets input, 2459 bytes, 0 no buffer
Received 25 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
33 packets output 7056 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

```

Наиболее важными в листинге команды `show interface` являются сведения о выходных линиях и о статусе протокола канального уровня. Если включен интерфейс `Ethernet 0`, то включены протоколы линии. Кроме того, работает сама линия.

```

RouterA#sh int e0
Ethernet0 is up, line protocol is up

```

Первый параметр относится к физическому уровню. Он включен, когда приемник это обнаружил. Второй параметр связан с канальным уровнем и указывает на время поддержания жизни (`keepalive`) на другом конце связи.

```

RouterA#sh int s0
Serial0 is up, line protocol is down

```

Если линия включена, но выключен протокол, возникают проблемы с тактовой частотой (`keepalive`) или кадрами. Проверьте значение параметра `keepalive` на обоих концах связи. Эти значения должны совпадать, должны быть установлены тактовые импульсы (при необходимости) и совпадать тип инкапсуляции на обоих концах соединения.

```

RouterA#sh int s0
Serial0 is down, line protocol is down

```

Если же выключены линия и протокол, то проблемы связаны с кабелем или с интерфейсом. Кроме того, если один конец связи выключен административно, то следует выключить и удаленный конец. Для включения интерфейса введите команду `no shutdown` in interface configuration.

```

RouterB#sh int s0
Serial0 is administratively down, line protocol is down

```

Следующая команда демонстрирует последовательную линию с установленным по умолчанию значением `MTU` (`Maximum Transmission Unit` — максимальный передаваемый элемент) равным 1500 байт. Кроме того, по умолчанию на всех последовательных линиях Cisco полоса пропускания (`BW`, `bandwidth`) равна 1.544 Kbs (Кбит/с). Это значение служит для подсчета полосы пропускания в протоколах маршрутизации

IGRP, EIGRP и OSPF. Еще один важный конфигурационный параметр — время поддержания жизни (keepalive) по умолчанию равен 10 с. Любой маршрутизатор посылает своему соседу сообщение keepalive через каждые 10 с. Если оба маршрутизатора не настроены на одинаковый интервал keepalive, то поддержание жизни не получится.

Для очистки счетчиков в интерфейсе служит команда clear counters.

```
Router#sh ints0
```

```
Serial0 is up, line protocol is up
```

```
Hardware is HD64570
```

```
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation HDLC, loopback not set keepalive set (10 sec)
```

```
Last input never, output never, 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
```

```
0 packets input, 0 bytes, 0 no buffer
```

```
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
```

```
0 packets output, 0 bytes, 0 underruns
```

```
0 output errors, 0 collisions, 16 interface resets
```

```
0 output buffer failures, 0 output buffers swapped out
```

```
0 carrier transitions
```

```
DCD=down DSR=down DTR=down RTS=down CTS=down
```

```
Router#clear counters ?
```

```
Ethernet IEEE 802.3
```

```
Null Null interface
```

```
Serial Serial
```

```
<cr>
```

```
Router#clear counters s0
```

```
Clear "show interface" counters on this interface [confirm]return
```

```
Router#
```

```
00:17:35: %CLEAR-5-COUNTERS: Clear counter on interface
```

```
Serial0 by console
```

```
Router#
```

## Использование команды Show Controllers

Команда show controllers показывает сведения о самом физическом интерфейсе. Она также выводит тип последовательного кабеля, подключенного к порту. Обычно таким кабелем является только кабель DTE, который подключается к интерфейсу в режиме DSU (Data Service Unit).

```
Router#sh controllers s 0
```

```
HD unit 0, idb = 0x1229E4, driver structure at 0x127E70
buffer size 1524 HD unit 0, V.35 DTE cable
cpb = 0xE2, eda = 0x4140, cda = 0x4000
```

```
Router#sh controllers s 1
```

```
HD unit 1, idb = 0x12C174, driver structure at 0x131600
buffer size 1524 HD unit 1, V.35 DCE cable
cpb = 0xE3, eda = 0x2940, cda = 0x2800
```

**Заметим**, что интерфейс serial 0 имеет кабель DTE, хотя к serial 1 подключен кабель DCE. Интерфейс serial 1 будет обеспечивать в линии тактовую частоту, установленную командой clock rate. Но интерфейс serial 0 будет получать тактовые импульсы от кабеля DSU. Следует помнить, что это единственная команда, после которой необходим пробел.

```
Router#sh controllers s 1
```

```
% Invalid input detected at '^' marker.
```

## Упражнение

Напишите команду (команды), решающую поставленную задачу.

1. Установить последовательный интерфейс в режим предоставления тактовой частоты 64к другому маршрутизатору.
2. Во время обращения по Telnet к маршрутизатору получен ответ "connection refused, password not set" (соединение прервано, пароль не установлен). Отмените вывод сообщения и приглашение для ввода пароля.
3. Введена команда show inter et 0 и показано, что порт административно выключен. Что делать дальше?
4. Нужно удалить конфигурацию в NVRAM.
5. Нужно установить пароль пользовательского режима для консольного порта.
6. Нужно установить пароль разрешенного секрета в значение cisco.
7. Нужно проверить, следует ли последовательному интерфейсу предоставлять тактовую частоту в линию.
8. Нужно узнать размер журнала терминала.
9. Какая устаревшая команда Cisco изменяет конфигурацию, хранящуюся на хосте TFTP?
10. Установите имя маршрутизатора в значение Chicago?

## Лабораторные работы

В этом разделе нужно вводить команды в маршрутизатор Cisco, чтобы лучше понять их предназначение. Достаточно одного маршрутизатора Cisco, но лучше использовать два или три.

### О Лабораторная работа 4.1.

#### Регистрация в маршрутизаторе

1. Нажмите Return для подключения к маршрутизатору. Мы попадем в пользовательский режим.
2. В приглашении Router> введите вопросительный знак (?).
3. Обратите внимание на — more — внизу экрана.
4. Нажмите Enter для построчного просмотра команд.
5. Нажмите пробел для поэкранного просмотра команд.
6. В любое время можно ввести q для выхода.
7. Введите enable или en, затем нажмите Enter. Мы перейдем в привилегированный режим, где можно просмотреть и изменить конфигурацию маршрутизатора.
8. В приглашении Router# введите вопросительный знак (?). Обратите внимание на количество команд привилегированного режима.
9. Введите q для выхода.
- 10.** Введите **config** и нажмите Enter.
- 11.** Нажмите Enter для конфигурации маршрутизатора с терминала.
12. В приглашении Router(config)# введите вопросительный знак (?), затем q для выхода или пробел для просмотра команд.
13. Введите interface e0 или **int** e0 и нажмите Enter. Это позволит перейти к настройке интерфейса Ethernet 0.
14. В приглашении Router(config-if)# введите вопросительный знак (?).
15. Введите **int s0** или interface s0 (команда interface serial 0) и нажмите Enter. Это позволит сконфигурировать интерфейс serial 0. Обратите внимание на простоту перехода между интерфейсами.
- 16.** Введите **encapsulation?**.
- 17.** Введите exit. Это вернет нас на один уровень назад.
- 18.** Одновременно нажмите клавиши Control и Z. Мы перейдем из режима конфигурации обратно в привилегированный режим.
- 19.** Введите disable. Мы перейдем в пользовательский режим.
20. Введите exit, что приведет к выходу из маршрутизатора.

<> Лабораторная работа 4.2.  
*Использование редактирования  
и возможностей справки*

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, введя **en** или **enable**.
2. Введите вопросительный знак (?).
3. Введите **cl?** и нажмите Enter. Будут показаны все команды, начинающиеся на "cl".
4. Введите **clock ?** и нажмите Enter.

**▼ВНИМАНИЕ**

Обратите **внимание** на различие между п. 3 и 4. В пункте 3 мы ввели символы **без** пробела и вопросительный знак, чтобы показать все **команды**, начинающиеся на "cl". В пункте 4 мы ввели команду, пробел и вопросительный знак, чтобы увидеть следующую доступную команду.

5. Установите тактовую частоту маршрутизатора командой **clock ?**, следуя инструкциям на выведенном экране справки, затем задайте дату и время в маршрутизаторе.
6. Введите **clock ?**.
7. Введите **clock set ?**.
8. Введите **clock set 10:30:30 ?**.
9. Введите **clock set 10:30:30 14 March ?**.
10. Введите **clock set 10:30:30 14 March 2001**.
11. Нажмите Enter.
12. Введите **show clock**, чтобы увидеть дату и время.
13. В привилегированном режиме введите **show access-list 10**. Не нажимайте Enter.
14. Нажмите **Ctrl+A**. Это вернет нас в начало строки.
15. Нажмите **Ctrl+E**. Это вернет курсор в конец строки.
16. Нажмите **Ctrl+A**, затем **Ctrl+F**. Это приведет к переходу вперед на один символ.
17. Нажмите **Ctrl+B**, чтобы вернуться на один символ назад.
18. Нажмите **Return**, затем **Ctrl+P**. Это повторит последнюю команду.
19. Нажмите на клавиатуре клавишу "стрелка вверх". Это тоже приведет к повторению последней команды.
20. Введите **sh history**. Будут показаны 10 последних введенных команд.

21. Введите **terminal history size ?**. Это изменит размер журнала.
22. Введите **show terminal** для показа статистики терминала и размера его журнала.
23. Введите **terminal no editing**. Это отключит улучшенные возможности редактирования. Повторите п. 14 — 18, чтобы увидеть отсутствие влияния клавиатурных комбинаций во время редактирования терминального ввода.
24. Введите **terminal editing** и нажмите Enter для восстановления улучшенных возможностей редактирования.
25. Введите **sh run**, затем нажмите клавишу Tab. Это приведет к автозавершению ввода команды.
26. Введите **sh star**, затем нажмите клавишу Tab. Это приведет к автозавершению ввода команды.

## О Лабораторная работа 4.3.

### *Сохранение конфигурации маршрутизатора*

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, введя **en** или **enable**, затем нажав Enter.
2. Для просмотра конфигурации из NVRAM введите **sh start** и нажмите Tab и Enter, либо введите **show startup-config** и нажмите Enter. Однако если конфигурация не была сохранена, то появится сообщение об ошибке.
3. Для сохранения конфигурации в NVRAM (конфигурации запуска **startup-config**) можно сделать одно из следующего:
  - Введите **copy run start** и нажмите Enter.
    - Введите **copy running**, нажмите Tab, введите **start**, нажмите Tab, затем нажмите Enter.
    - Введите **copyrunning-config startup-config** и нажмите Enter.
4. Введите **sh start**, нажмите Tab, затем нажмите Enter.
5. Введите **sh run**, нажмите Tab, затем нажмите Enter.
6. Введите **erase start**, нажмите Tab, затем нажмите Enter.
7. Введите **sh start**, нажмите Tab, затем нажмите Enter. Должно появиться сообщение об ошибке.
8. Введите **reload** и нажмите Enter. Подтвердите перезапуск, нажав Enter. Подождите пока перезапустится маршрутизатор.
9. Укажите по в приглашении перехода к режиму установки либо нажмите **Ctrl+C**.

## О Лабораторная работа 4.4.

### Установка паролей

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, введя `en` или `enable`.
2. Введите `config t` и нажмите Enter.
3. Введите `enable ?`.
4. Установите пароль разрешенного секрета, введя `enable secret password` (слово `password` должно быть заменено на Ваш личный пароль) и нажмите Enter. Не добавляйте команду `password` после команды `secret` (это сделает паролем слово `password`). В примере мы будем использовать пароль `todd` для разрешенного секрета.
5. Проверим, что произойдет с маршрутизатором после выхода и последующего входа в систему. Выйдите, нажав `Ctrl+Z`, затем введите `exit` и нажмите Enter. Перейдите в привилегированный режим. Перед входом в этот режим будет запрошен пароль. Если успешно ввести секретный пароль, то можно продолжить работу.
6. Удалите секретный пароль. Перейдите в привилегированный режим, введите `config t` и нажмите Enter. Введите `no enable secret` и нажмите Enter. Выйдите и снова войдите в систему, причем опять будет запрошен пароль.
7. Еще один пароль для входа в привилегированный режим называется разрешенным паролем. Это старый и менее защищенный пароль, который не используется, если установлен секретный пароль. Пример установки разрешенного пароля:  

```
config t
enable password todd1
```
8. Обратите внимание, что разрешенный секрет и разрешенный пароль отличаются друг от друга. Они не могут быть одинаковыми.
9. Введите `config t`, чтобы перейти на нужный уровень для установки консольного и вспомогательного пароля, затем введите `line ?`.
10. Обратите внимание на вывод команды `line` для паролей вспомогательного порта, `vty` и консоли. Мы установим все три пароля.
11. Для установки пароля Telnet (пароля `vty`) введите `line vty 0 4` и нажмите Enter. Значение `0 4` показывает пять доступных виртуальных линий для подключения по Telnet. В версии Enterprise IOS число линий может быть иным. Введите вопросительный знак, чтобы определить последнюю из доступных линий маршрутизатора.
12. Следующая команда служит для включения или выключения аутентификации. Введите `login` и нажмите Enter для вывода приглашения ввода пароля пользовательского режима при обращении к маршрутизатору по Telnet. Нельзя использовать этот протокол для доступа, если не установлен соответствующий пароль.

**Т ВНИМАНИЕ** Можно применить команду по login для отключения в сеансе Telnet приглашения для ввода пароля пользовательского режима.

13. Еще одна команда нужна для установки пароля vty в значение password. Введите password *password* для установки пароля (слово *password* нужно заменить собственным паролем).

**14.** Пример установки пароля VTY:

```
Config t
Line vty 0 4
Login
Password todd
```

15. Установите вспомогательный пароль, предварительно введя line auxiliary 0 или line **aux** 0.

16. Введите Login.

**17.** Введите password *password*.

18. Установите пароль консоли, предварительно введя line console 0 или line con 0.

19. Введите login.

20. Введите password *password*. Пример использования обеих команд:

```
Config t
Line con 0
Login
Password todd1
Line aux 0
Login
Password todd
```

21. Можно применить команду Exec-timeout 0 0 к линии console 0. Это отменит тайм-аут консоли и приведет к выходу из терминального режима. Пример этой команды:

```
config t
line con 0
login
password todd2
exec-timeout 0 0
```

22. Установите режим запрета перезаписи сообщениями консоли вводимой команды, используйте logging synchronous.

```
config t
line con 0
logging synchronous
```

## О Лабораторная работа 4.5.

### *Настройка имени хоста, описания, IP-адреса и тактовой частоты*

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, введя **en** или **enable**.
2. Установите для маршрутизатора имя хоста командой `hostname`. Обратите внимание, что команда состоит из одного слова. Пример установки имени хоста:  

```
Router#config t
Router(config)#hostname RouterA
RouterA(config)#
```

Имя хоста в маршрутизаторе изменится после нажатия на клавишу Enter.

3. Установите баннер для сетевого администратора командой `banner`.
4. Введите **config t, banner ?**.
5. Можно ввести разные баннеры. Мы рассмотрим только баннеры входа в систему и Message of the Day (MOTD).
6. Установите баннер MOTD, который выводится при подключении к консольному порту маршрутизатора, вспомогательному порту или по Telnet. Для этого введите:

```
config t
banner motd #
This is an motd banner (это баннер MOTD)
#
```

7. В предыдущем примере в качестве разделителя использовался символ `#`. Он указывает маршрутизатору на конец текста баннера. Нельзя использовать символ-разделитель внутри баннера.
8. Удалите баннер MOTD:  

```
config t
no banner motd
```
9. Установите баннер входа в систему (login banner):  

```
config t
banner login #
This is a login banner (это баннер входа в систему)
ff
```

10. Баннер входа в систему выводится сразу же после баннера MOTD, но перед приглашением для ввода пароля пользовательского режима. Запомните, что для установки паролей пользовательского режима нужно ввести пароли консоли, вспомогательного порта и линии vty.

11. Можно удалить баннер входа в систему:

```
config t
no banner login
```

12. Добавить в интерфейс IP-адрес позволяет команда IP address. Сначала следует перейти в режим конфигурации, а затем ввести команду, например:

```
config t
int e0 (можно вводить int Ethernet0 too)
ip address 1.1.1.1 255.255.0.0
no shutdown
```

IP-адрес (1.1.1.1) и маска подсети (255.255.0.0) присваиваются в одной строке. Команда no shutdown (краткая форма no shut) служит для разрешения (включения) интерфейса. По умолчанию выключены все интерфейсы.

13. Идентификатор интерфейса добавляется командой description. Она используется для указания описания подключения. Это описание выводится только администраторам, но не пользователям. Пример:

```
config t
int s0
ip address 1.1.1.2 255.255.0.0
no shut
description Wan link to Miami
```

(описание: линия региональной сети в Майами)

14. Последовательной линии можно присвоить полосу пропускания, а также значение тактовой частоты для линий DCE региональных сетей (WAN). Пример:

```
config t
int s0
bandwidth 64
clock rate 64000
```

## Проверочные вопросы

---

- Откуда по умолчанию загружается IOS при первом запуске маршрутизатора?
  - Boot ROM
  - NVRAM
  - Флэш-память
  - ROM
- Какие два способа позволяют войти в режим установки маршрутизатора?

- A. Ввод команды clear flash
  - B. Ввод команды erase start и перезагрузка маршрутизатора
  - C. Ввод команды setup
  - D. Ввод команды setup mode
3. Какая команда **позволит** перейти из привилегированного в пользовательский режим?
- A. **Exit**
  - B. Quit
  - C. Disable
  - D. Control+Z
4. Какая команда редактирования переместит курсор в начало строки?
- A. Ctrl+E
  - B. Ctrl+F
  - C. Ctrl+B
  - D. Ctrl+A
5. Какая команда редактирования переместит курсор в конец строки?
- A. **Ctrl+E**
  - B. Ctrl+F
  - C. Esc+B
  - D. Ctrl+A
6. Какая команда редактирования переместит курсор на один символ вперед?
- A. Ctrl+E
  - B. Ctrl+F
  - C. Ctrl+B
  - D. Ctrl+A
7. Какая команда редактирования переместит курсор на одно слово назад?
- A. Ctrl+E
  - B. Ctrl+F
  - C. Esc+B
  - D. Ctrl+A
8. Какая команда покажет версию IOS, исполняемую маршрутизатором?
- A. Show flash
  - B. Show flash file
  - C. Show ip flash
  - D. Sh ver
9. Какая команда покажет содержимое памяти EEPROM маршрутизатора?

- A. Show flash
  - B. Show flash file**
  - C. Show ip flash
  - D. Sh ver
10. Какая команда покажет подключение кабеля DTE или DCE к интерфейсу serial 0?
- A. Sh int s0
  - B. Sh int serial 0**
  - C. Sho controllers s 0
  - D. Sho controllers sO
11. Какая команда предотвратит перезапись консольными сообщениями вводимую команду?
- A. No logging
  - B. Logging**
  - C. Logging asynchronous
  - D. Logging synchronous
12. Какая команда позволит пользователям подключаться к маршрутизатору по Telnet без приглашения на ввод пароля пользовательского режима?
- A. Login
  - B. No login**
  - C. You can telnet by default, so no command is needed.
  - D. No password
13. Какая команда установит для консоли тайм-аут в одну секунду?
- A. Timeout 1 0
  - B. Timeout 0 1**
  - C. Exec-timeout 1 0
  - D. Exec-timeout 0 1
14. Как установить пароль bob только для линии 1 и протокола Telnet?
- A. line vty 0 1  
Login  
Password bob
  - B. line vty 0 4**  
Login  
Password bob
  - C. line vty 1  
Login  
Password bob
  - D. line vty 1  
Password bob  
Login

15. Как установить пароль вспомогательного порта?
- A. Line aux 1
  - B. Line aux 0**
  - C. Line aux 0 4
  - D. Line aux port
16. Какая команда зашифрует пароль Telnet в маршрутизаторе Cisco?
- A. Line telnet 0, encryption on, password todd
  - B. Line vty 0, password encryption, password todd
  - C. Service password encryption, line vty 0 4, password todd
  - D. Password encryption, line vty 0 4, password todd
17. Какая команда вернет текущую исполняемую конфигурацию и перезапустит ее при перезагрузке маршрутизатора?
- A. (Config)#copy current to starting
  - B. Router#copy starting to running**
  - C. Router(config)#copy running-config star
  - D. Router#copy run startup
18. Каковы в режиме установки два разных режима обслуживания конфигурации установки?
- A. Basic (базовый)
  - B. Advanced (улучшенный)**
  - C. Extended (развернутый)
  - D. Expanded (расширенный)
19. Какая команда удалит содержимое NVRAM в маршрутизаторе?
- A. Delete NVRAM
  - B. Delete Startup-config**
  - C. Erase NVRAM
  - D. Erase start
20. Какая возникает проблема в интерфейсе, когда ввод команды show interface serial 0 приводит к сообщению:  
Serial0 is administratively down, line protocol is down  
(интерфейс Serial0 выключен административно, протокол линии выключен)
- A. Различаются значения интервалов поддержания жизни (keepalive).**
  - B. Администратор выключил интерфейс.
  - C. Администратор выполняет проверку интерфейса по Ping.
  - D. К интерфейсу не подключен кабель.

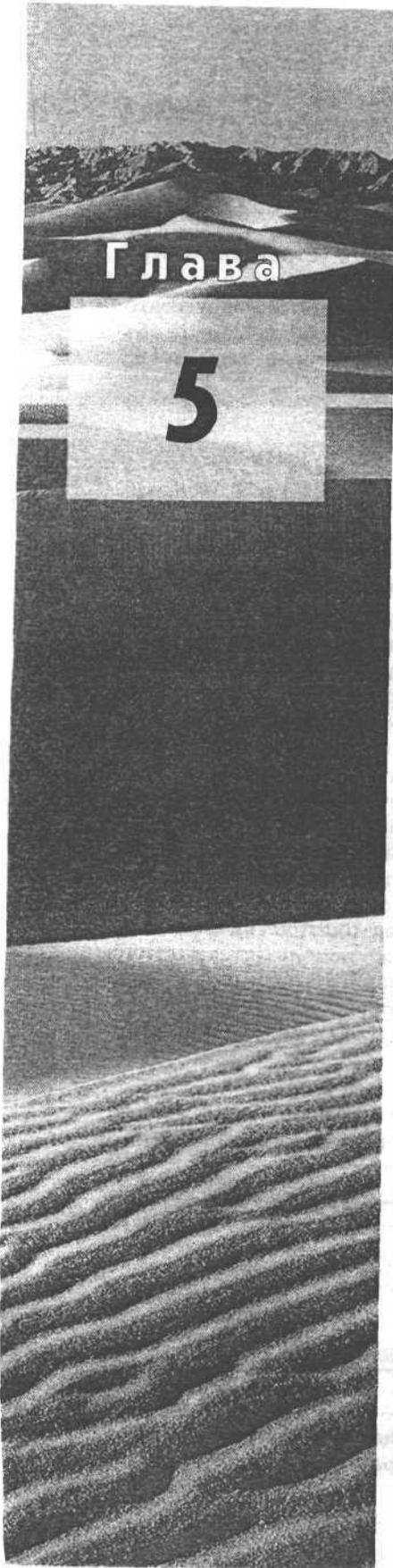
## Ответы к упражнению

1. clock rate 64000
2. config t line vtty 0 4, no login
3. config t int e0, no shut
4. erase startup-config
5. config t, line console 0, login, password todd
6. config t, enable secret cisco
7. show controllers s 0
8. show terminal
9. config net
10. config t hostname Chicago

## Ответы к проверочным вопросам

- |         |          |
|---------|----------|
| 1. C    | 11. D    |
| 2. B, C | 12. B    |
| 3. C    | 13. D    |
| 4. D    | 14. C    |
| 5. A    | 15. B    |
| 6. B    | 16. C    |
| 7. C    | 17. D    |
| 8. D    | 18. A, C |
| 9. A    | 19. D    |
| 10. C   | 20. B    |





Глава

5

## Маршрутизация по протоколу IP

## Маршрутизация

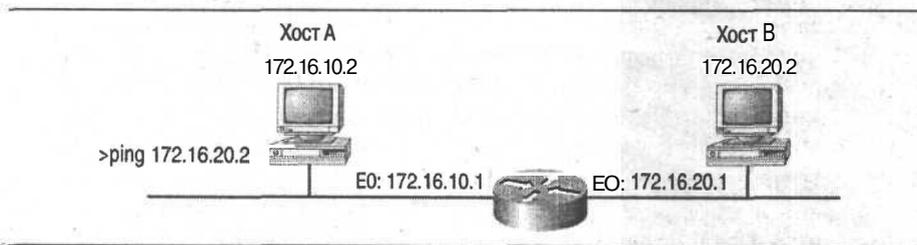
Маршрутизация служит для приема пакета от одного устройства и передачи его по сети другому устройству через другие сети. Если в сети нет маршрутизаторов, то не поддерживается маршрутизация. Маршрутизаторы направляют (перенаправляют) трафик во все сети, составляющие объединенную сеть. Для маршрутизации пакета маршрутизатор должен владеть следующей информацией:

- Адрес назначения
- Соседний маршрутизатор, от которого он может узнать об удаленных сетях
- Доступные пути ко всем удаленным сетям
- Наилучший путь к каждой удаленной сети
- Методы обслуживания и проверки информации о маршрутизации

Маршрутизатор узнает об удаленных сетях от соседних маршрутизаторов или от сетевого администратора. Затем маршрутизатор строит таблицу маршрутизации, которая описывает, как найти удаленные сети. Если сеть подключена непосредственно к маршрутизатору, он уже знает, как направить пакет в эту сеть. Если же сеть не подключена напрямую, маршрутизатор должен узнать (изучить) пути доступа к удаленной сети с помощью статической маршрутизации (ввод администратором вручную местоположения всех сетей в таблицу маршрутизации) или с помощью динамической маршрутизации. Динамическая маршрутизация — это процесс протокола маршрутизации, определяющий взаимодействие устройства с соседними маршрутизаторами. Маршрутизатор будет обновлять сведения о каждой изученной им сети. Если в сети произойдет изменение, протокол динамической маршрутизации автоматически информирует об изменении все маршрутизаторы. Если же используется статическая маршрутизация, обновить таблицы маршрутизации на всех устройствах придется системному администратору.

## Процесс IP-маршрутизации

IP-маршрутизация — простой процесс, который одинаков в сетях любого размера. Например, на рис. 5.1 показан процесс пошагового взаимодействия хоста А с хостом В в другой сети.



**Рис. 5.1.** Пример IP-маршрутизации для двух хостов и одного маршрутизатора

В примере пользователь хоста А запрашивает по Ping IP-адрес хоста В. Дальнейшие операции не так просты, поэтому рассмотрим их подробнее:

1. В командной строке пользователь вводит ping **172.16.20.2**. На хосте А генерируется пакет с помощью протоколов сетевого уровня IP и ICMP.
2. IP обращается к протоколу **ARP** для выяснения сети назначения для пакета, просматривая IP-адрес и маску подсети хоста А. Это запрос к удаленному хосту, т.е. пакет не предназначен хосту локальной сети, поэтому пакет должен быть направлен маршрутизатору для перенаправления в нужную удаленную сеть.
3. Чтобы хост А смог послать пакет маршрутизатору, хост должен знать аппаратный адрес интерфейса **маршрутизатора**, подключенный к локальной сети. Сетевой уровень передает пакет и аппаратный адрес назначения канальному уровню для деления на кадры и пересылки локальному хосту. Для получения аппаратного адреса **хост** ищет местоположение точки назначения в собственной памяти, называемой кэшем ARP.
4. Если IP-адрес еще не был доступен и не присутствует в кэше ARP, хост посылает широковещательную рассылку **ARP** для поиска **аппаратного** адреса по IP-адресу 172.16.10.1. Именно поэтому первый запрос Ping обычно заканчивается тайм-аутом, но четыре остальных запроса будут успешны. После кэширования адреса тайм-аута обычно не возникает.
5. Маршрутизатор отвечает и сообщает аппаратный адрес интерфейса **Ethernet**, подключенного к локальной сети. Теперь хост имеет всю информацию для пересылки пакета маршрутизатору по локальной сети. Сетевой уровень спускает пакет вниз для генерации эхо-запроса ICMP (Ping) на канальном уровне, дополняя пакет аппаратным адресом, по которому хост **должен** послать пакет. Пакет имеет IP-адреса источника и назначения вместе с указанием на тип пакета (ICMP) в поле протокола сетевого уровня.
6. Канальный уровень формирует кадр, в котором инкапсулируется пакет вместе с управляющей **информацией**, необходимой для пересылки по локальной сети. К такой информации относятся аппаратные адреса источника и назначения, а также значение в поле типа, установленное протоколом сетевого уровня (это будет поле типа, поскольку IP по умолчанию пользуется кадрами Ethernet II). Рис. 5.2 показывает кадр, генерируемый на канальном уровне и пересылаемый по локальному носителю.

На рис. 5.2 показана вся информация, необходимая для взаимодействия с маршрутизатором: аппаратные адреса источника и назначения, IP-адреса источника и назначения, данные, а также контрольная сумма CRC кадра, находящаяся в поле FCS (Frame Check Sequence).

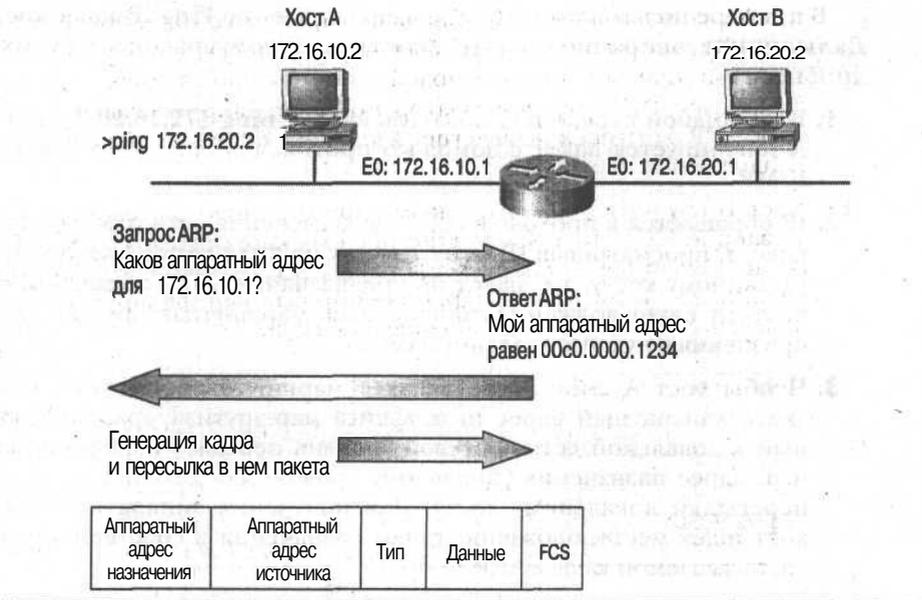


Рис. 5.2. Кадр, сгенерированный хостом А

7. Канальный уровень хоста А передает кадр физическому уровню. Там выполняется кодирование нулей и единиц в цифровой сигнал с последующей передачей этого сигнала по локальной физической сети.
8. Сигнал достигает интерфейса Ethernet 0 маршрутизатора, который синхронизируется по преамбуле цифрового сигнала для извлечения кадра. Интерфейс маршрутизатора после построения кадра проверяет CRC, а в конце приема кадра сравнивает полученное значение с содержимым поля FCS. Кроме того, он проверяет процесс передачи на отсутствие фрагментации и конфликтов носителя.
9. Проверяется аппаратный адрес назначения. Поскольку он совпадает с адресом маршрутизатора, анализируется поле типа кадра для определения дальнейших действий с этим пакетом данных. В поле типа указан протокол IP, поэтому маршрутизатор передает пакет процессу протокола IP, исполняемому маршрутизатором. Кадр удаляется. Исходный пакет (сгенерированный хостом А) помещается в буфер маршрутизатора.
10. Протокол IP смотрит на IP-адрес назначения в пакете, чтобы определить, не направлен ли пакет самому маршрутизатору. Поскольку IP-адрес назначения равен 172.16.20.2, маршрутизатор определяет по своей таблице маршрутизации, что сеть 172.16.20.0 непосредственно подключена к интерфейсу Ethernet 1.
11. Маршрутизатор передает пакет из буфера в интерфейс Ethernet 1. Маршрутизатору необходимо сформировать кадр для пересылки

пакета хосту назначения. Сначала маршрутизатор проверяет свой кэш ARP, чтобы определить, был ли уже разрешен аппаратный адрес во время предыдущих взаимодействий с данной сетью. Если адреса нет в кэше ARP, маршрутизатор посылает широковещательный запрос ARP в интерфейс Ethernet 1 для поиска аппаратного адреса для IP-адреса 172.16.20.2.

12. Хост В откликается аппаратным адресом своего сетевого адаптера на запрос ARP. Интерфейс Ethernet 1 маршрутизатора теперь имеет все необходимое для пересылки пакета в точку окончательного приема. Рис. 5.3 показывает кадр, сгенерированный маршрутизатором и переданный по локальной физической сети.

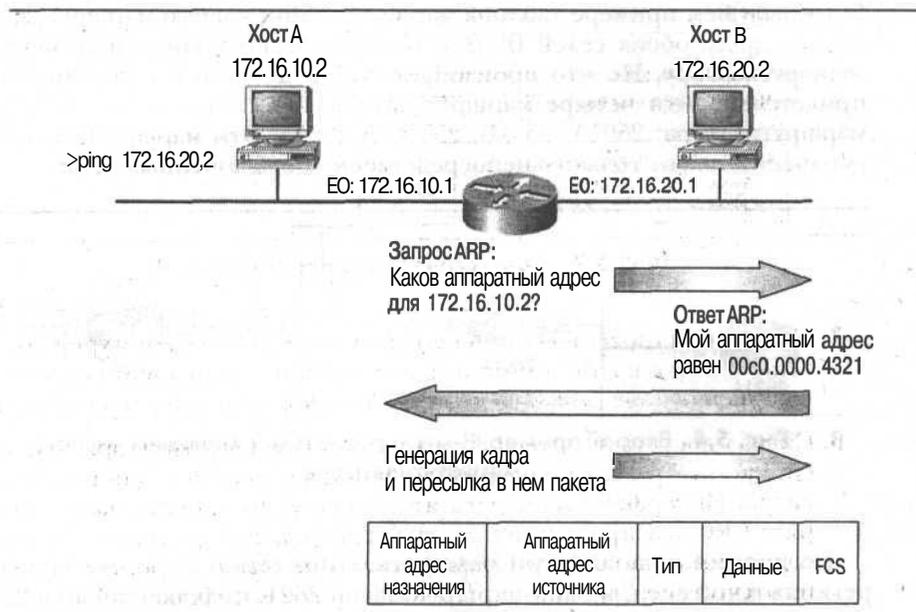


Рис. 5.3. Кадр, сгенерированный маршрутизатором

Кадр, сгенерированный интерфейсом Ethernet 1 маршрутизатора, имеет аппаратный адрес источника от интерфейса Ethernet 1 и аппаратный адрес назначения для сетевого адаптера хоста В. Важно отметить, что, несмотря на изменения аппаратных адресов источника и назначения, в каждом передаваемом пакете интерфейсе маршрутизатора, IP-адреса источника и назначения никогда не изменяются. Пакет никоим образом не модифицируется, но меняются кадры.

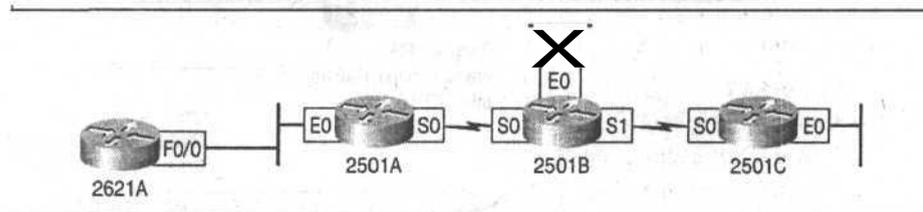
13. Хост В принимает кадр и проверяет CRC. Если проверка будет успешной, кадр удаляется, а пакет передается протоколу IP. Он анализирует IP-адрес назначения. Поскольку IP-адрес назначения совпадает с установленным в хосте В адресом, протокол IP исследует поле протокола для определения цели пакета.

14. В нашем пакете содержится эхо-запрос ICMP, поэтому хост В генерирует новый эхо-ответ ICMP с IP-адресом источника, равным адресу хоста В, и IP-адресом назначения, равным адресу хоста А. Процесс запускается заново, но в противоположном направлении. Однако аппаратные адреса всех устройств по пути следования пакета уже известны, поэтому все устройства смогут **получить** аппаратные адреса интерфейсов из собственных кэшей ARP.

В крупных сетях процесс происходит **аналогично**, но пакету придется пройти больше участков по пути к хосту назначения.

## IP-маршрутизация в крупных сетях

В предыдущем примере таблица маршрутизации нашего маршрутизатора имела адреса обеих сетей IP. Эти сети непосредственно подключены к маршрутизатору. Но что произойдет, когда по пути следования пакету придется пройти четыре маршрутизатора? Рис. 5.4 показывает четыре маршрутизатора: 2501A, 2501B, 2501C и 2621A. Эти маршрутизаторы по умолчанию знают только о непосредственно подключенных сетях.



**Рис. 5.4.** Второй пример IP-маршрутизации с большим числом маршрутизаторов

На рис. 5.4 показаны три маршрутизатора серии 2501, связанные по региональной сети, и один маршрутизатор 2621, подключенный к 2501A по сети Ethernet. Каждый маршрутизатор имеет непосредственно подключенную сеть Ethernet.

Прежде всего, необходимо правильно сконфигурировать каждый маршрутизатор. В таблице 5.1 показаны использованные IP-адреса. После рассказа о настройке сетей, мы обсудим сам процесс конфигурации IP-маршрутизации. Все сети в примере имеют 24-разрядную маску подсети (255.255.255.0).

Настройка конфигурации маршрутизатора — очень простой процесс, поскольку нужно только добавить интерфейсам IP-адреса, а затем выполнить для них команду `no shutdown`. Дальше процесс будет сложнее. Сначала выполним простую задачу по конфигурации IP-адресов в сетях.

**Таблица 5.1.**  
**Адреса для сетей IP**

Маршрутизатор	Сетевой адрес	Интерфейс	Адрес
2621A	172.16.10.0	Г0/0	172.16.10.1
2501A	172.16.10.0	e0	172.16.10.2
2501A	172.16.20.0	s0	172.16.20.1
2501B	172.16.20.0	s0	172.16.20.2
2501B	172.16.40.0	s1	172.16.40.1
2501B	172.16.30.0	e0	172.16.30.1
2501C	172.16.40.0	s0	172.16.40.2
2501C	172.16.50.0	e0	172.16.50.1

### Конфигурация 2621A

Для настройки маршрутизатора 2621 следует добавить IP-адрес интерфейсу FastEthernet O/O. Конфигурация имен хостов в каждом маршрутизаторе позволит упростить их идентификацию в сети. Пример настройки;

```
Router> en
Router#config t
Router(config)#hostname 2621A
2621A(Config)#interface fa0/0
2621A(Config-if)#ip address 172.16.10.1 255.255.255.0
2621A(Config-if)#no shut
```

Для настройки потребовалось ввести несколько строк (для лучшего понимания использованных команд можно обратиться к главе 4).

Для просмотра созданной в маршрутизаторе Cisco таблицы IP-маршрутизации служит привилегированная команда `show ip route`. Ниже показан пример результата выполнения этой команды. В таблице маршрутизации заданы только настроенные в устройстве сети, т.е. только известная маршрутизатору сеть 172.16.10.0.

```
2621A#sh 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, * - candidate default U - per-user static route, o - ODR, P - periodic downloaded static route T - traffic engineered route
```

(Коды: С - подключенный, S - статический, I - IGRP, R - RIP, M - мобильный, B - BGP D - EIGRP, EX - внешний EIGRP, O - OSPF, IA - межобластной OSPF N1 - OSPF NSSA внешнего типа 1, N2 - OSPF NSSA внешнего типа 2 E1 - OSPF внешнего типа 1, E2 - OSPF внешнего типа 2, E - EGP i - IS-IS, L1 - IS-IS уровня 1, L2 - IS-IS уровня 2, \* - кандидат для значения по умолчанию U - статический маршрут для конкретных пользователей, o - ODR, P - периодически загружаемый статический маршрут T - маршрут инженерного трафика)

```

Gateway of last resort is not set
(шлюз на крайний случай не установлен)
 172.16.0.0/24 is subnetted, 1 subnets
 (выделение подсетей 172.16.0.0/24, одна подсеть)
C 172.16.10.0 is directly connected, FastEthernet0/0
(С сеть 172.16.10.0 подключена непосредственно, интерфейс FastEthernet0/0)
2621A#

```

В показанной таблице маршрутизации непосредственно подключенной является сеть 172.16.10.0. На это указывает символ "С". Коды аббревиатур для каждого типа подключения перечислены в верхней части листинга команды `show ip route`. Далее в этой главе для краткости будем пользоваться только кодами подключений.

## Конфигурация 2501А

Настроим следующий маршрутизатор. В 2501А следует сконфигурировать два интерфейса: Ethernet 0 и serial 0.

```

Router>en
Router#config t
Router(config)#hostname 2501A
2501A(config)#int e0
2501A(config-if)#ipaddress 172.16.10.2 255.255.255.0
2501A(config-if)#no shut
2501A(config-if)#int s0
2501A(config-if)#ipaddress 172.16.20.1 255.255.255.0
2501A(config-if)#no shut

```

В данном случае serial 0 настроен на сеть 172.16.20.0, а интерфейс Ethernet 0 — на сеть 172.16.10.0. Покажем это командой `show ip route`:

```

2501A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
Gateway of last resort is nqt set
 172.16.0.0/24 is subnetted, 2 subnets
C 172.16.20.0 is directly connected, Serial0
C 172.16.10.0 is directly connected, Ethernet0
2501A#

```

Маршрутизатор 2501А знает, как обратиться к сетям 172.16.10.0 и 172.16.20.0. Маршрутизаторы 2621 и А способны взаимодействовать, поскольку находятся в одной локальной сети.

## Конфигурация 2501В

Конфигурация 2501В не отличается от предыдущего примера, за исключением установки тактовой частоты командой `clock rate` в интерфейсе DCE, подключенном к обоим последовательным портам (интерфейсы DCE и команда `clock rate` рассмотрены в главе 4).

```
Router>en
Router#config t
Router(config)#hostname 2501B
2501B(config)#int e0
2501B(config-if)#ip address 172.16.30.1 255.255.255.0
2501B(config-if)#no shut
2501B(config-if)#int s0
2501B(config-if)#ip address 172.16.20.2 255.255.255.0
2501B(config-if)#clock rate 64000
2501B(config-if)#no shut
2501B(config-if)#int s1
2501B(config-if)#ip address 172.16.40.1 255.255.255.0
2501B(config-if)#clock rate 64000
2501B(config-if)#no shut
```

В показанной конфигурации определены имя хоста и IP-адрес, а также тактовая частота последовательных интерфейсов. Вывод команды `show ip route` покажет непосредственно подключенные сети 172.16.20.0, 172.16.30.0 и 172.16.40.0.

```
2501B#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 3 subnets
C 172.16.40.0 is directly connected, Serial1
C 172.16.30.0 is directly connected, Ethernet0
C 172.16.20.0 is directly connected, Serial0
2501B#
```

Маршрутизаторы А и В могут взаимодействовать, поскольку находятся в одной региональной сети. Однако маршрутизатор В не может обратиться к маршрутизатору 2621, поскольку не знает о сети 172.16.10.0. Маршрутизатор А способен обратиться по Ping к маршрутизаторам 2621 и 2501В, но маршрутизаторы 2501В и 2621 не смогут "увидеть" друг друга.

## Конфигурация 2501С

Конфигурационные параметры маршрутизатора 2501С аналогичны параметрам настройки 2501А за исключением другого идентификатора сети.

```
Router>en
Router#config t
Router(config)#hostname 2501C
2501C(config)#int e0
2501C(config-if)#ip address 172.16.50.1 255.255.255.0
2501C(config-if)#no shut
```

```

2501C(config-if)#int s0
2501C(config-if)#ip address 172.16.40.2 255.255.255.0
2501C(config-if)#no shut

```

Интерфейс Ethernet 0 настроен на сеть 172.16.50.0, а интерфейс serial 0 — на региональную сеть 172.16.40.0. Листинг команды `show ip route` показывает сети, непосредственно подключенные к маршрутизатору 2501C:

```

2501C#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 2 subnets
C 172.16.50.0 is directly connected, Ethernet0
C 172.16.40.0 is directly connected, Serial0
2501C#

```

Маршрутизатор 2501C может взаимодействовать с 2501B, поскольку они находятся в одной региональной сети. Однако по умолчанию 2501C "не видит" другие маршрутизаторы и сети.

## IP-маршрутизация в сети

Показанная в предыдущем примере сеть была настроена на **корректное** разрешение IP-адресов. Однако как будут маршрутизатору пересылать пакеты в удаленные сети? Маршрутизатор передает пакет только по данным из таблицы маршрутизации, где указан путь для достижения удаленной сети. Мы настроили маршрутизаторы только на непосредственно подключенные к ним сети. Что произойдет, когда маршрутизатор получит пакет для сети, которая не указана в таблице маршрутизации? Нельзя послать широковещательную рассылку для обнаружения удаленной сети — другие маршрутизаторы прервут распространение такой рассылки.

Существует несколько разных способов настройки таблицы маршрутизации на все сети в нашем примере, что позволит успешно перенаправлять пакеты. Однако путь от одной сети к другой может быть трудным. Если изучить доступные типы маршрутизации, то мы сможем выбрать наилучший для конкретных условий метод выбора пути.

В этой главе мы рассмотрим следующие типы маршрутизации:

- Статическая маршрутизация
- Маршрутизация по умолчанию
- Динамическая маршрутизация

Начнем с наиболее простой статической маршрутизации в нашей сети, поскольку реализация и понимание этого метода станет хорошей основой для дальнейшего изучения маршрутизации в объединенных сетях.

## Статическая маршрутизация

*Статическая маршрутизация* — это процесс ввода администратором сети путей в таблицы маршрутизации всех маршрутизаторов. Как и остальные типы маршрутизации, статическая маршрутизация имеет собственные преимущества и недостатки.

Преимущества статической маршрутизации:

- Нет нагрузки на процессор маршрутизатора
- Не используется полоса пропускания связей между маршрутизаторами
- Хорошая защита (поскольку только администратор устанавливает маршрутизацию к определенным сетям)

Недостатки статической маршрутизации:

- Администратор должен хорошо понимать особенности объединенной сети и правильно настроить каждый маршрутизатор.
- Если в объединенную сеть добавляется новая сеть, то администратору придется добавить новые пути во все маршрутизаторы.
- Статическая маршрутизация неприменима в крупных сетях, поскольку требует большого объема работы.

Команда добавления статического пути (маршрута) в таблицу маршрутизации:

```
ip route [сеть_назначения] [маска] [адрес_следующего_участка или
интерфейс_выхода] [административное_расстояние][постоянный]
```

Рассмотрим каждый из аргументов этой команды:

**ip route** Команда создания статического пути.

**сеть\_назначения (destination network)** Сеть, которая указывается в таблице маршрутизации.

**маска (mask)** Используемая маска подсети.

**адрес\_следующего\_участка (next hop address)** Адрес следующего участка, по которому маршрутизатор должен отправить к удаленной сети полученный пакет. Это интерфейс маршрутизатора для непосредственно подключенной сети. Перед добавлением таблицы маршрутизации, интерфейс нужно проверить по Ping.

**интерфейс\_выхода (exit interface)** Служит для указания адреса следующего участка. Применяется только для связей "точка-точка" (например, линий региональной сети), но не используется в локальных сетях, например в Ethernet.

**административное\_расстояние (administrative distance)** По умолчанию статический путь имеет административное расстояние, равное 1. Можно изменить значение по умолчанию, указав после аргумента новое значение административного "веса" пути.

постоянный (permanent) Если интерфейс выключен или маршрутизатор не может связаться с маршрутизатором следующего участка, путь автоматически удаляется из таблицы маршрутизации. Установка свойства "постоянный" позволит сохранить элемент в таблице маршрутизации при любых обстоятельствах.

Чтобы показать установку статических путей, вернемся к примеру объединенной сети на рис. 5.4.

## 2621A

Любая таблица маршрутизации автоматически заполняется сведениями о непосредственно подключенных сетях. Для направления пакетов во все объединенные сети таблица маршрутизации должна содержать информацию о местоположении и способе доступа к удаленным сетям.

Маршрутизатор 2621 подключен только к сети 172.16.10.0. Чтобы маршрутизатор 2621A смог перенаправлять пакеты во все сети, в таблице маршрутизации следует сконфигурировать сведения о следующих сетях:

- 172.16.20.0
- 172.16.30.0
- 172.16.40.0
- 172.16.50.0

Ниже показан листинг с информацией о статических путях маршрутизатора 2621A и содержимым таблицы маршрутизации после настройки устройства. Чтобы маршрутизатор 2621A смог найти удаленную сеть, в таблице маршрутизации должен находиться элемент для описания этой сети, включающий маску и местоположение. Заметим, что все статические пути предполагают направление пакетов в сеть 172.16.10.2, которая является для маршрутизатора 2621 следующим участком.

```
2621A(Config)#iproute 172.16.20.0 255.255.255.0 172.16.10.2
2621A(Config)#iproute 172.16.30.0 255.255.255.0 172.16.10.2
2621A(Config)#iproute 172.16.40.0 255.255.255.0 172.16.10.2
2621A(Config)#iproute 172.16.50.0 255.255.255.0 172.16.10.2
```

После настройки маршрутизатора можно ввести команду `show running-config` или `show ip route` для показа статических путей. Запомните, что если пути нет в таблице маршрутизации, значит маршрутизатор не может взаимодействовать с установленным в таблице адресом следующего участка. Использование параметра `permanent` позволит сохранить путь в таблице маршрутизации, даже если нельзя подключиться к устройству следующего участка.

```
2621A#sh ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
```

```
Gateway of last resort is not set
```

```
172.16.0.0/24 is subnetted, 5 subnets
```

```
S 172.16.50.0 [1/0] via 172.16.10.2
S 172.16.40.0 [1/0] via 172.16.10.2
S 172.16.30.0 [1/0] via 172.16.10.2
S 172.16.20.0 [1/0] via 172.16.10.2
C 172.16.10.0 is directly connected, FastEthernet0/0
2621A#
```

Маршрутизатор 2621 имеет всю информацию, необходимую для взаимодействия с другими удаленными сетями. Однако если маршрутизатор 2501A не сконфигурирован на ту же самую информацию, то пакеты будут отбрасываться маршрутизатором 2501A.

## 2501A

Маршрутизатор 2501A подключен к сетям 172.16.10.0 и 172.16.20.0. В нем необходимо конфигурировать следующие статические пути:

- 172.16.30.0
- 172.16.40.0
- 172.16.50.0

Конфигурация маршрутизатора 2501A:

```
2501A(Config)#ip route 172.16.30.0 255.255.255.0 172.16.20.2
2501A(Config)#ip route 172.16.40.0 255.255.255.0 172.16.20.2
2501A(Config)#ip route 172.16.50.0 255.255.255.0 172.16.20.2
```

Просмотрев таблицу маршрутизации, мы увидим, что маршрутизатор 2501A теперь знает о том, как найти каждую сеть.

```
2501A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - [листинг сокращен]
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets
S 172.16.50.0 [1/0] via 172.16.20.2
S 172.16.40.0 [1/0] via 172.16.20.2
S 172.16.30.0 [1/0] via 172.16.20.2
C 172.16.20.0 is directly connected, Serial0
C 172.16.10.0 is directly connected, Ethernet0
2501A#
```

Символ S в элементе таблицы маршрутизации означает, что установлен статический путь к сети. Административное расстояние равно [1/0], а количество участков к удаленной сети — 0.

Маршрутизатор 2501A получил полную таблицу маршрутизации. Поскольку она согласована с таблицами других маршрутизаторов объединенной сети, 2501A может взаимодействовать со всеми удаленными сетями.

## 2501B

Маршрутизатор 2501B непосредственно подключен к сетям 172.16.20.0, 172.16.30.0 и 172.16.40.0. Нужно добавить только два пути: 172.16.10.0 и 172.16.50.0.

```
2501B(Config)#ip route 172.16.10.0 255.255.255.0 172.16.20.1
2501B(Config)#ip route 172.16.50.0 255.255.255.0 172.16.40.2
```

Ниже показано содержимое таблицы маршрутизации устройства 2501B.

```
2501B#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 5 subnets
S 172.16.50.0 [1/0] via 172.16.40.2
C 172.16.40.0 is directly connected, Serial1
C 172.16.30.0 is directly connected, Ethernet0
C 172.16.20.0 is directly connected, Serial0
S 172.16.10.0 [1/0] via 172.16.20.1
2501B#
```

Маршрутизатор 2501B показал сведения обо всех сетях объединенной сети и может взаимодействовать с маршрутизаторами, а также с удаленными сетями. Исключением является сеть 172.16.50.0, которая пока не установлена в маршрутизаторе 2501C.

## 2501C

Маршрутизатор 2501C непосредственно подключен к сетям 172.16.40.0 и 172.16.50.0. В таблицу маршрутизации нужно добавить сведения о сетях 172.16.10.0, 172.16.20.0 и 172.16.30.0. Для этого введите команды:

```
2501C(Config)#ip route 172.16.10.0 255.255.255.0 172.16.40.1
2501C(Config)#ip route 172.16.20.0 255.255.255.0 172.16.40.1
2501C(Config)#ip route 172.16.30.0 255.255.255.0 172.16.40.1
```

Ниже показан листинг команды show ip route, введенной в маршрутизатор 2501C.

```
2501C#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 5 subnets
C 172.16.50.0 is directly connected, Ethernet0
C 172.16.40.0 is directly connected, Serial0
S 172.16.30.0 [1/0] via 172.16.40.1
S 172.16.20.0 [1/0] via 172.16.40.1
```

```
S 172.16.10.0 [1/0] via 172.16.40.1
2501C#
```

Теперь все маршрутизаторы имеют корректные таблицы, поэтому маршрутизаторы и хосты должны без проблем взаимодействовать друг с другом. Однако если добавить в объединенную сеть дополнительные пути или маршрутизаторы, придется вручную обновить таблицы маршрутизации на всех маршрутизаторах. Это допустимо в небольшой сети, но займет слишком много времени в крупной объединенной сети.

## Проверка конфигурации

После настройки таблиц во всех маршрутизаторах нужно выполнить проверку. Лучше всего использовать программу Ping. Проверка по Ping связи между маршрутизаторами 2621A и 2501C позволит подтвердить работу сети от одного конца до другого.

Пример листинга Ping для сети 172.16.50.0 на маршрутизаторе 2621A:

```
2621A#ping 172.16.50.1
```

```
Type escape sequence to abort.
```

```
(введите последовательность escape для выхода)
```

```
Sending 5, 100-byte ICMP Echos to 172.16.50.1, timeout is 2 seconds:
```

```
(отправлено 5 100-байтовых эхо-запросов ICMP к 172.16.50.1, тайм-аут равен 2 с)
```

```
!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 64/66/68 ms
```

```
(уровень успешности 80% - 5 из пяти, времена "туда и обратно"
```

```
мин/среднее/макс = 64/66/68 мс)
```

```
2621A#
```

Первый ответ отмечен точкой, поскольку во время первого запроса по Ping произошло ожидание запроса и ответа ARP. Как только протокол ARP нашел аппаратный адрес шлюза по умолчанию, преобразование IP-в-Ethernet стало выполняться через кэш ARP, причем запись сохраняется в кэше в течение четырех часов. Все остальные подключения по IP к маршрутизаторам следующих участков уже не сопровождаются тайм-аутом, поскольку больше не выполняется широковещательная рассылка ARP.

С маршрутизатора 2501C проверка по Ping к 172.16.10.0 позволит подтвердить успешное подключение по IP. Вывод в этом маршрутизаторе:

```
2501C#ping 172.16.10.1
```

```
Введите escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 64/67/72 ms
```

Первый запрос Ping уже прошел без тайм-аута, поскольку широковещательная рассылка ARP выполнена в локальной сети, а не в региональной. Проверка по Ping из конца в конец не выявила проблем, значит наша статическая конфигурация правильна!

## Маршрутизация по умолчанию

*Маршрутизация по умолчанию* используется для пересылки пакетов в удаленную сеть назначения, которая не отмечена в таблице маршрутизации через маршрутизатор следующего участка. Можно использовать маршрутизацию по умолчанию в тупиковых сетях (stub network), т.е. сетях, имеющих только один выходной порт.

В нашем примере объединенной сети в тупиковых сетях находятся только маршрутизаторы 2621A и 2501C. Если попытаться установить путь по умолчанию в маршрутизаторах 2501A и 2501B, то станет невозможным перенаправление пакетов, поскольку эти устройства имеют более одного интерфейса маршрутизации к другим маршрутизаторам. Однако несмотря на наличие в маршрутизаторе 2501C двух подключений, он не имеет установленного пути к сети 172.16.50 для отправки туда пакетов. Маршрутизатор 2501C посылает пакеты только в сеть 172.16.40.1, т.е. в интерфейс устройства 2501B. Маршрутизатор 2621A направляет пакеты только в сеть 172.16.10.1 интерфейса 2501A.

Для настройки пути по умолчанию в сетевом адресе и маске статического пути используются символы-заменители (wildcards). Можно считать путь по умолчанию статическим маршрутом, указанным с заменителями информации о сети и маске. В этом разделе книги мы покажем создание пути по умолчанию в маршрутизаторе 2501C.

Маршрутизатор 2501C непосредственно подключен к сетям 172.16.40.0 и 172.16.50.0. В таблице маршрутизации должны быть сведения о сетях 172.16.10.0, 172.16.20.0 и 172.16.30.0. Для настройки в маршрутизаторе перенаправления пакетов в три отмеченные выше сети мы создали в таблице маршрутизации три статических пути. За счет использования пути по умолчанию можно обойтись одной записью о статических путях. Сначала удалим три существующие статические пути из маршрутизатора, а затем добавим путь по умолчанию.

```
2501C(Config)#no ip route 172.16.10.0 255.255.255.0 172.16.40.1
2501C(Config)#no ip route 172.16.20.0 255.255.255.0 172.16.40.1
2501C(Config)#no ip route 172.16.30.0 255.255.255.0 172.16.40.1
2501C(Config)#ip route 0.0.0.0 0.0.0.0 172.16.40.1
```

Если теперь вывести таблицу маршрутизации, мы увидим только две непосредственно подключенные сети, а также строку с символом S\*. Это указывает на элемент, являющийся кандидатом для пути по умолчанию.

```
2501C#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
-IS-ISlevel-1, L2 - IS-ISlevel-2, * - candidate defaultU - per-user static route,
o - ODR

Gateway of last resort is 172.16.40.1 to network 0.0.0.0 172.16.0.0/24
is subnetted, 5 subnets
C 172.16.50.0 is directly connected, Ethernet0
C 172.16.40.0 is directly connected, Serial0
```

```
S* 0.0.0.0/0 [1/0] via 172.16.40.1
2501C#
```

Обратите внимание, что в таблице маршрутизации не указан шлюз на крайний случай (gateway of last resort). Отметим еще одну команду для бесклассовой маршрутизации по протоколу IP. Ее следует применять для путей по умолчанию: `ip classless`. Все маршрутизаторы Cisco являются полноклассовыми, т.е. предполагают наличие маски подсети по умолчанию в каждом интерфейсе. Когда маршрутизатор получает пакет для подсети назначения, которой нет в таблице маршрутизации, по умолчанию пакет отбрасывается. Для использования маршрутизации по умолчанию необходимо применять команду `ip classless`, поскольку удаленной подсети нет в таблице маршрутизации.

В маршрутизаторе применяется версия 12.x операционной системы IOS, поэтому команда `ip classless` используется по умолчанию. Если указана маршрутизация по умолчанию, но такой команды нет в конфигурации устройства, необходимо добавить ее в конфигурацию маршрутизатора:

```
2501C(Config)#ipclassless
```

Это команда режима глобального конфигурирования. Интересно, что маршрутизация по умолчанию иногда срабатывает и без команды `ip classless`. Однако в некоторых случаях требуется явно указать эту команду в конфигурации. Рекомендуем всегда включать команду `ip classless`, когда используется маршрутизация по умолчанию.

## Динамическая маршрутизация

*Динамическая маршрутизация* — это процесс использования протокола для поиска и обновления таблиц маршрутизации в устройствах. Динамическая маршрутизация проще статической, но требует существенных ресурсов процессора маршрутизатора и полосы пропускания сетевых линий связи. Протокол маршрутизации определяет набор правил, используемых маршрутизаторами для взаимодействия с соседними маршрутизаторами.

В нашей книге мы обсудим два протокола маршрутизации: RIP (Routing Information Protocol — протокол информации о маршрутизации) и IGRP (Interior Gateway Routing Protocol — протокол маршрутизации внешнего шлюза). Информацию о других протоколах маршрутизации, например Enhanced Interior Gateway Routing Protocol (EIGRP) и Open Shortest Path First (OSPF), можно получить в учебном пособии *CCNP: Routing Study Guide* издательства Sybex, предназначенного для подготовки к новому сертификационному экзамену Advanced Cisco Router Configuration.

**Т ВНИМАНИЕ** | Для сдачи экзамена CCNA 2 нужно знание только протоколов маршрутизации RIP и IGRP.

В объединенных сетях используются два типа протоколов маршрутизации: ИОР (Interior Gateway Protocol — протокол внутреннего шлюза) и ЕГР (Exterior Gateway Protocol — протокол внешнего шлюза). Протокол маршрутизации ИОР служит для обмена информацией о путях между маршрутизаторами одной автономной системы AS (autonomous system). Автономная система AS — это набор сетей в пределах общего административного домена. Протокол ЕГР нужен для взаимодействия между автономными системами AS. Примером протокола типа ЕГР является ВГР (Border Gateway Protocol — протокол граничного шлюза), который рассмотрен в учебном пособии *CCNP: Routing Study Guide*.

## Административное расстояние

Во время настройки протокола маршрутизации необходимо позаботиться об административном расстоянии AD (administrative distance). Это значение определяет степень доверия к информации о маршрутизации, полученной маршрутизатором от соседнего устройства. Административное расстояние выражено целым числом в диапазоне от 0 до 255, где 0 означает наибольшее доверие, а 255 — запрет передачи трафика по данному пути.

В таблице 5.2 показаны административные расстояния по умолчанию, которыми пользуются маршрутизаторы Cisco во время выбора пути к удаленной сети.

**Таблица 5.2.**

### Административные расстояния по умолчанию

Источник пути	Расстояние по умолчанию
Подключенный интерфейс	0
Статический путь	1
EIGRP	90
IGRP	100
OSPF	110
RIP	120
Внешний EIGRP	170
Неизвестен	255 (этот путь не будет использован)

Если сеть подключена непосредственно к маршрутизатору, то всегда используется интерфейс подключения. Если администратор установит статический путь, маршрутизатор всегда будет предпочитать его всем другим путям к той же сети. Можно изменить административное расстояние для статического пути, но по умолчанию оно равно 1.

## Протоколы маршрутизации

Существуют три класса протоколов маршрутизации:

**Вектора расстояния (Distance vector)** Протоколы маршрутизации по вектору расстояния используют для поиска наилучшего пути расстояние до удаленной сети. Каждое перенаправление пакета маршрутизатором называется участком (hop). Наилучшим считается путь к удаленной сети с наименьшим количеством участков. Вектор определяет направление к удаленной сети. Примерами протоколов маршрутизации по вектору расстояния являются RIP и IGRP.

**Состояние связи (Link state)** Обычно называется — "первым - кратчайший путь" (shortest path first). Каждый маршрутизатор создает три отдельные таблицы. Одна из них отслеживает непосредственно подключенных соседей, вторая — определяет топологию всей объединенной сети, а третья является таблицей маршрутизации. Устройство, действующее по протоколу типа состояния связи, имеет больше сведений об объединенной сети, чем любой протокол вектора расстояния. Примером IP-маршрутизации по состоянию связи является протокол OSPF.

**Гибридный (Hybrid)** Использует отдельные характеристики протоколов состояния связи и вектора расстояния (например, EIGRP).

Не существует единого способа конфигурации протоколов маршрутизации в любой произвольной сетевой среде. Эта задача решается с учетом особенностей конкретной сети. Однако знание различий в действии разных протоколов маршрутизации поможет выбрать наилучшее решение. В нашей книге и соответствующем сертификационном экзамене освещаются только теоретические аспекты протоколов маршрутизации и особенности протоколов маршрутизации по вектору расстояния.

### Протоколы маршрутизации по вектору расстояния

Алгоритм маршрутизации по вектору расстояния предполагает пересылку всей таблицы маршрутизации соседним устройствам. После этого соседний маршрутизатор объединяет полученную таблицу с собственной таблицей маршрутизации для построения полной карты сети. Это можно назвать маршрутизацией "за счет распространения слухов", поскольку маршрутизатор, получивший обновление от соседа, должен полностью полагаться на достоверность принятых от соседа данных об удаленной сети и не пытаться искать эту сеть самостоятельно.

Вполне возможно, что в сети существует несколько путей к одной удаленной сети. В этом случае сначала сравниваются административные расстояния путей. При совпадении значений, наилучший путь определяется по другим метрикам.

Протокол RIP пользуется при определении наилучшего пути в объединенной сети только счетчиком участков. Если RIP находит несколько путей к одной удаленной сети с одинаковыми счетчиками участков, автоматически выполняется циклическое чередование путей (карусельная

балансировка нагрузки — round-robin load balance). RIP способен сбалансировать нагрузку по шести связям с одинаковой стоимостью.

Однако при использовании в маршрутизации этого типа метрики проблема возникает, когда два пути к удаленной сети имеют одинаковые счетчики участков, но разную полосу пропускания. На рис. 5.5 показан пример двух связей с удаленной сетью 172.16.50.0.

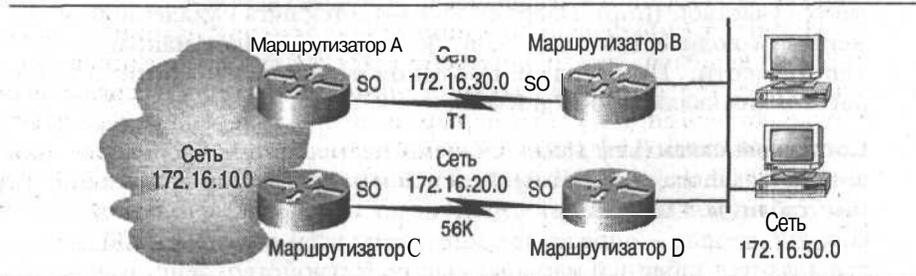
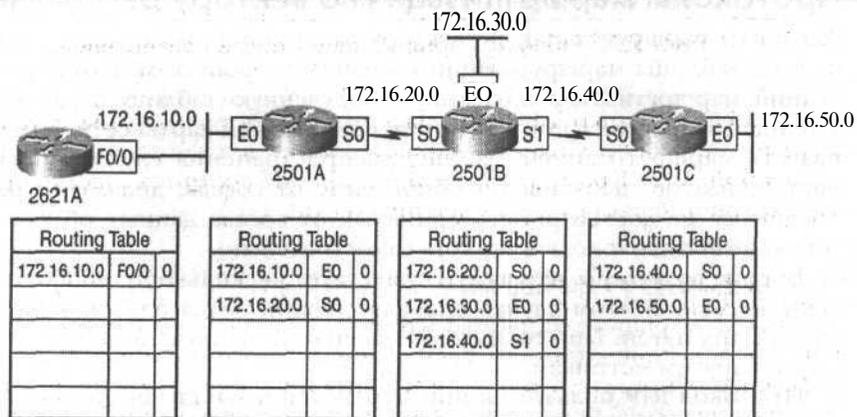


Рис. 5.5. Перегрузка по "узкому месту"

Сеть 172.16.30.0 является линией T1 с полосой пропускания 1.544 Мбит/с, а сеть 172.16.20.0 — линией 56К, поэтому маршрутизатор должен выбрать T1, а не связь 56К. Однако в маршрутизации по протоколу RIP единственной метрикой является счетчик участков, поэтому обе связи считаются одинаковыми по "весу". Такая ситуация называется *перегрузкой по "узкому месту"* (pinhole congestion).

Важно хорошо понять процедуру начала работы протокола маршрутизации по вектору расстояния. На рис. 5.6 показано, как четыре маршрутизатора начинают работу в состоянии, когда в таблице маршрутизации присутствуют сведения только о непосредственно подключенных сетях. После запуска протокола маршрутизации по вектору расстояния на



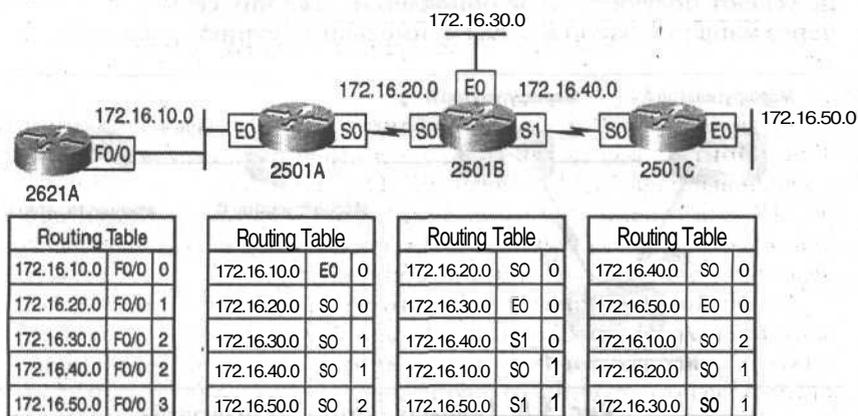
Routing Table - Таблица маршрутизации

Рис. 5.6. Объединенная сеть с маршрутизацией по вектору расстояния

каждом маршрутизаторе таблицы обновляются за счет добавления сведений о путях, собранных у соседних маршрутизаторов.

Как видно на рис. 5.6, каждый маршрутизатор имеет в таблице только записи о непосредственно подключенных сетях. Каждый маршрутизатор отправляет эту таблицу во все свои активные интерфейсы к другим маршрутизаторам. Таблица маршрутизации сопровождается данными о номере сети, выходном интерфейсе и счетчике участков.

На рис. 5.7 завершено создание таблиц маршрутизации, поскольку в них уже включена вся информация обо всех сетях объединенной сети. Это завершился процесс конвергенции (convergence, согласования). После конвергенции в сети маршрутизаторы завершают пересылку данных из своих таблиц. Поэтому, чем быстрее пройдет конвергенция, тем лучше. Заметим, что одним из основных недостатков протокола RIP является медленная конвергенция.



Routing Table - Таблица маршрутизации

Рис. 5.7. Таблицы маршрутизации после конвергенции

В таблице маршрутизации каждого устройства указаны сетевой номер, интерфейс, в который маршрутизатор должен направить пакет к удаленной сети. Кроме того, задано значение счетчика участков (метрики), которое характеризует удаленную сеть.

### Петля маршрутизации

Протокол "маршрутизация по вектору расстояния" отслеживает все изменения в объединенной сети за счет периодической широковещательной рассылки обновлений во все активные интерфейсы маршрутизации. В широковещательную рассылку включено все содержимое таблицы маршрутизации. Этот метод прекрасно работает, хотя требует процессорных циклов и полосы пропускания линий связи. Однако во время сбоя в сети могут возникнуть проблемы. Низкое время конвергенции протокола

"маршрутизация по вектору расстояния" приводит к несогласованности таблиц маршрутизации и возникновению петель маршрутизации (routing loop).

Петли (зацикливание пакетов) возникают из-за неодновременного обновления информации во всех маршрутизаторах. Предположим, отказал интерфейс к сети 5 на рис. 5.8. Все маршрутизаторы знают, что сеть 5 достижима через маршрутизатор Е. Маршрутизатор А в своей таблице имеет запись о пути в сеть 5 через маршрутизаторы В, С и Е. Когда отказывает сеть 5, маршрутизатор Е сообщает об этом маршрутизатору С. В свою очередь, маршрутизатор С останавливает маршрутизацию в сеть 5 через маршрутизатор Е. Однако маршрутизаторы А, В и D еще не знают об отказе сети 5, поэтому продолжают посылать информацию об обновлении, которая уже стала некорректной. Маршрутизатор С может послать такое обновление, что приведет к остановке маршрутизатором В процесса маршрутизации в сеть 5, но, возможно, что маршрутизаторы А и D еще не успеют получить такое обновление. Для них сеть 5 все еще доступна через маршрутизатор В с путем, имеющим метрику, равную трем.

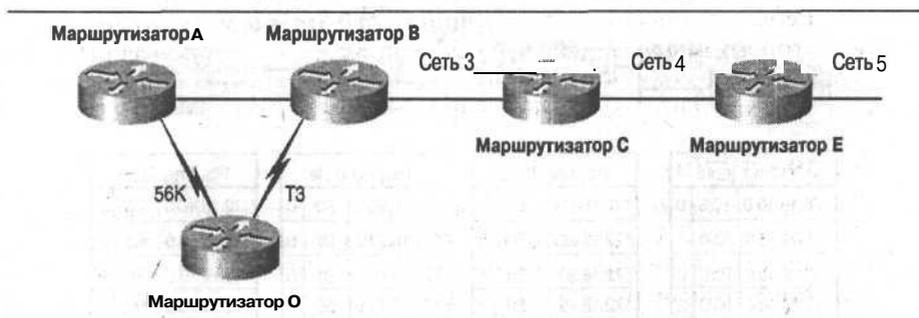


Рис. 5.8. Пример формирования петли

Маршрутизатор А посылает свое регулярное сообщение об обновлении через 30 с: "Привет, я все еще здесь — ниже перечислены связи, о которых мне известно". Причем в сообщении указано о достижимости сети 5. Маршрутизаторы В и D получают эту новость и поверят, что сеть 5 можно достичь через маршрутизатор А, поэтому отправят эту некорректную новость о доступности сети 5. Любой пакет к сети 5 будет направляться в маршрутизатор А, затем в В, а далее опять в А. Это и называется петлей маршрутизации. Возникает вопрос: "Как остановить этот процесс?"

### Максимальный счетчик участков

Рассмотренная выше проблема с петлей маршрутизации часто называется *счетом до бесконечности* (counting to infinity) и связана с распространением в объединенной сети "слухов" о некорректных путях. Без внешнего воздействия на этот процесс счетчик участков в пакете будет увеличиваться до бесконечности, за счет добавления единицы при проходе пакета через любой маршрутизатор.

Решить проблему позволит ограничение *максимального значения в счетчике участков*. Протокол вектора расстояния (RIP) предполагает счет участков до 15, поэтому любой путь с количеством участков 16 считается недостоверным (недостижимым). Следовательно, после подсчета до 15 участков сеть 5 считается отказавшей. Это означает, что устранение подсчета до бесконечности позволит устранить постоянное перемещение пакетов по петлям маршрутизации. Это решение действительно, но не устраняет саму **причину** формирования петель маршрутизации. Пакеты все же будут **какое-то** время перемещаться по петлям, поскольку вместо оперативной проверки пакеты удаляются (отбрасываются) после достижения счетчиком участков значения 16.

### Деление (расщепление) горизонта

Другим решением проблемы петель маршрутизации является *деление горизонта* (split horizon). Этот процесс устраняет некорректную информацию о маршрутизации и о перегрузке в протоколе вектора расстояния за счет установки правила. Согласно ему информация о маршрутизации не может передаваться в обратном направлении относительно направления, по которому она была получена. Деление горизонта не позволит маршрутизатору А послать обновление сведений обратно в маршрутизатор В, если они были получены от маршрутизатора В.

### Порча путей

Еще одной проблемой несогласованности обновлений является *порча путей* (route poisoning). Например, когда отказывает сеть 5, маршрутизатор Е сознательно инициирует порчу путей за счет вноса в таблицу записей для сети 5 со значением 16, т.е. устанавливает для этой сети состояние *недостижимости* (иногда называемое "бесконечным расстоянием" — infinite). За счет такого искажения пути к сети 5 маршрутизатор С перестает воспринимать некорректные обновления информации о путях в сеть 5. Когда маршрутизатор С получает сообщение о порче пути от маршрутизатора Е, то возвращает маршрутизатору Е специальное обновление, называемое "опасный реверс" (poison reverse). Это гарантирует, что все пути в его сегменте получили информацию о порче пути к удаленной сети.

Порча путей совместно с удержанием (см. ниже) позволяет ускорить время конвергенции, поскольку соседние маршрутизаторы могут не ждать 30 с (это целая вечность в мире компьютеров) перед объявлением о порче пути.

### Удержание

*Удержание* (holddown) предотвращает регулярные обновления о восстановлении пути, который был некоторое время недоступным, а также не допускает слишком быстрое изменение за счет установки определенного времени ожидания перед началом рассылки информации о восстановленном пути, либо стабилизации работы некоторой сети. Подобная задержка не позволяет слишком быстро начать изменение сведений о

наилучших путях. Маршрутизаторам предписывается ограничить на определенный период времени рассылку любых изменений, которые могут воздействовать на переключение состояния недавно удаленных путей. Это предотвращает преждевременное изменение таблиц маршрутизации за счет сведений о временно неработоспособных маршрутизаторах.

Когда маршрутизатор получает от своего соседа сообщение, указывающее, что ранее работоспособная сеть стала недоступной или выключенной, запускается таймер удержания. Если от соседа вскоре будет получено сообщение с лучшей метрикой доступа, чем для исходного пути к сети, состояние удержания заканчивается и возобновляется пересылка данных. Если же сообщение от соседнего маршрутизатора будет получено до сброса таймера удержания и оно определит меньшую метрику, чем у исходного пути, то такое сообщение игнорируется, а действие таймера удержания не прерывается. За счет удержания старых сведений увеличивается время конвергенции в сети.

В процессе удержания используются триггерные обновления. Они сбрасывают счетчики удержания для уведомления соседнего маршрутизатора об изменениях в сети. А отличие от сообщений об обновлении от соседнего маршрутизатора заключается в том, что триггерные обновления инициируют создание новой таблицы маршрутизации, которая медленно рассылается всем соседним устройствам. Подобное обновление определяет изменение топологии сети.

Существуют три условия, определяющие сброс счетчика удержания при получении триггерного обновления:

1. Закончилось время удержания.
2. Маршрутизатор нагружен заданиями по обработке пропорционально количеству связей в объединенной сети.
3. Другое обновление указывает на изменение статуса (состояния) сети.

## Протокол RIP

Протокол RIP (Routing Information Protocol) в полной мере является протоколом маршрутизации по вектору расстояния. Этот протокол предписывает рассылку полной таблицы маршрутизации во все активные интерфейсы устройства через 30 с. RIP пользуется для выбора наилучшего пути к удаленной сети только счетчиком участков, но допускается счет только до 15 участков, т.е. значение 16 этого счетчика говорит о недостижимости сети. RIP подходит для небольших сетей, но не применим в крупных сетях с медленными связями по региональным промежуточным сетям, либо в сетях с большим числом установленных маршрутизаторов.

RIP версии 1 использует только полноклассовую маршрутизацию, т.е. все устройства в сети обязаны иметь одинаковую маску подсети. Это связано с тем, что RIP версии 1 не дополняет сообщения об обновлениях сведениями о маске подсети. RIP версии 2 обеспечивает префиксную

маршрутизацию (prefix routing) и включает в обновления о путях сведения о маске подсети. Это называется *бесклассовой маршрутизацией*. Далее в книге обсуждается только протокол RIP версии 1, поскольку этого достаточно для сдачи сертификационного экзамена CCNA.

## Таймеры RIP

Для управления производительностью в RIP используются три типа таймеров:

**Таймер обновления пути (Route update timer)** Устанавливает интервал (обычно 30 с) между периодическими обновлениями информации о маршрутизации. Здесь маршрутизатор отправляет полную копию своей таблицы маршрутизации всем своим соседям.

**Таймер некорректного пути (Route invalid timer)** Определяет время (90 с), по истечению которого маршрутизатор начинает считать путь неправильным. Это решение основывается на том, что за установленный период времени не было никаких уведомлений о данном пути. Когда это происходит, маршрутизатор посылает обновления всем своим соседям, указывая на некорректность такого пути.

**Таймер очистки пути (Route flush timer)** Устанавливает время (240 с) между признанием пути некорректным и удалением его из таблицы маршрутизации. Перед удалением пути из таблицы маршрутизатор уведомляет своих соседей о неправильности пути. Значение таймера некорректного пути должно быть меньше значения таймера очистки пути. Это предоставит маршрутизатору достаточное время для уведомления соседей о неправильном пути перед тем, как будет обновлена таблица маршрутизации.

## Настройка маршрутизации по протоколу RIP

Для настройки маршрутизации по протоколу RIP нужно включить этот протокол командой `router rip` и указать протоколу RIP сеть, в которой будет проводиться маршрутизация. Покажем на примере четырех наших маршрутизаторов настройку RIP в объединенной сети.

### 2621A

RIP имеет административное расстояние равное 120. Статические пути имеют административное расстояние 1 по умолчанию и, поскольку мы уже ранее настроили статические пути, таблицы маршрутизации не будут распространять сведения для протокола RIP. Предварительно удалите статические пути во всех маршрутизаторах. Это выполняется командой `ip route`. Заметим, что в показанном ниже листинге для маршрутизатора 2621A необходимо ввести команду `ip route` для удаления элементов таблицы.

```
2621A#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
2621A(config)#no ip route 172.16.20.0 255.255.255.0 172.16.10.2
2621A(config)#no ip route 172.16.30.0 255.255.255.0 172.16.10.2
2621A(config)#no ip route 172.16.40.0 255.255.255.0 172.16.10.2
2621A(config)#no ip route 172.16.50.0 255.255.255.0 172.16.10.2
```

После удаления из конфигурации статических путей можно добавить протокол маршрутизации RIP командой `route rip` и командой `network`. Команда `network` указывает протоколу маршрутизации сеть, где нужно выполнять рассылку обновлений. Заметим, что в показанной ниже конфигурации маршрутизатора не указана подсеть, следовательно, границами рассылки станет полноклассовая область в сети. RIP найдет нужную подсеть и будет уведомлять о ней устройства.

```
2621A(config)#router rip
2621A(config-router)#network 172.16.0.0
2621A(config-router)#^Z
2621A#
```

Как показывает листинг, достаточно двух команд, что гораздо меньше, чем при установке статических путей. Однако не следует забывать о дополнительной нагрузке на процессор маршрутизатора и занимаемую полосу пропускания.

## 2501A

Для настройки RIP в маршрутизаторе 2501A следует удалить три статических пути, созданных в предыдущей серии упражнений. Проверив, что в таблице маршрутизации больше нет путей с административным расстоянием меньше 120, можно добавить RIP. Если не удалить статические пути, то маршрутизатор не будет использовать протокол RIP.

```
2501A#config t
Enter configuration commands, one per line. End with CNTL/Z.
2501A(config)#no ip route 172.16.30.0 255.255.255.0 172.16.20.2
2501A(config)#no ip route 172.16.40.0 255.255.255.0 172.16.20.2
2501A(config)#no ip route 172.16.50.0 255.255.255.0 172.16.20.2
2501A(config)#router rip
2501A(config-router)#network 172.16.0.0
2501A(config-router)#^Z
2501A#
```

## 2501B

Маршрутизатор 2501B имеет только два статических пути. После их удаления можно включить маршрутизацию по протоколу RIP.

```
2501B#config t
Enter configuration commands, one per line. End with CNTL/Z.
2501B(config)#no ip route 172.16.10.0 255.255.255.0 172.16.20.1
2501B(config)#no ip route 172.16.50.0 255.255.255.0 172.16.40.2
```

```
2501B(config)#router rip
2501B(config-router)#network 172.16.0.0
2501B(config-router)#^Z
2501B#
```

## 2501C

Маршрутизатор 2501C был маршрутизатором по умолчанию, поскольку мы ввели команду default route. После удаления режима путей по умолчанию, можно добавить маршрутизацию RIP.

```
RouterC#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterC(config)#no ip route 0.0.0.0 0.0.0.0 172.16.40.1
RouterC(config)#router rip
RouterC(config-router)#network 172.16.0.0
RouterC(config-router)#^Z
RouterC#
05:10:31: %SYS-5-CONFIG_I: Configured from console by console
```

Важно понять причины выполнения показанных операций. Непосредственно подключенные пути имеют административное расстояние 0, статические пути — административное расстояние 1, а протокол RIP — 120. Часто протокол RIP называют "распространителем слухов и сплетен", поскольку иногда с его помощью рассылаются некорректные данные.

## Проверка таблиц маршрутизации для протокола RIP

На данный момент все таблицы маршрутизации в нашем примере хранят сведения о непосредственно подключенных путях и путях, добавленных протоколом RIP по обновлениям от соседних маршрутизаторов.

Ниже показано содержимое таблицы маршрутизации устройства 2621A.

```
2621A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets
R 172.16.50.0 [120/3] via 172.16.10.2, FastEthernet0/0
R 172.16.40.0 [120/2] via 172.16.10.2, FastEthernet0/0
R 172.16.30.0 [120/2] via 172.16.10.2, FastEthernet0/0
R 172.16.20.0 [120/1] via 172.16.10.2, FastEthernet0/0
C 172.16.10.0 is directly connected, FastEthernet0/0
2621A#
```

Согласно листингу, таблица маршрутизации содержит те же самые записи, что и для случая со статическими путями. Однако символ R в записи указывает на динамически добавленную сеть по протоколу маршрутизации RIP. Значение [120/3] — это административное расстояние пути (120) вместе с количеством участков до удаленной сети (3).

В следующем листинге показана таблица маршрутизации устройства 2501A.

```
2501A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 5 subnets
R 172.16.50.0 [120/2] via 172.16.20.2, 00:00:11, Serial0
R 172.16.40.0 [120/1] via 172.16.20.2, 00:00:11, Serial0
R 172.16.30.0 [120/1] via 172.16.20.2, 00:00:11, Serial0
C 172.16.20.0 is directly connected, Serial0
C 172.16.10.0 is directly connected, Ethernet0
2501A#
```

В данном случае мы опять получили записи о тех же самых путях, хотя и не вводили их вручную.

Следующие таблицы маршрутизации получены в устройствах 2501B и 2501C.

```
2501B#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 5 subnets
R 172.16.50.0 [120/1] via 172.16.40.2, 00:00:26, Serial1
C 172.16.40.0 is directly connected, Serial1
C 172.16.30.0 is directly connected, Ethernet0
C 172.16.20.0 is directly connected, Serial0
R 172.16.10.0 [120/1] via 172.16.20.1, 00:00:04, Serial0
2501B#
```

```
RouterC#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M — [листинг сокращен]
Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 5 subnets
C 172.16.50.0 is directly connected, Ethernet0
C 172.16.40.0 is directly connected, Serial0
R 172.16.30.0 [120/1] via 172.16.40.1, 00:00:06, Serial0
R 172.16.20.0 [120/1] via 172.16.40.1, 00:00:06, Serial0
R 172.16.10.0 [120/2] via 172.16.40.1, 00:00:06, Serial0
RouterC#
```

RIP работает с маршрутизацией в небольших сетях. Однако при максимальном значении счетчика участков 15 (значение 16 трактуется как недостижимость сети) и полном обновлении таблицы маршрутизации через каждые 30 секунд, протокол не сможет поддержать работу крупной объединенной сети.

## Удержание распространения информации по протоколу RIP

Иногда разумнее ограничить распространение информации RIP по всей локальной или региональной сети. Например, можно запретить отсылку уведомлений протокола RIP в Интернет.

Существуют разные способы остановки распространения нежелательных уведомлений RIP по всем локальным или региональным сетям. Проще всего использовать команду `passive-interface`. Она предотвращает отправку в указанный интерфейс широковещательных уведомлений RIP. Однако подобный интерфейс сохраняет способность принимать обновления RIP.

Пример настройки маршрутизатора командой `passive-interface`:

```
RouterA#config t
RouterA(config)#router rip
RouterA(config-router)#network 10.0.0.0
RouterA(config-router)#passive-interfaceserial 0
```

Данная команда отменит распространение обновлений RIP через последовательный интерфейс `serial 0`, но этот же интерфейс будет принимать обновления RIP от внешних источников.

## Протокол IGRP

Протокол маршрутизации внутреннего шлюза IGRP (Interior Gateway Routing Protocol) — это лицензированный компанией Cisco протокол маршрутизации по вектору расстояния. Для использования IGRP в сети все маршрутизаторы должны быть маршрутизаторами Cisco. Компания Cisco разработала этот протокол маршрутизации для устранения недостатков протокола RIP.

IGRP имеет максимальное значение счетчика участков 255, причем по умолчанию используется значение 100. Это полезно в крупных сетях, где недостаточно коротких путей из 15 участков, которые способен поддерживать протокол RIP. Кроме того, протокол IGRP использует иную метрику, чем протокол RIP. В IGRP оцениваются полоса пропускания и задержка линии, причем эти две характеристики применяются по умолчанию для выбора наилучшего пути в объединенной сети. Такая метрика называется композитной (*composite metric*). Можно использовать надежность, нагрузку и MTU (Maximum Transmission Unit — максимальный передаваемый элемент), но эти характеристики не применяются по умолчанию.

## Таймеры IGRP

Для управления производительностью протокол IGRP использует следующие таймеры при указанных ниже значениях по умолчанию:

**Таймер обновления (Update timer)** Определяет, как часто должны отсылаться сообщения обновлений о маршрутизации. Значение по умолчанию равно 90 с.

**Таймер некорректности (Invalid timer)** Указывает, как долго маршрутизатор должен ожидать перед объявлением пути неправильным, если маршрутизатор не получает обновлений об этом пути. Значение по умолчанию в три раза больше таймера обновления.

**Таймер удержания (Holddown timer)** Определяет период удержания. Значение по умолчанию равно троекратному значению таймера обновления плюс 10 с.

**Таймер очистки (Flush timer)** Указывает, насколько долго следует отложить очистку записи о пути в таблице маршрутизации. Значение по умолчанию в семь раз больше таймера обновления.

## Настройка маршрутизации по протоколу IGRP

Для настройки маршрутизации по протоколу IGRP используются те же самые команды, что и для конфигурации маршрутизации по протоколу RIP. Однако существует одно отличие: необходимо указывать номер автономной системы (AS). Все маршрутизаторы в пределах одной автономной системы должны использовать одинаковый номер AS. В противном случае они не смогут обмениваться информацией о маршрутизации. Пример включения маршрутизации по протоколу IGRP:

```
RouterA#config t
RouterA(config)#router igrp 10
RouterA(config-router)#network 172.16.0.0
```

На листинге видно, что настроить маршрутизацию по протоколу IGRP не сложнее, чем сконфигурировать RIP, хотя обязательным является указание номера AS. Этот номер предписывает посылать уведомления только тем маршрутизаторам, с которыми предполагается совместно использовать информацию о маршрутизации.

Протокол IGRP способен балансировать нагрузку по шести неэквивалентным линиям связи. В сетях RIP для балансировки нагрузки необходимо иметь одинаковые значения счетчиков участков, но в IGRP для принятия решения о балансировке используется полоса пропускания. Для балансировки нагрузки между связями с неодинаковой стоимостью служит команда `variance`, которая распределяет нагрузку согласно наилучшей и наихудшей метрики.

Еще две команды помогают управлять распределением трафика между совместно используемыми путями IGRP: `traffic-share balanced` и `traffic-share min`.

Ниже показаны доступные параметры при вводе команды `router igrp`.

`Router(config-router)#variance ?`

<1-128> Metric variance multiplier  
(множитель метрики `variance` — "изменение")

`Router(config-router)#traffic-share ?`

`balanced` Share inversely proportional to metric  
(совместное использование обратно пропорционально метрике)  
`min` All traffic shared among min metric paths  
(весь трафик направляется по пути с минимальной метрикой)

В листинге из маршрутизатора показано, что команда `variance` имеет множитель метрики. У команды `traffic-share` есть два параметра: `balanced` и `min`. Команда `traffic-share balanced` указывает протоколу маршрутизации IGRP на совместное использование связей обратно пропорционально метрикам, а команда `traffic-share min` предписывает маршрутизацию только по связям с минимальным "весом".

#### Т ВНИМАНИЕ

Балансировка нагрузки и совместное использование линий для разделения трафика рассмотрено в книге *CCNP: Routing Study Guide* издательства Sybex.

## Настройка IGRP в объединенной сети

Настройка протокола IGRP — понятный процесс, мало отличающийся от конфигурации RIP. Следует выбрать номер автономной системы AS еще до начала настройки маршрутизаторов. Помните, что все маршрутизаторы в объединенной сети должны иметь одинаковый номер AS, чтобы обмениваться информацией о маршрутизации. В нашем примере объединенной сети использован номер AS, равный 10.

Начнем настройку объединенной сети на маршрутизацию по протоколу IGRP.

### 2621A

Показанный в листинге из маршрутизатора номер AS может быть любым целым числом из диапазона 1 — 65535. Маршрутизатор может быть членом столько автономных систем AS, сколько требуется в конкретной сети.

```
2621A#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
2621A(config)#router igrp ?
```

```
<1-65535> Autonomous system number
```

V

```
2621A(config)#router igrp 10
2621A(config-router)#netw 172.16.0.0
2621A(config-router)#^Z
2621A#
```

Команда `router igrp` включает маршрутизацию **IGRP**. Как и для протокола **RIP**, нужно добавить номер сети, в которой предполагается распространение обновлений. **IGRP** пользуется полноклассовой маршрутизацией, т.е. в сообщениях об обновлении не указана маска подсети.

## 2501A

Для настройки маршрутизатора **2501A** достаточно включить **IGRP** с номером **AS**, равным **10**, а затем добавить сетевой номер:

```
2501A#config t
Enter configuration commands, one per line. End with CNTL/Z.
2501A(config)#router igrp 10
2501A(config-router)#netw 172.16.0.0
2501A(config-router)#^Z
2501A#
```

## 2501B

Для настройки **2501B** следует, как и прежде, включить **IGRP** с номером **AS**, равным **10**.

```
2501B#config t
Enter configuration commands, one per line. End with CNTL/Z.
2501B(config)#router igrp 10
2501B(config-router)#netw 172.16.0.0
2501B(config-router)#^Z
2501B#
```

## 2501C

Последним настраивается маршрутизатор **2501C**, причем тоже с номером **AS**, равным **10**.

```
2501C#config t
Enter configuration commands, one per line. End with CNTL/Z.
2501C(config)#router igrp 10
2501C(config-router)#netw 172.16.0.0
2501C(config-router)#^Z
RouterC#
```

## Проверка таблиц маршрутизации по протоколу IGRP

После настройки маршрутизаторов проверьте их конфигурации. Используйте команду `show ip route`.

Во всех показанных ниже листингах присутствуют только пути к непосредственно подключенным сетям и пути, добавленные протоколом IGRP. Поскольку мы не выключили RIP, этот протокол продолжает работать в фоновом режиме, причем, как и раньше, занимает циклы процессоров маршрутизаторов и полосу пропускания линий. Однако в таблицах маршрутизации никогда не будут использованы пути, найденные по протоколу RIP, поскольку IGRP имеет лучшее административное расстояние по сравнению с RIP.

Пример листинга для маршрутизатора 2621A (обратите внимание, что в таблице маршрутизации присутствуют все пути).

```
2621A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - [листинг сокращен]
 T - traffic engineered route
Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 5 subnets
I 172.16.50.0 [100/160360] via 172.16.10.2, FastEthernetO/0
I 172.16.40.0 [100/160260] via 172.16.10.2, FastEthernetO/0
I 172.16.30.0 [100/158360] via 172.16.10.2, FastEthernetO/0
I 172.16.20.0 [100/158260] via 172.16.10.2, FastEthernetO/0
C 172.16.10.0 is directly connected, FastEthernetO/0
```

Символом I отмечены пути, добавленные по протоколу IGRP. Значение [100/160360] показывает административное расстояние IGRP и ком-  
позитивную метрику. Чем меньше значение этой метрики, тем лучше путь.

Ниже показана таблица маршрутизации из устройства 2501A.

```
2501A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - [листинг сокращен]
 U - per-user static route, o - ODR
Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 5 subnets
I 172.16.50.0 [100/160350] via 172.16.20.2, 00:00:49, Serial0
I 172.16.40.0 [100/160250] via 172.16.20.2, 00:00:49, Serial0
I 172.16.30.0 [100/158350] via 172.16.20.2, 00:00:49, Serial0
C 172.16.20.0 is directly connected, Serial0
C 172.16.10.0 is directly connected, Ethernet0
2501A#
```

Таблица маршрутизации из 2501B:

```
2501B#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - [листинг сокращен]
 U - per-user static route, o - ODR
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets
I 172.16.50.0 [100/8576] via 172.16.40.2, 00:01:11, Serial1
C 172.16.40.0 is directly connected, Serial1
C 172.16.30.0 is directly connected, Ethernet0
C 172.16.20.0 is directly connected, Serial0
I 172.16.10.0 [100/158350] via 172.16.20.1, 00:00:36, Serial0
2501B#
```

Таблица маршрутизации из 2501C:

```
2501C#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - [листинг сокращен]
 U - per-user static route, o - ODR
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets
C 172.16.50.0 is directly connected, Ethernet0
C 172.16.40.0 is directly connected, Serial0
I 172.16.30.0 [100/8576] via 172.16.40.1, 00:00:28, Serial0
I 172.16.20.0 [100/160250] via 172.16.40.1, 00:00:28, Serial0
I 172.16.10.0 [100/160350] via 172.16.40.1, 00:00:28, Serial0
2501C#
```

## Проверка конфигурации

После завершения настройки следует проверить конфигурацию, чтобы гарантировать завершение самого процесса настройки. Ниже перечислены команды, используемые для проверки в маршрутизаторе Cisco выполнения процесса маршрутизации и используемого для этого протокола. Первая из представленных команд уже обсуждалась в предыдущем разделе книги. Остальные команды рассмотрены ниже.

- show ip route
- show protocols
- show ip protocol
- debug ip rip
- debug ip igrp events
- debug ip igrp transactions

## Команда Show Protocols

Команда show protocols показывает сконфигурированные в каждом интерфейсе адреса сетевого уровня.

```
2501B#sh protocol
Global values:
 Internet Protocol routing is enabled
 (разрешена маршрутизация по протоколу IP)
Ethernet0 is up, line protocol is up
(интерфейс Ethernet0 включен, протокол линии включен)
 Internet address is 172.16.30.1/24
 (адрес Интернета: 172.16.30.1/24)
Serial0 is up, line protocol is up
 Internet address is 172.16.20.2/24
Serial1 is up, line protocol is up
 Internet address is 172.16.40.1/24
2501B#
```

В листинге показаны IP-адреса интерфейсов Ethernet 0, serial 0 и serial 1 маршрутизатора 2501B. Если в маршрутизаторе сконфигурированы протоколы IPX или AppleTalk, то для них будут дополнительно показаны сетевые адреса.

## Команда Show IP Protocol

Команда show ip protocol показывает протоколы, сконфигурированные в маршрутизаторе. Обратите внимание, что в показанном ниже листинге представлены два протокола (RIP и IGRP), которые исполняются маршрутизатором, но только IGRP содержится в таблице маршрутизации, поскольку этот протокол имеет меньшее административное расстояние.

Команда show ip protocols выводит значения таймеров протокола маршрутизации. В листинге отмечено, что RIP посылает обновления каждые 30 с, что устанавливается по умолчанию. Кроме того, RIP выполняет маршрутизацию в сети 172.16.0.0, а два соседних маршрутизатора найдены по адресам 172.16.40.2 и 172.16.20.1.

```
2501B#sh ip protocol
Routing Protocol is "rip"
 Sending updates every 30 seconds, next due in 6 seconds Invalid after
 180 seconds, hold down 180, flushed after 240
 (Обновления отсылаются каждые 30 с, причем следующее будет отправлено
 через 6 с. Некорректность наступает через 180 с, удержание — 180,
 а очистка — 240)
 Outgoing update filter list for all interfaces is
 (выходной фильтр обновление для всех интерфейсов)
 Incoming update filter list for all interfaces is
 (входной фильтр обновление для всех интерфейсов)
```

```

Redistributing: rip
(перераспределение по протоколу RIP)
Default version control: send version 1, receive any version
(управление версией по умолчанию: для отсылки — версия 1,
для приема — любая версия)
 Interface Send Recv Key-chain
(Интерфейс Послано Получено Ключевая цепочка)
 Ethernet0 1 12
 Serial0 1 12
 Serial1 1 12

Routing for Networks:
(маршрутизация для сети)
 172.16.0.0

Routing Information Sources:
(источники информации о маршрутизации)
 Gateway Distance Last Update
(Шлюз Расстояние Последнее обновление)
 172.16.40.2 120 00:00:21
 172.16.20.1 120 00:00:23

Distance: (default is 120)
(расстояние: по умолчанию 120)

```

В показанном листинге из маршрутизатора последний элемент определяет административное расстояние по умолчанию для RIP (120).

В следующем листинге показана информация о маршрутизации по протоколу IGRP. По умолчанию значение таймера обновления равно 90 с, а административное расстояние — 100.

```

Routing Protocol is "igrp 10"
 Sending updates every 90 seconds, next due in 42 seconds
 Invalid after 270 seconds, hold down 280, flushed after 630
 Outgoing update filter list for all interfaces is
 Incoming update filter list for all interfaces is
 Default networks flagged in outgoing updates
(сеть по умолчанию маркирована для выходных обновлений)
 Default networks accepted from incoming updates
(сеть по умолчанию доступна для входных обновлений)
 IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
(вес метрики IGRP: K1=1, K2=0, K3=1, K4=0, K5=0)
 IGRP maximum hopcount 100
(максимальное значение счетчика участков IGRP: 100)
 IGRP maximum metric variance 1
(максимальное изменение метрики IGRP: 1)
 Redistributing: eigrp 10, igrp 10
 Routing for Networks:
 172.16.0.0
 Routing Information Sources:

```

Gateway	Distance	Last Update
172.16.40.2	100	00:00:47
172.16.20.1	100	00:01:18

Distance: (default is 100)

В выведенной командой `show ip protocols` информации присутствует номер AS, значения таймеров маршрутизации, сети, в которых выполняются уведомления, а также шлюзы и административное расстояние (100).

Таймер некорректности установлен в 270 с, что в три раза больше таймера обновления. Если обновления от маршрутизатора не будут получены в течение трех периодов обновления, путь считается некорректным. Таймер удержания равен 280 с, что примерно в три раза больше таймера обновления. Это значение определяет подавление пути при ожидании поступления нового обновления. Если новое обновление не будет получено в течение интервала таймера удержания, то запускается счет таймера очистки. Когда истечет и этот интервал, путь удаляется из маршрутизатора.

## Команда Debug IP RIP

Команда `debug ip rip` посылает и принимает обновление маршрутизации от имени устройства в консольном сеансе. Если подключиться к маршрутизатору по Telnet, придется ввести команду `terminal monitor`, чтобы получить листинг из команды `debug`.

В показанном ниже примере листинга видно, что обновления протокола RIP посланы и получены интерфейсами `serial 1`, `serial 0` и `Ethernet 0`. Команда `debug ip rip` является хорошим отладочным средством, а метрикой выступает счетчик участков.

```
2501B#debug ip rip
RIP protocol debugging is on
2501B#
07:12:56: RIP: received v1 update from 172.16.40.2 on Serial1
07:12:56: 172.16.50.0 in 1 hops
07:12:56: RIP: received v1 update from 172.16.20.1 on Serial0
07:12:56: 172.16.10.0 in 1 hops
07:12:58: RIP: sending v1 update to 255.255.255.255 via
Ethernet0 (172.16.30.1)
07:12:58: subnet 172.16.40.0, metric 1
07:12:58: subnet 172.16.20.0, metric 1
07:12:58: RIP: sending v1 update to 255.255.255.255 via
Serial0 (172.16.20.2)
07:12:58: subnet 172.16.40.0, metric 1
07:12:58: subnet 172.16.30.0, metric 1
07:12:58: RIP: sending v1 update to 255.255.255.255 via
Serial1 (172.16.40.1)
```

```
07:12:58: subnet 172.16.30.0, metric 1
07:12:58: subnet 172.16.20.0, metric 1
2501B#undebug all
All possible debugging has been turned off
2501B#
```

Для выключения режима отладки следует ввести `undebug all` или `no debug all`. Можно использовать краткую форму `un all`.

## Команда Debug IP IGRP

Команда `debug ip igrp` имеет два параметра: `events` (события) и `transactions` (транзакции), что и показано в листинге:

```
2501B#debug ip igrp ?
 events IGRP protocol events
 transactions IGRP protocol transactions
```

Различия между двумя видами команды рассмотрено **ниже**.

## Команда Debug IP IGRP Events

Команда `debug ip igrp events` выводит итоговые сведения о маршрутизации IGRP в сети. Ниже показан листинг, где выведены источник, назначение для каждого обновления, а также количество маршрутизаторов. Данная команда не генерирует информацию о некорректных путях.

```
2501B#debug ip igrp events
IGRP event debugging is on
07:13:50: IGRP: received request from 172.16.40.2 on Serial1
07:13:50: IGRP: sending update to 172.16.40.2 via Serial1
(172.16.40.1)
07:13:51: IGRP: Update contains 3 interior, 0 system, and 0 exterior routes.
07:13:51: IGRP: Total routes in update: 3
07:13:51: IGRP: received update from 172.16.40.2 on Serial1
07:13:51: IGRP: Update contains 1 interior, 0 system, and 0 exterior routes.
07:13:51: IGRP: Total routes in update: 1
2501B#un
07:13:52: IGRP: received update from 172.16.40.2 on Serial1
07:13:52: IGRP: Update contains 1 interior, 0 system, and 0 exterior routes.
07:13:52: IGRP: Total routes in update: 1
2501B#un all
All possible debugging has been turned off

Выключить режим отладки позволит команда undebug all.
```

### Команда Debug IP IGRP Transactions

Команда `debug ip igrp transactions` показывает сообщения запросов от соседних маршрутизаторов с требованием на обновление, а также широко-вещательные рассылки, посланные маршрутизатором соседнему маршрутизатору.

В показанном ниже листинге запрос получен от соседнего маршрутизатора из сети 172.16.40.2 в интерфейс serial 1 устройства 2501B. Маршрутизатор 2501B ответил на запрос пакетом обновления.

```
2501B#debug ip igrp transactions
```

```
IGRP protocol debugging is on
```

```
07:14:05: IGRP: received request from 172.16.40.2 on Serial1
```

```
07:14:05: IGRP: sending update to 172.16.40.2 via Serial1 (172.16.40.1)
```

```
07:14:05: subnet 172.16.30.0,metric=1100
```

```
07:14:05: subnet 172.16.20.0, metric=158250
```

```
07:14:05: subnet 172.16.10.0,metric=158350
```

```
07:14:06: IGRP: received update from 172.16.40.2 on Serial1
```

```
07:14:06: subnet 172.16.50.0,metric 8576 (neighbor 1100)
```

```
2501B#un all
```

```
All possible debugging has been turned off
```

```
2501B#
```

Действие данной команды отключается `undebug all` (краткая форма: `un all`).

## Упражнение

---

Запишите ответы на следующие вопросы.

1. Создайте статический путь к сети 172.16.10.0/24 для шлюза следующего участка 172.16.20.1 и административного расстояния 150.
2. Напишите команду включения в маршрутизаторе протокола RIP и рассылки уведомлений в сети 10.0.0.0.
3. Напишите команду запрета распространения протоколом RIP информации в интерфейсе serial 1.
4. Напишите команду создания автономной системы AS с номером 10 и протоколом IGRP в сети 172.16.0.0.
5. Напишите команду настройки пути по умолчанию из маршрутизатора в сеть 172.16.50.3.
6. Что работает с триггерными обновлениями и помогает устранить петли маршрутизации в сетях с протоколом по вектору расстояния?

7. Что устраняет петли маршрутизации в сетях с протоколом по вектору расстояния за счет пересылки максимального значения счетчика участков при неисправности связи?
8. Что устраняет петли маршрутизации в сетях с протоколом по вектору расстояния за счет отмены повторной отправки информации, полученной из того же самого интерфейса?
9. Команда управления балансировкой нагрузки между наибольшей и наименьшей допустимыми метриками.
10. Какая команда используется для отправки и получения обновлений маршрутизации из консольного сеанса?

## Лабораторная работа

В следующей лабораторной работе мы сконфигурируем сеть, содержащую три маршрутизатора 2501 и один маршрутизатор 2621.

На рис. 5.9 показаны исходные данные для настройки каждого маршрутизатора.

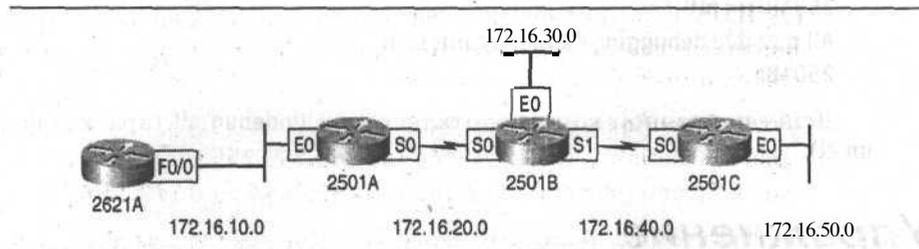


Рис. 5.6. Объединенная сеть для лабораторной работы

### О Лабораторная работа 5.1.

#### Создание статических путей

В первой лабораторной работе мы создадим статические пути в четырех маршрутизаторах, для маршрутизации во всей объединенной сети. Проверку конфигураций проведем программой Ping.

1. Маршрутизатор 2621 подключен к сети 172.16.10.0/24. Он не знает о сетях 172.16.20.0/24, 172.16.30.0/24, 172.16.40.0/24 и 172.16.50.0/24. Статические пути в маршрутизаторе 2621 создаются для того, чтобы он смог "увидеть" все сети.

```
2621#config t
2621(config)#ip route 172.16.20.0 255.255.255.0 172.16.10.1
2621(config)#ip route 172.16.30.0 255.255.255.0 172.16.10.1
2621(config)#ip route 172.16.40.0 255.255.255.0 172.16.10.1
2621(config)#ip route 172.16.50.0 255.255.255.0 172.16.10.1
```

2. Сохраните текущую конфигурацию маршрутизатора 2621, перейдя в режим разрешения (enabled mode), а затем указав команду `copy run start` и нажав `Enter`.
3. В маршрутизаторе А создадим статические пути к сетям 172.16.10.0/24, 172.16.30.0/24, 172.16.40.0/24 и 172.16.50.0/24.

```
RouterA#config t
RouterA(config)#iproute 172.16.30.0255.255.255.0 172.16.20.2
RouterA(config)#iproute 172.16.40.0 255.255.255.0 172.16.20.2
RouterA(config)#iproute 172.16.50.0 255.255.255.0 172.16.20.2
```

Эти команды указывают маршрутизатору А на то, как достичь сети 172.16.30.0/24 и использовать IP-адрес 172.16.20.2, который является ближайшим соседним интерфейсом, подключенным к сети 172.16.30.0/24 (т.е. маршрутизатору В). Этот же интерфейс будет использоваться для доступа к сетям 172.16.40.0/24 и 172.16.50.0/24.

4. Сохраните конфигурацию маршрутизатора А, перейдя в режим разрешения, напечатав `copy run start` и нажав `Enter`.
5. В маршрутизаторе В создайте статический путь к сетям 172.16.10.0/24 и 172.16.50.0/24, которые подключены к устройству непосредственно. Создайте в маршрутизаторе В статические пути для "видимости" остальных сетей:

```
RouterB#config t
RouterB(config)#iproute 172.16.10.0 255.255.255.0 172.16.20.1
RouterB(config)#iproute 172.16.50.0 255.255.255.0 172.16.40.2
```

Первая команда указывает маршрутизатору В, что для доступа к сети 172.16.10.0/24 следует использовать 172.16.20.1. Следующая команда предписывает доступ к сети 172.16.50.0/24 через 172.16.40.2.

Перейдите в режим разрешения, введите `copy run start` и нажмите `Enter`, чтобы сохранить текущую конфигурацию маршрутизатора В.

6. Маршрутизатор С подключен к сетям 172.16.50.0/24 и 172.16.40.0/24. Это устройство не знает о сетях 172.16.30.0/24, 172.16.20.0/24 и 172.16.10.0/24. Создайте статические пути, чтобы маршрутизатор С "увидел" все сети:

```
RouterC#config t
RouterC(config)#iproute 172.16.30.0 255.255.255.0 172.16.40.1
RouterC(config)#iproute 172.16.20.0 255.255.255.0 172.16.40.1
RouterA(config)#iproute 172.16.10.0 255.255.255.0 172.16.40.1
```

Перейдите в режим разрешения, введите `copy run start` и нажмите `Enter`, чтобы сохранить текущую конфигурацию маршрутизатора С.

Проверьте по `Ping` хосты и маршрутизаторы с каждого маршрутизатора. Если все настроено правильно, должны быть успешными все проверки.

## О Лабораторная работа 5.2.

### Динамическая маршрутизация по протоколу RIP

В этой лабораторной работе мы используем динамический протокол маршрутизации RIP вместо статической маршрутизации и маршрутизации по умолчанию.

1. Удалите все статические пути в маршрутизаторах командой по ip route. Например:

```
RouterA#config t
RouterA(config)#no ip route 172.16.10.0 255.255.255.0 172.16.11.2
RouterA(config)#no ip route 172.16.30.0 255.255.255.0 172.16.20.2
RouterA(config)#no ip route 172.16.40.0 255.255.255.0 172.16.20.2
RouterA(config)#no ip route 172.16.50.0 255.255.255.0 172.16.20.2
RouterA(config)#no ip route 172.16.55.0 255.255.255.0 172.16.20.2
```

Те же самые операции нужно выполнить в маршрутизаторах В, С и 2621. Введите **sh run** и нажмите Enter в каждом маршрутизаторе, чтобы проверить очистку все статических путей и путей по умолчанию.

2. После отмены статической маршрутизации и маршрутизации по умолчанию перейдите в устройстве А в режим настройки, введя **config t**.
3. Укажите маршрутизатору на использование протокола RIP, введя **router rip** и нажав Enter:

```
config t
router rip
```

4. Добавьте номер сети, где будут проводиться уведомления о маршрутизации, введя **network 172.16.0.0** и нажав Enter.
5. Нажмите **Ctrl+Z** для выхода из режима конфигурации (настройки).
6. В маршрутизаторах В, С и 2621 введите аналогичные команды:

```
Config t
Router rip
Network 172.16.0.0
```

7. Проверьте работу RIP в каждом маршрутизаторе, введя в каждом из них следующую последовательность команд:

```
show ip protocol
show ip route
show running-config or show run
```

8. Сохраните конфигурацию. В каждом маршрутизаторе введите **copy run start** или **copy running-config startup-config** и нажмите Enter.

9. Проверьте работу сети, протестировав по Ping все удаленные сети и хосты.

## О Лабораторная работа 5.3.

### *Динамическая маршрутизация по протоколу IGRP*

В этой лабораторной работе мы запустим протокол маршрутизации IGRP одновременно с маршрутизацией по протоколу RIP.

1. Войдите в систему маршрутизатора, перейдите в привилегированный режим и введите **en** или **enable**.
2. Сохраните во всех маршрутизаторах протокол RIP и проверьте работу этого протокола в каждом устройстве. Если нужно удалить RIP, то *следует* ввести команду режима глобального конфигурирования по `router rip`, например:

```
config t
no router rip
```

3. В режиме настройки маршрутизатора А введите **router igrp ?**.
4. Появится приглашение для ввода номера автономной системы. Номер AS служит для указания набора взаимодействующих маршрутизаторов. Введите 10 и нажмите Enter. Маршрутизатор можно настроить на участие в нескольких автономных системах AS.
5. В приглашении настройки маршрутизатора (`config-router`) введите **network 172.16.0.0**. Это установит полноклассовые сетевые границы для рассылки обновлений вместо использования номеров подсетей.
6. Нажмите **Ctrl+Z** для выхода из режима настройки.
7. В маршрутизаторах В, С и 2621 введите такие команды:

```
RouterB(config)#router igrp 10
RouterB(config-router)#network 172.16.0.0
```

8. Проверьте работу IGRP, введя в каждом маршрутизаторе:

```
show ip protocol
```

Будут показаны сведения о протоколах маршрутизации RIP и IGRP, а также значения таймеров обновления.

```
ship route
```

Это позволит "видеть" в сети все восемь подсетей: 10, 11, 15, 20, 30, 40, 50 и 55. Некоторые из них подключены непосредственно, но к другим сетям ведут пути, помеченные символом I, т.е. добавленные протоколом IGRP. Продолжает работать протокол RIP, но в таблице маршрутизации записи для сетей имеют сетевой номер (100/23456). Первое число (100) определяет степень достоверности. Поскольку для RIP по умолчанию степень достоверности равна 120, пути от протокола IGRP будут использованы раньше, чем пути от протокола

RIP. Второе число показывает метрику (или вес) пути, что служит для выбора наилучшего пути в сети.

**show running-config**

Посмотрим, как сконфигурированы RIP и IGRP.

9. Для сохранения конфигурации введите `copy running-config startup-config` или `copy run start` и нажмите Enter в каждом маршрутизаторе.
10. Проверьте сеть, обратившись утилитой Ping ко всем маршрутизаторам, переключателям и хостам.

## Проверочные вопросы

1. Какой алгоритм маршрутизации используется в протоколе RIP?
  - A. Маршрутизируемой информации
  - B. Связывания
  - C. Состояния связи
  - D. Вектора расстояния
2. Какой алгоритм маршрутизации используется в протоколе IGRP?
  - A. Маршрутизируемой информации
  - B. Связывания
  - C. Состояния связи
  - D. Вектора расстояния
3. Какая команда вводится в приглашении маршрутизатора для проверки частоты широковещательных рассылок по протоколу IGRP?
  - A. `sh ip route`
  - B. `sh ip protocol`
  - C. `sh ip broadcast`
  - D. `debug ip igrp`
4. Какая метрика маршрутизации используется в протоколе RIP?
  - A. Счет до бесконечности
  - B. Счетчик участков
  - C. Время жизни TTL
  - D. Полоса пропускания, задержка
5. Какая команда остановит вывод в интерфейс обновлений маршрутизации?
  - A. `Router(config-if)#no routing`
  - B. `Router(config-if)#passive-interface`
  - C. `Router(config-router)#passive-interfacesO`
  - D. `Router(config-router)#no routing updates`

6. Какая метрика маршрутизации используется по умолчанию в протоколе IGRP? (Укажите все правильные ответы.)
- A. Счет до бесконечности
  - B. Счетчик участков
  - C. Время жизни TTL
  - D. Полоса пропускания
  - E. Задержка
7. Что определяет метрика в 16 участков для сетей с маршрутизацией по протоколу RIP?
- A. 16 мс
  - B. Количество маршрутизаторов в объединенной сети
  - C. Количество участков
  - D. 16-ый участок недостижим
  - E. Последний доступный участок
8. Для чего используется удержание?
- A. Для удержания в протоколе от перехода на следующий участок
  - B. Для предотвращения восстановления отказавших путей при получении периодических обновлений
  - C. Для предотвращения восстановления только что заработавших участков при получении периодических обновлений
  - D. Для предотвращения восстановления отказавших путей при получении нерегулярных обновлений
9. Что такое деление горизонта?
- A. Маршрутизатор отмечает интерфейс получения пакета и не выполняет в нем распространение обновлений маршрутизации.
  - B. Большая шина (горизонт) физической сети делится трафиком.
  - C. Предотвращение широковещательных рассылок периодических обновлений в отказавших связях.
  - D. Предотвращение периодических обновлений при восстановлении отказавших путей.
10. Что такое опасный реверс?
- A. Возвращение сообщения протокола, полученного маршрутизатором для стабилизации состояния, что останавливает регулярные обновления
  - B. Информация, полученная от маршрутизатора, которая не может быть ему возвращена
  - C. Предотвращение периодических обновлений при восстановлении отказавших путей
  - D. Определяет, когда маршрутизатор устанавливает метрику для отказавшей линии, чтобы обеспечить счет до бесконечности

11. Каково административное расстояние по умолчанию в протоколе IGRP?
  - A. 90
  - B. 100
  - C. 120
  - D. 220
12. Что из перечисленного является корректным путем по умолчанию?
  - A. `route ip 172.0.0.0 255.0.0.0 s0`
  - B. `ip route 0.0.0.0 0.0.0.0 172.16.20.1`
  - C. `ip route 0.0.0.0 255.255.255.255 172.16.20.1`
  - D. `route ip 0.0.0.0 0.0.0.0 172.16.10.1150`
13. Что является протоколом состояния связи в сетях IP?
  - A. RIP V2
  - B. EIGRP
  - C. OSPF
  - D. IGRP
14. Какие команды доступны для поддержки сетей RIP? (Укажите все правильные ответы)
  - A. `sh ip route`
  - B. `sh ip rip`
  - C. `sh rip network`
  - D. `debug ip rip`
15. Что справедливо для сетей с протоколом по вектору расстояния? (Выберите наилучший ответ.)
  - A. Передача частичных обновлений каждые 60 с.
  - B. Передача полной таблицы маршрутизации каждые 60 с.
  - C. Отправка полной таблицы маршрутизации каждые 30 с.
  - D. Обновления каждые 90 с.
16. Какая команда Cisco IOS позволяет вывести таблицу маршрутизации IP?
  - A. `sh ip config`
  - B. `sh ip arp`
  - C. `sh ip route`
  - D. `sh ip table`
17. Как используется административное расстояние в маршрутизации?
  - A. Определяется сетевым администратором при вводе пути
  - B. Создает базу данных
  - C. Определяет достоверность источника и выражается целым числом в диапазоне от 0 до 255

- D. Определяет достоверность источника и выражается целым числом в диапазоне от 0 до 1023
18. Что означает символ S в листинге таблицы маршрутизации?
- A. Динамическое подключение
  - B. Непосредственное подключение
  - C. Статическое подключение
  - D. Пересылку пакетов
19. Что справедливо для IP-маршрутизации?
- A. IP-адрес назначения изменяется на каждом участке.
  - B. IP-адрес источника изменяется на каждом участке.
  - C. Кадры не изменяются на любом участке.
  - D. Кадры изменяются на каждом участке.
20. Что справедливо для создания статических путей? (Укажите все правильные ответы)
- A. Параметр маски необязателен.
  - B. Необходим параметр шлюза.
  - C. Необходимо административное расстояние.
  - D. Административное расстояние необязательно.
  - E. Ни одно из вышеперечисленного не является справедливым.

## Ответы к упражнению

---

1. ip route 172.16.10.0 255.255.255.0 172.16.20.1 150
2. config t  
router rip  
network 10.0.0.0
3. config t  
router rip  
passive-interface serial 1
4. config t  
router igrp 10  
network 172.16.0.0
5. config t  
ip route 0.0.0.0 0.0.0.0 172.16.50.3
6. Таймер удержания
7. Опасный реверс
8. Деление горизонта
9. variance
10. debug ip rip

## Ответы к проверочным вопросам

- |         |          |
|---------|----------|
| 1. D    | 11. B    |
| 2. D    | 12. B    |
| 3. B    | 13. C    |
| 4. B    | 14. A, D |
| 5. C    | 15. C    |
| 6. D, E | 16. C    |
| 7. D    | 17. C    |
| 8. B    | 18. C    |
| 9. A    | 19. D    |
| 10. D   | 20. B, D |



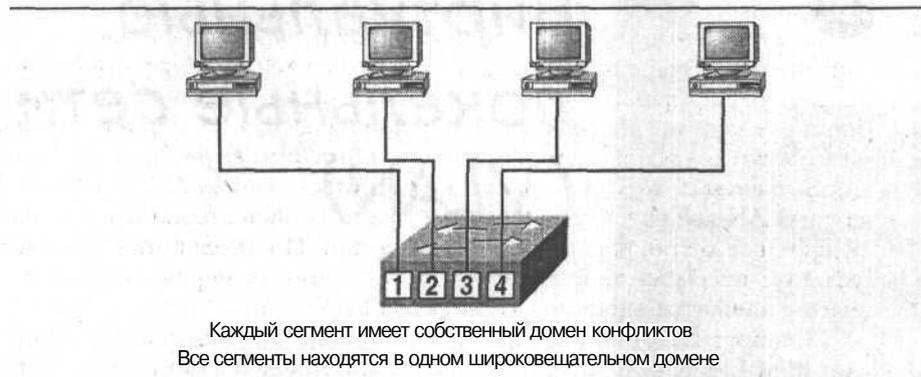
Глава

6

## Виртуальные локальные сети (VLAN)

## Виртуальные локальные сети (Virtual LAN)

В коммутируемых сетях уровня 2 сеть представляется "плоской" (см. рис. 6.1). Любой широковещательный пакет пересылается всем устройствам, вне зависимости от того, нужно ли устройству принимать эти данные.



**Рис. 6.1.** Плоская сетевая структура

Поскольку коммутация на уровне 2 формирует отдельные домены конфликтов для каждого подключенного к переключателю устройства, снижаются ограничения на длину сегмента Ethernet, т.е. можно строить более крупные сети. Увеличение количества пользователей и устройств приводит к увеличению количества широковещательных рассылок и пакетов, обрабатываемых каждым устройством.

Еще одной проблемой "плоской" коммутации уровня 2 является безопасность сети. Имейте в виду, что все пользователи "видят" все устройства. Нельзя отменить широковещательные рассылки в устройстве и ответы пользователей на эти рассылки. Увеличить уровень безопасности позволяет защита паролями серверов и других устройств.

Создание виртуальной локальной сети VLAN помогает решить многие проблемы коммутации уровня 2, что и будет показано ниже.

### Управление широковещательными рассылками

Широковещательные рассылки свойственны любому протоколу, но их частота зависит от особенностей протокола, исполняемых в объединенной сети приложений и методов использования сетевых служб.

Иногда приходится переписывать старые приложения, чтобы сократить количество широковещательных рассылок. Однако приложения нового поколения требовательны к полосе пропускания и занимают все ресурсы, которые обнаруживают. Мультимедийные приложения интенсивно пользуются широковещательными и многоадресными

рассылками. На степень интенсивности широковещательных рассылок приложения влияют сбои оборудования, неадекватная сегментация и плохо разработанные брандмауэры. Во время проектирования сети рекомендуется принимать специальные меры, поскольку широковещательные рассылки распространяются по коммутируемой сети. По умолчанию маршрутизаторы возвращают такие рассылки только в исходную сеть, но переключатели направляют широковещательные рассылки во все сегменты. Именно поэтому сеть называется "плоской", ведь формируется единый домен широковещательных рассылок.

Сетевой администратор обязан гарантировать правильность сегментации сети, чтобы проблемы отдельного сегмента не распространялись на всю сеть. Эффективнее всего сделать это с помощью коммутации и маршрутизации. Поскольку переключатель имеет лучшее отношение стоимости к эффективности, многие компании переходят от "плоских" сетей к сетям с полной коммутацией или к сетям VLAN. Все устройства сети VLAN являются членами одного широковещательного домена и получают все широковещательные рассылки. По умолчанию широковещательные рассылки фильтруются на всех портах переключателей, которые не являются членами одной сети VLAN.

Маршрутизаторы, переключатели уровня 3 и модули коммутации путей RSM (route switch module) надо использовать совместно с переключателями, чтобы предоставить соединения между сетями VLAN и предотвратить распространения по всей сети широковещательных рассылок.

## Безопасность

Еще одной проблемой плоских сетей является безопасность, что определяется соединением концентраторов и переключателей через маршрутизаторы. Защита сети обеспечивается маршрутизаторами. Однако любой человек, подключившийся к физической сети, получает доступ к ее ресурсам. Кроме того, пользователь может подключить сетевой анализатор к концентратору и наблюдать весь сетевой трафик. Дополнительная проблема связана с включением пользователя в рабочую группу — достаточно подключить сетевую станцию к концентратору.

Использование VLAN и создание нескольких групп широковещательных рассылок позволит администратору управлять каждым портом и пользователем. Пользователи уже не смогут самостоятельно подключать свои рабочие станции к произвольному порту переключателя и получать доступ к сетевым ресурсам. Администратор контролирует каждый порт и все предоставляемые пользователям ресурсы.

Группы формируются на основе требований пользователей к сетевым ресурсам, поэтому переключатель можно настроить на режим уведомления сетевой станции управления о любых попытках неавторизованного доступа к сетевым ресурсам. Если присутствуют коммуникации между сетями VLAN, можно реализовать ограничения на доступ через маршрутизаторы. Ограничения накладываются на аппаратные адреса, протоколы и приложения.

## Гибкость и масштабируемость

Переключатель уровня 2 не фильтрует, а только читает кадры, поскольку не анализирует сведения протокола сетевого уровня. Это приводит к перенаправлению переключателем всех широковещательных рассылок. Однако создание сети VLAN формирует домены широковещательных рассылок. Эти рассылки из узла одной сети VLAN не будут направлены в порты другой сети VLAN. За счет присваивания коммутируемых портов и пользователей определенной группе VLAN одного переключателя или группы связанных переключателей (такая группа называется *фабрикой коммутации* — *switch fabric*) мы увеличиваем гибкость при добавлении пользователя только в один домен широковещательной рассылки, причем вне зависимости от физического местоположения пользователя. Это предотвращает распространение во всей объединенной сети шторма широковещательных рассылок при неисправности сетевого адаптера (NIC, network interface card) или приложения.

Когда сеть VLAN становится очень большой, можно сформировать новые сети VLAN, не позволив широковещательным рассылкам занять слишком много полосы пропускания. Чем меньше пользователей в сети VLAN, тем на меньшее количество пользователей действуют широковещательные рассылки.

Для понимания того, как VLAN выглядит с точки зрения переключателя, полезно сначала рассмотреть обычные локализованные магистрали. На рис. 6.2 показана локализованная магистраль (*collapsed backbone*), созданная за счет подключения физических локальных сетей к маршрутизатору.

Каждая сеть подключена к маршрутизатору и имеет собственный логический номер сети. Каждый узел отдельной физической сети должен соблюдать этот сетевой номер для взаимодействия в полученной объединенной сети. Рассмотрим ту же схему на основе переключателя. Рис. 6.3 показывает, как переключатель устраняет физические границы взаимодействия в объединенной сети.

Переключатель обладает большей гибкостью и масштабируемостью, чем маршрутизатор. Можно группировать пользователей в сообщества по интересам, что называется организационной структурой сети VLAN.

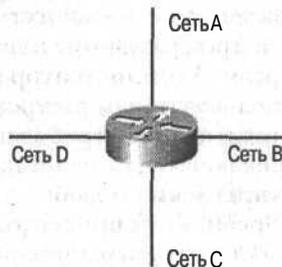


Рис. 6.1. Физические локальные сети, подключенные к маршрутизатору

Использование переключателя вроде бы отменяет необходимость в маршрутизаторе. Это не так. На рис. 6.3 видны четыре сети VLAN (домены широковещательных рассылок). Узлы в каждой сети VLAN могут взаимодействовать друг с другом, но не с другими сетями VLAN или с их узлами. Во время конфигурации VLAN узлы должны находиться в пределах локализованной магистрали (см. рис. 6.2). Что же нужно хосту на рис. 6.2 для обращения к узлу или хосту другой сети? Хосту необходимо обратиться через маршрутизатор или другое устройство уровня 3, как и при коммуникации внутри VLAN (см. рис. 6.3). Взаимодействие между сетями VLAN, как и между физическими сетями, должно проводиться через устройство уровня 3.

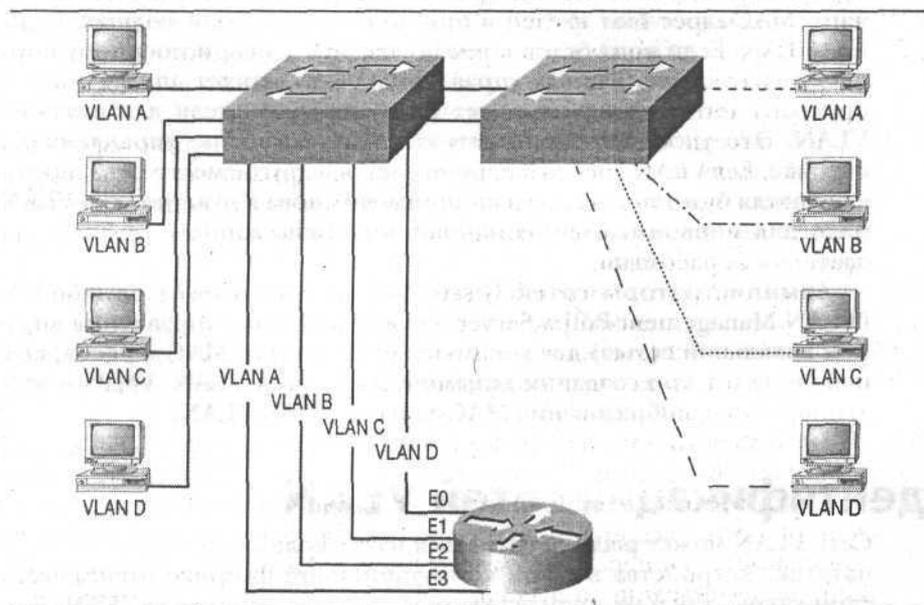


Рис. 6.3. Переключатель устраняет физические границы сетей

## Членство в сети VLAN

Сеть VLAN обычно создается администратором, который присваивает ей порты переключателя. Такой способ называется статической виртуальной локальной сетью (static VLAN). Если администратор немного постарается и присвоит через базу данных аппаратные адреса всех хостов, переключатель можно настроить на динамическое создание сети VLAN.

### Статические сети VLAN

*Статические сети VLAN* являются типичным способом формирования таких сетей и отличаются высокой безопасностью. Присвоенные сети VLAN порты переключателей всегда сохраняют свое действие, пока

администратор не выполнит новое присваивание портов. Этот тип VLAN легко конфигурировать и отслеживать, причем статические VLAN хорошо подходят для сетей, где контролируется перемещение пользователей. Программы сетевого управления помогут выполнить присваивание портов. Однако подобные программы использовать не обязательно.

## Динамические сети VLAN

*Динамические сети VLAN* автоматически отслеживают присваивание узлов. Использование интеллектуального программного обеспечения сетевого управления допускает формирование динамических VLAN на основе аппаратных адресов (MAC), протоколов и даже приложений. Предположим, MAC-адрес был введен в приложение централизованного управления VLAN. Если порт будет затем подключен к неприсвоенному порту переключателя, база данных управления VLAN найдет аппаратный адрес, присвоит его и сконфигурирует порт переключателя для нужной сети VLAN. Это упрощает административные задачи по управлению и настройке. Если пользователь перемещается в другое место сети, порт переключателя будет автоматически присвоен снова в нужную сеть VLAN. Однако для первоначального наполнения базы данных администратору придется поработать.

Администраторы сетей Cisco могут пользоваться службой VMPS (VLAN Management Policy Server, сервер политики управления виртуальной локальной сетью) для установки базы данных MAC-адресов, которая используется при создании динамических сетей VLAN. VMPS — это база данных для преобразования MAC-адресов в сети VLAN.

## Идентификация сетей VLAN

Сеть VLAN может распространяться на несколько соединенных переключателей. Устройства в такой коммутационной фабрике отслеживают как сами кадры, так и их принадлежность определенной сети VLAN. Для этого выполняется маркирование кадров (frame tagging). Переключатели смогут направлять кадры в соответствующие порты.

В такой среде коммутации существуют два разных типа связей:

**Связи доступа (Access link)** Связи, принадлежащие только одной сети VLAN и считающиеся основной связью отдельного порта переключателя. Любое устройство, подключенное к связи доступа, не подозревает о своем членстве в сети VLAN. Это устройство считает себя частью широковещательного домена, но не подозревает о реальном членстве в физической сети. Переключатели удаляют всю информацию о VLAN еще до передачи кадра в связь доступа. Устройства на связях доступа не могут взаимодействовать с устройствами вне своей сети VLAN, если только пакеты не проходят через маршрутизатор.

**Магистральные связи (Trunk link)** Магистральные линии способны обслуживать несколько сетей VLAN. Название этих линий заимствовано из

телефонных систем, где магистральные линии способны одновременно передавать несколько телефонных переговоров. В компьютерных сетях магистральные линии служат для связи переключателей с переключателями, маршрутизаторами и даже с серверами. В магистральных связях поддерживаются только протоколы Fast Ethernet или Gigabit Ethernet. Для идентификации в кадре принадлежности к определенной сети VLAN, построенной на технологии Ethernet, переключатель Cisco поддерживает две разные схемы идентификации: ISL и 802.1q. Магистральные связи служат для транспорта VLAN между устройствами и могут настраиваться на поддержку всех или только нескольких сетей VLAN. Магистральные связи сохраняют принадлежность к "родной" VLAN (т.е. виртуальной локальной сети по умолчанию), которая используется при отказе магистральной линии.

## Маркировка кадров

Переключателю объединенной сети необходимо отслеживать пользователей и кадры, которые проходят через коммутационную фабрику и сеть VLAN. Коммутационной фабрикой называют группу переключателей, совместно использующих одинаковую информацию о сети VLAN. *Идентификация (маркировка) кадров* предполагает присваивание кадрам уникального идентификатора, определенного пользователем. Часто это называют присваиванием VLAN ID или присваиванием цвета.

Компания Cisco разработала метод маркировки кадров, используемый для передачи кадров Ethernet по магистральным связям. Маркер (тег) сети VLAN удаляется перед выходом кадра из магистральной связи. Любой получивший кадр переключатель обязан идентифицировать VLAN ID, чтобы определить дальнейшие действия с кадром на основе таблицы фильтрации. Если кадр попадает в переключатель, подключенный к другой магистральной связи, кадр направляется в порт этой магистральной линии. Когда кадр попадает в конец магистральной связи и должен поступить в связь доступа, переключатель удаляет идентификатор VLAN. Оконечное устройство получит кадр без какой-либо информации о сети VLAN.

## Методы идентификации VLAN

Для отслеживания кадров, перемещающихся через коммутационную фабрику, используется идентификатор VLAN. Он отмечает принадлежность кадров определенной сети VLAN. Существует несколько методов отслеживания кадров в магистральных связях:

**Протокол ISL** Протокол ISL (Inter-Switch Link — связи между переключателями) лицензирован для переключателей компании Cisco и используется только в линиях сетей FastEthernet и Gigabit Ethernet. Протокол может применяться к порту переключателя, интерфейсу маршрутизатора или интерфейсу сетевого адаптера на сервере, который является магистральным. Такой магистральный сервер пригоден для создания сетей VLAN,

не нарушающих правила "80/20". Магистральный сервер одновременно является членом всех сетей VLAN (доменов широковещательных рассылок). Пользователям не нужно пересекать устройство уровня 3 для доступа к серверу, совместно используемому в организации.

**IEEE 802.1q** Протокол создан институтом IEEE в качестве стандартного метода маркирования кадров. Протокол предполагает вставку в кадр дополнительного поля для идентификации VLAN. Для создания магистральной связи между коммутируемыми линиями Cisco и переключателем другого производителя придется использовать протокол 802.1q, который обеспечит работу магистральной связи.

**LANE** Протокол эмуляции локальной сети LANE (LAN emulation) служит для взаимодействия нескольких VLAN поверх ATM.

**802.10 (FDDI)** Позволяет пересылать информацию VLAN поверх FDDI. Использует поле SAID в заголовке кадра для идентификации VLAN. Протокол лицензирован для устройств Cisco.

▼ **ВНИМАНИЕ** | Для сдачи экзамена CCNA достаточно знать только метод ISL.

## Протокол ISL

Протокол ISL (Inter-Switch Link) является способом явного маркирования информации о VLAN в кадрах Ethernet. Маркировка позволяет мультиплексировать VLAN в магистральных линиях с помощью внешнего метода инкапсуляции. За счет ISL можно обеспечить межсоединения нескольких переключателей при сохранении информации о VLAN, причем при перемещении трафика как через переключатель, так и по магистральной связи. Протокол ISL характеризуется небольшой задержкой и высокой производительностью на уровне линий связи для FastEthernet в полу- и полнодуплексном режиме.

Протокол ISL разработан компанией Cisco, поэтому ISL считают лицензионным только для устройств Cisco. Если необходим нелицензионный протокол для VLAN, используйте 802.1q (см. в книге *CCNP: Switching Study Guide*).

ISL является внешним процессом маркирования, т.е. исходный кадр никак не изменяется, но дополняется новым 26-байтным заголовком ISL. Кроме того, в конец кадра вставляется второе 4-байтное поле проверочной последовательности кадра FCS (frame check sequence). Поскольку кадр инкапсулируется, прочитав его смогут только устройства, поддерживающие протокол ISL. Кадры не должны превышать 1522 байтов. Получившее кадр ISL устройство может посчитать этот кадр слишком большим, учитывая, что в Ethernet максимальная длина сегмента равна 1518 байт.

В портах нескольких VLAN (магистральные порты) каждый кадр маркируется при поступлении в переключатель. Сетевой адаптер (NIC, network interface card), поддерживающий протокол ISL, позволяет серверу получать и отправлять маркированные кадры для нескольких сетей

VLAN. Причем кадры могут проходить по нескольким VLAN без пересечения маршрутизатора, что снижает задержку. Такая технология может использоваться в сетевых зондах и анализаторах. Пользователь сможет подключиться к серверу, не пересекая маршрутизатор при каждом обращении к любому информационному ресурсу. Например, сетевой администратор может пользоваться технологией ISL для одновременного включения файлового сервера в несколько сетей VLAN.

Важно понять, что информация протокола ISL о VLAN добавляется в кадр только при перенаправлении в порт, настроенный на режим магистральной связи. Инкапсуляция ISL удаляется из кадра, как только он попадает в связь доступа.

## Магистральные связи

Магистральные линии являются соединениями "точка-точка" на скорости 100- или 1000 Мбит/с между двумя переключателями, между переключателем и маршрутизатором или между переключателем и сервером. Магистральные связи способны доставлять трафик в несколько сетей VLAN (одновременно поддерживается от 1 до 1005 сетей). Не допускается работа магистральных связей в линиях 10 Мбит /с.

Магистральная связь позволяет одновременно сделать порт членом нескольких сетей VLAN, чтобы, например, магистральный сервер смог одновременно находиться в двух широковещательных доменах. Пользователи смогут не пересекать устройство уровня 3 (маршрутизатор) при входе и использовании сервера. Кроме того, при соединении переключателей магистральная связь позволит переносить по линии отдельную или всю информацию VLAN. Если не сформировать магистральную связь между переключателями, то по умолчанию эти устройства смогут передавать по связи только информацию одной сети VLAN. Все сети VLAN конфигурируются с магистральными связями, если только они не создаются администратором вручную.

Переключатели Cisco используют протокол DTP (Dynamic Trunking Protocol, протокол динамических магистральных взаимодействий) для управления отказом от магистрального режима в программном двигателе переключателя Catalyst версии 4.2 или выше и использования протокола ISL или 802.1q. DTP — это протокол "точка-точка", который создан для передачи информации о магистральных связях по магистральным линиям 802.1q.

## Маршрутизация между сетями VLAN

Хосты в сети VLAN находятся в собственном широковещательном домене и свободно взаимодействуют друг с другом. Сеть VLAN формирует сетевые области и разделение трафика на уровне 2 по спецификации OSI. Для взаимодействия хостов или любых других устройств из разных сетей VLAN абсолютно необходимы устройства уровня 3.

Можно использовать маршрутизатор, имеющий интерфейсы в каждой сети VLAN, либо маршрутизатор с поддержкой маршрутизации по протоколу ISL. Самыми дешевыми маршрутизаторами с поддержкой ISL являются устройства серии 2600. В сериях 1600, 1700 и 2500 маршрутизация ISL не поддерживается.

Если присутствует небольшое число VLAN (две или три виртуальные сети), возьмите маршрутизатор с двумя или тремя подключениями по ЮBaseT или FastEthernet. Подойдет и ЮBaseT, но наилучшим выбором будет FastEthernet.

Однако если сетей VLAN больше, чем интерфейсов у маршрутизатора, придется применить маршрутизацию ISL на одном из портов FastEthernet или приобрести модуль коммутации путей RSM (route switch module) для переключателя серии 5000. Модуль RSM способен поддержать до 1005 сетей VLAN, причем действует непосредственно через объединяющую плату переключателя. Режим с одним интерфейсом FastEthernet и маршрутизацией по протоколу ISL компания Cisco называет каскадом маршрутизаторов (router-on-a-stick — дословно: "маршрутизатор на палочке").

## Протокол VTP

Cisco разработала *протокол VTP* (VLAN Trunk Protocol — протокол магистральных связей виртуальных локальных сетей) для управления конфигурацией VLAN в пределах объединенной коммутируемой сети и поддержки согласованности по всей этой сети. VTP позволяет администратору добавлять, удалять и переименовывать VLAN, причем управление распространяется на все переключатели сети.

Протокол VTP обеспечивает следующие преимущества для коммутируемой сети:

- Согласованность конфигураций VLAN во всех переключателях
- Магистральные связи VLAN поверх смешанных сетей, например Ethernet поверх ATM LANE или FDDI
- Точное отслеживание и мониторинг VLAN
- Динамические отчеты о добавлении VLAN во всех переключателях
- Добавление VLAN методом Plug-and-Play (подключи и работай)

Чтобы протокол VTP смог управлять VLAN во всей сети, нужно предварительно создать сервер VTP. Все серверы, совместно использующие информацию о сетях VLAN, обязаны иметь одинаковое доменное имя, а переключатель может одновременно быть членом только одного домена. Следовательно, переключатель способен использовать общий домен VTP только с переключателями, настроенными на тот же самый домен VTP.

Домен VTP необходим, когда к сети подключено несколько переключателей. Если все переключатели сети принадлежат только одной VLAN, протокол VTP не нужен. Информация по протоколу VTP пересылается между переключателями по магистральным портам.

Переключатели уведомляют в специальных параметрах об управляющей информации в домене VTP, а также о номере версии конфигурации и всех известных им сетях VLAN. Можно настроить переключатель на передачу информации VTP через магистральный порт. При этом надо запретить прием информации об обновлениях или об изменении собственной базы данных VTP. Такой режим называется "прозрачным" (VTP transparent mode).

Для управления добавлением переключателей в домен VTP можно установить пароль, но такой пароль должен быть одинаков во всех переключателях, что не очень удобно.

Переключатели обнаруживают дополнительные сети VLAN через уведомления VTP, после чего подготавливаются для приема информации на своих транковых портах, в которой специфицируется вновь введенная сеть VLAN. Такая информация может находиться в полях VLAN ID, 802.10 SAID или поле информации LANE. Обновления отсылаются согласно номерам версий, которые равны номеру уведомления плюс единица. Как только переключатель обнаруживает больший номер версии, становится ясно, что получена более свежая информация, которую необходимо внести в базу данных.

## Режимы VTP

Существуют три режима операций в домене VTP (см. рис. 6.4).

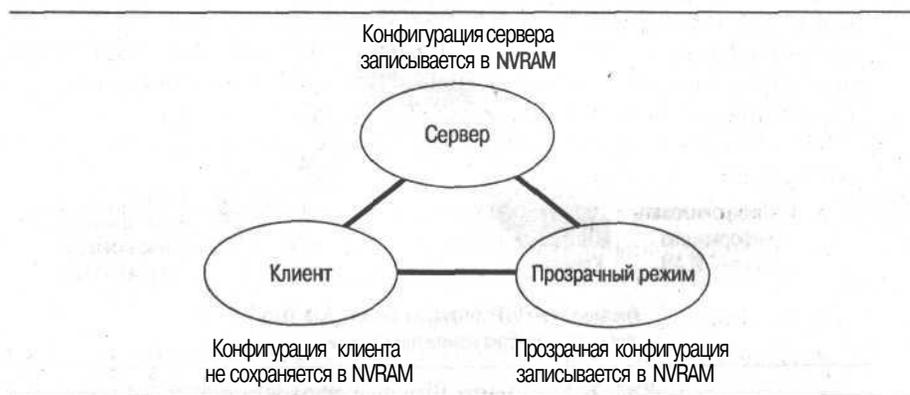


Рис. 6.4. Режимы VTP

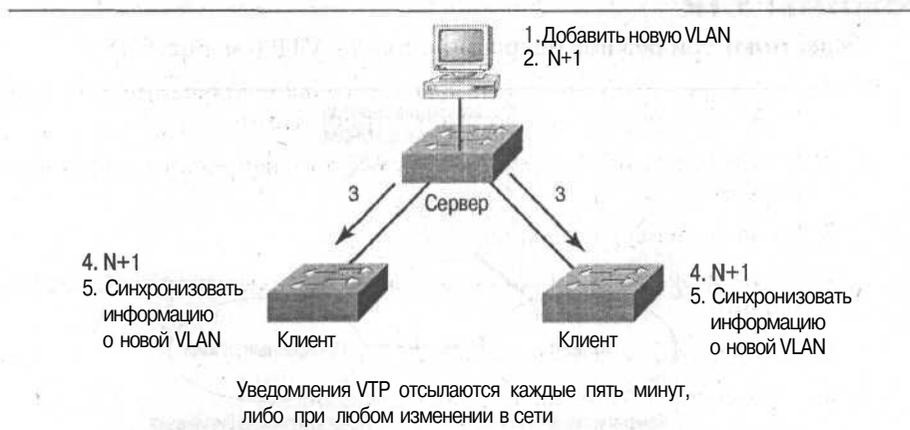
**Сервер (Server)** Этот режим установлен по умолчанию во всех переключателях Catalyst. В домене VTP необходим хотя бы один сервер для распространения по домену информации о VLAN. Переключатель обязан находиться в серверном режиме для создания, добавления или удаления сетей VLAN в домене VTP. Изменение информации VTP тоже должно производиться в режиме сервера. Любые изменения, сделанные в серверном переключателе, рассылаются по всему домену VTP.

**Клиент (Client)** Принимает информацию от серверов VTP, а также принимает и отправляет обновления, хотя не способен проводить изменений. Порты клиентского переключателя не могут быть присвоены новой сети VLAN, пока сервер VTP не уведомит клиентский переключатель о новой сети VLAN. Чтобы сделать переключатель сервером, необходимо сначала включить на нем клиентский режим для получения всей информации VLAN, а затем перейти в серверный режим.

**Прозрачный режим (Transparent)** Устройство не участвует в домене VTP, но пересылает уведомления VTP по подключенным к нему магистральным связям. Прозрачный режим VTP в переключателе позволяет добавлять и удалять VLAN согласно собственной базе данных устройства, но этот режим запрещает совместное использование информации с другими переключателями. Прозрачный режим имеет смысл только для локального использования.

## Номер версии конфигурации

Номер версии (revision number) — это наиболее важная часть в уведомлениях VTP. На рис. 6.5 показан пример использования номера версии в уведомлениях.



**Рис. 6.5.** Номер версии в протоколе VTP

На рисунке номер версии конфигурации показан как "N." При изменении в базе данных сервер VTP увеличивает на единицу номер версии. Затем сервер VTP уведомляет всех о базе данных с новым номером версии. Когда уведомление попадает к переключателю и имеет больший номер версии, то база данных в NVRAM перезаписывается информацией из уведомления.

## Сокращение действия VTP

Можно сократить требования к полосе пропускания, если настроить протокол VTP на снижение объема ширококвещательных, многоадресных и одноадресных пакетов, которым требуется сетевая полоса пропускания. Этот процесс называется сокращением действия (pruning). Сокращение действия VTP предписывает отправку ширококвещательных рассылок только по магистральным связям, которым необходима такая информация. Когда в магистральной линии ширококвещательная информация не требуется, то рассылка не отправляется. Например, если переключатель не имеет портов, настроенных для сети VLAN 5, а ширококвещательная рассылка отправлена именно по сети VLAN 5, то такая рассылка не попадет в магистральную связь к нашему переключателю. Сокращение действия VTP отменено по умолчанию во всех переключателях.

Если разрешить сокращение действия VTP на сервере, то этот режим распространяется на весь домен. По умолчанию сети VLAN 2 — 1005 допускают режим сокращения действия. VLAN 1 никогда не работает в этом режиме, поскольку является административной сетью VLAN.

## Упражнение

---

Ответьте на следующие вопросы.

1. Какой режим VTP предписывает только получение информации VLAN без обмена его с другими устройствами?
2. Какой метод идентификации VLAN лицензирован в маршрутизаторах Cisco?
3. Какие домены разделяет VLAN?
4. Какие домены могут по умолчанию быть разделенными переключателями?
5. Каков режим VTP по умолчанию?
6. Что обеспечивают магистральные связи?
7. Что такое маркирование кадров?
8. Справедливо ли утверждение: Инкапсуляция ISL удаляется из кадра, как только кадр попадает в связь доступа?
9. Связи какого типа могут быть частью только одной сети VLAN и считаются "естественными" для портов VLAN?
10. Какой тип информации маркирования Cisco поддерживает мультиплексирование VLAN по магистральным связям с помощью внешнего метода инкапсуляции?

## Проверочные вопросы

1. Что справедливо для сетей VLAN ? (Укажите все правильные ответы.)
  - A. Необходимо определить не менее двух VLAN в любой коммутируемой сети Cisco.
  - B. Все VLAN конфигурируются на самые быстрые переключатели и по умолчанию распространяют эту информацию по всем остальным переключателям.
  - C. Нельзя иметь более 10 переключателей в одном домене VTP.
  - D. Протокол VTP служит для передачи информации VLAN в переключатели, объединенные в домен VTP.
2. Какими двумя способами администратор может установить членство в сети VLAN?
  - A. Через сервер DHCP
  - B. Статически
  - C. Динамически
  - D. Через базу данных VTP
3. Какой размер допустим для кадров ISL?
  - A. 1518
  - B. 1522
  - C. 4202
  - D. 8190
4. Как настраиваются динамические сети VLAN ?
  - A. Статически
  - B. Администратором
  - C. Через сервер DHCP
  - D. Через службу Management Policy Server сети VLAN
5. Какие протоколы используются для настройки магистральных связей в переключателе? (Укажите все правильные ответы.)
  - A. Virtual Trunk Protocol
  - B. VLAN
  - C. Trunk
  - D. ISL
6. Что справедливо для VTP? (Укажите все правильные ответы.)
  - A. Сокращение действия VTP разрешено по умолчанию во всех переключателях.
  - B. Сокращение действия VTP запрещено по умолчанию во всех переключателях.

- C.** Сокращение действия VTP поддерживается только в переключателях серии 5000 и выше.
  - D.** Сокращение действия VTP конфигурируется по умолчанию во всех переключателях, если этот режим включен хотя бы на одном серверном переключателе VTP.
7. Что является стандартом Cisco для инкапсуляции кадров и добавления нового поля FCS?
- A.** ISL
  - B.** 802.lq
  - C.** 802.3z
  - D.** 802.3u
8. К чему приводит установка прозрачного режима VTP?
- A.** Прозрачный режим предписывает передачу только сообщений и уведомлений, но не добавление их в базу данных.
  - B.** Прозрачный режим предписывает перенаправление сообщений и уведомлений, а также добавление их в собственную базу данных устройства.
  - C.** Прозрачный режим запрещает передачу сообщений и уведомлений.
  - D.** Прозрачный режим устанавливает динамическую защиту в переключателе.
9. Какие преимущества дает использование VTP в коммутируемых сетях? (Укажите все правильные ответы.)
- A.** Несколько широковещательных доменов в сети VLAN 1
  - B.** Управление всеми переключателями и маршрутизаторами объединенной сети
  - C.** Согласование конфигурации VLAN во всех переключателях сети
  - D.** Разрешает мультиплексирование VLAN в магистральных связях смешанных сетей, подобных Ethernet поверх ATM LANE или FDDI
  - E.** Точное отслеживание и мониторинг VLAN
  - F.** Динамические отчеты о добавлении VLAN во всех переключателях
  - G.** Добавление VLAN в режиме Plug-and-Play
  - H.** Настройка режима Plug-and-Play
10. Что справедливо для протокола VTP?
- A.** Все переключатели по умолчанию являются серверами VTP.
  - B.** Все переключатели по умолчанию работают в прозрачном режиме VTP.
  - C.** Протокол VTP включен во всех переключателях Cisco с именем домена по умолчанию Cisco.
  - D.** Все переключатели по умолчанию являются клиентами VTP.

- 11.** Что справедливо для магистральных связей?
- A.** Сконфигурированы по умолчанию во всех портах переключателя.
  - B.** Действуют только в сетях Ethernet, но не в Token Ring, FDDI или ATM.
  - C.** Могут устанавливаться только в любых портах со скоростями 10-, 100- или 1000 Мбит/с.
  - D.** Необходимо вручную удалить все ненужные VLAN.
- 12.** Когда переключатель обновляет свою базу данных VTP?
- A.** Каждые 60 с.
  - B.** Когда переключатель получает уведомление с большим номером версии, переключатель перезаписывает базу данных в памяти NVRAM новой информацией из уведомления.
  - C.** Когда переключатель рассылает широковещательное уведомление с меньшим номером версии, переключатель перезаписывает базу данных в памяти NVRAM новой информацией из уведомления.
  - D.** Когда переключатель получает уведомление с тем же номером версии, переключатель перезаписывает базу данных в памяти NVRAM новой информацией из уведомления.
- 13.** Что является стандартом IEEE для маркирования кадров?
- A.** ISL
  - B.** 802.32
  - C.** 802.1q
  - D.** 802.3u
- 14.** Что характерно для магистральных связей?
- A.** Способны мультиплексировать несколько сетей VLAN.
  - B.** Переключатели удаляют любую информацию о VLAN из кадра, перед его отправкой по связи доступа к устройству.
  - C.** Устройство на связи доступа не может взаимодействовать с устройством вне сети VLAN, если только пакеты не перенаправляются через маршрутизатор.
  - D.** Служат для транспорта VLAN между устройствами и могут конфигурироваться на транспорт всех или отдельных сетей VLAN.
- 15.** Что характерно для связей доступа?
- A.** Способны мультиплексировать несколько сетей VLAN.
  - B.** Переключатели удаляют любую информацию о VLAN из кадра, перед его отправкой по связи доступа к устройству.
  - C.** Устройство на связи доступа не может взаимодействовать с устройством вне сети VLAN, если только пакеты не перенаправляются через маршрутизатор.
  - D.** Служат для транспорта VLAN между устройствами и могут конфигурироваться на транспорт всех или отдельных сетей VLAN.

16. Как определяются связи доступа?
- A. Способны мультиплексировать несколько сетей VLAN
  - B. Служат для транспорта VLAN между устройствами и могут конфигурироваться на транспорт всех или отдельных сетей VLAN
  - C. Могут использоваться только в сетях FastEthernet и Gigabit Ethernet
  - D. Могут быть частью только одной VLAN и считаются "родными" для порта VLAN
17. Как называется метод IEEE для маркировки кадров?
- A. ISL
  - B. LANE
  - C. Поле SAID
  - D. 802.1q
18. В каком режиме VTP не предполагается участие в домене VTP, но сохраняется возможность пересылки уведомлений VTP по сконфигурированным магистральным связям?
- A. ISL
  - B. Клиентский
  - C. Прозрачный
  - D. Серверный
19. Каков размер заголовка ISL?
- A. 2 байта
  - B. 6 байт
  - C. 26 байт
  - D. 1522 байта
20. Когда используется маркировка кадров?
- A. Когда информация VLAN передается по связям доступа
  - B. Когда информация VLAN передается по магистральным связям
  - C. Когда в связи доступа используется протокол ISL
  - D. Когда в связи доступа применяется протокол 802.1q

## Ответы к упражнению

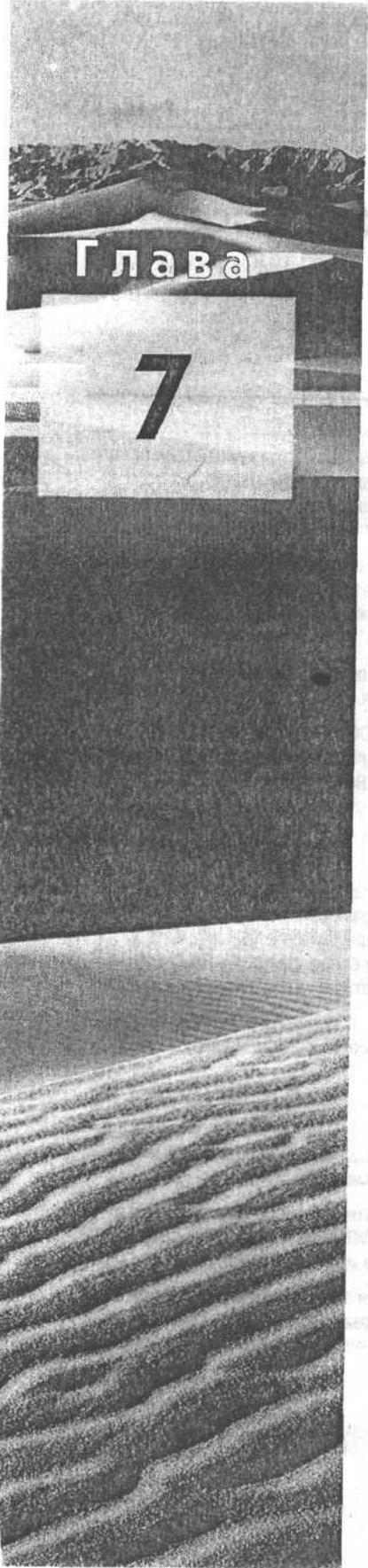
---

1. Клиентский режим
2. ISL
3. Широковещательный домен
4. Домен конфликтов
5. Серверный режим

6. Магистральная связь позволяет одному порту одновременно стать частью нескольких сетей VLAN.
7. Идентификация (маркирование) кадров состоит в присвоении каждому кадру уникального и определенного пользователем идентификатора. Часто называется VLAN ID или цветом кадра.
8. Да
9. Связь доступа
10. ISL

## Ответы на проверочные вопросы

- |                     |          |
|---------------------|----------|
| 1. D                | 11. D    |
| 2. B, C             | 12. B    |
| 3. B                | 13. C    |
| 4. D                | 14. A, D |
| 5. C, D             | 15. B, C |
| 6. B, D             | 16. D    |
| 7. A                | 17. D    |
| 8. A                | 18. C    |
| 9. B, C, D, E, F, G | 19. C    |
| 10. A               | 20. B    |



Глава

7

# Управление объединенными сетями Cisco

## Компоненты маршрутизаторов Cisco

Для настройки и диагностики объединенных сетей Cisco необходимо знать основные компоненты маршрутизаторов Cisco и их назначение (см. таблицу 7.1).

**Таблица 7.1.**

**Компоненты маршрутизатора Cisco**

Компонент	Описание
Bootstrap (начальная загрузка)	Образ начальной загрузки хранится в микрокоде памяти ROM и используется для установки маршрутизатора во время его инициализации. Выполняется запуск самого маршрутизатора и загрузка операционной системы IOS.
POST (power-on self test - самотестирование по включению питания)	Тест POST хранится в микрокоде памяти ROM и используется для проверки базовых функций оборудования маршрутизатора, а также выявления присутствующих интерфейсов.
ROM monitor (монитор памяти "только чтение")	Хранится в микрокоде памяти ROM и применяется для проверки тестирования и диагностики производителем.
Mini-IOS (мини-ОС)	Другое название: RXBOOT или загрузчик (bootloader) компании Cisco. Это небольшой образ операционной системы IOS в памяти ROM, используемый для установки интерфейсов и загрузки Cisco IOS во флэш-память. Операционная система mini-IOS способна выполнять несколько операций по обслуживанию устройства.
RAM (random access memory — память с произвольным доступом)	Служит для хранения пакетов в буфере, таблиц маршрутизации, а также программного обеспечения и структур данных, обеспечивающих функции маршрутизатора. Конфигурация Running-config хранится в RAM, а IOS в некоторых маршрутизаторах может также запускаться из RAM.
ROM (read-only memory — память "только чтение")	Служит для запуска и обслуживания маршрутизатора.
Flash memory (флэш-память)	Используется маршрутизатором для хранения Cisco IOS. Флэш-память не стирается при перезагрузке маршрутизатора. В качестве флэш-памяти используется микросхема EEPROM компании Intel.
NVRAM (nonvolatile RAM, энергонезависимая память с произвольным доступом)	Служит для хранения конфигурации маршрутизатора или переключателя. NVRAM не стирается при перезагрузке маршрутизатора или переключателя.
Configuration register (конфигурационные регистры)	Служат для управления загрузкой маршрутизатора. Данные в этих регистрах можно вывести командой show version. Обычно это значение равно 0x2102, что указывает маршрутизатору на загрузку IOS из флэш-памяти.

## Последовательность загрузки маршрутизатора

Во время загрузки маршрутизатора последовательно выполняется несколько операций по тестированию оборудования и загрузке необходимого программного обеспечения:

1. Маршрутизатор выполняет тест POST, который проверяет, что присутствуют и работают все аппаратные компоненты устройства. Например, тест POST проверяет разные интерфейсы маршрутизатора. Тест POST хранится и запускается из памяти ROM.
2. Загрузчик ищет и загружает программное обеспечение Cisco IOS. Загрузчик — это программа из ROM, используемая для выполнения других программ. Загрузчик отвечает за поиск местоположения всех программ IOS и загрузку соответствующих файлов. По умолчанию программное обеспечение IOS загружается из флэш-памяти во всех маршрутизаторах Cisco.
3. Программное обеспечение IOS ищет корректный конфигурационный файл в NVRAM. Он называется `startup-config` и представляет собой файл, скопированный администратором в память NVRAM.
4. Если файл `startup-config` найден в NVRAM, маршрутизатор загружает и запускает его файл. После этого маршрутизатор начинает работать. Если же файла `startup-config` нет в NVRAM, маршрутизатор после загрузки переходит в режим установки конфигурации (`setup mode configuration`).

## Управление конфигурационными регистрами

Все маршрутизаторы Cisco имеют 16-разрядный программный регистр. Его содержимое хранится в NVRAM. По умолчанию конфигурационный регистр определяет загрузку Cisco IOS из флэш-памяти и поиск файла `startup-config` в NVRAM.

### Разряды конфигурационного регистра

Шестнадцать разрядов конфигурационного регистра помечены как 15-0, слева направо. По умолчанию в конфигурационном регистре маршрутизатора Cisco записано значение 0x2102. Это означает включение разрядов 13, 8 и 1 (см. таблицу 7.2). Заметим, что все наборы из четырех разрядов помечены значениями 1, 2, 4 и 8 справа налево.

#### ▼ ВНИМАНИЕ

В адресе конфигурационного регистра присутствует 0x, что означает шестнадцатеричное представление значений.

**Таблица 7.2.**  
**Нумерация разрядов конфигурационного регистра**

Конфигурационный регистр	2	1	0	2
Номер разряда	15 14 13 12	11 10 9 8	7 6 5 4	3 2 1 0
Двоичный вид	0 0 1 0	0 0 0 1	0 0 0 0	0 0 1 0

В таблице 7.3 представлено соответствие между разрядами регистра и конфигурацией программного обеспечения. Разряд 6 предписывает игнорирование содержимого NVRAM. Он служит для восстановления пароля (см. ниже).

**Таблица 7.3.**  
**Соответствие программной конфигурации**

Разряд	Шестнадцатеричное значение	Описание
0-3	0x0000 — 0x000F	Поля загрузки (см. таблицу 7.4).
6	0x0040	Игнорировать содержимое NVRAM.
7	0x0080	Разрешить разряд OEM.
8	0x0100	Запретить останов.
10	0x0400	IP-адрес широковещательной рассылки со всеми нулями.
11-12	0x0800 — 0x1000	Скорость консольной линии.
13	0x2000	Загрузить программное обеспечение по умолчанию из ROM, если будет неудачной загрузка по сети.
14	0x4000	IP-адрес широковещательной рассылки не использует номера сетей.
15	0x8000	Разрешить диагностические сообщения и игнорировать содержимое NVM.

Поле загрузки (разряды 0 — 3) конфигурационного регистра управляет загрузочной последовательностью маршрутизатора. В таблице 7.4 показан смысл разрядов поля загрузки.

**▼ ВНИМАНИЕ**

В шестнадцатеричной записи используются цифры 0 — 9 и буквы A — F (A=10, B=11, C=12, D=13, E=14 и F=15). Т.е. значение 210F в конфигурационном регистре реально соответствует 210(15) или 1111 в двоичном виде.

**Таблица 7.4.**  
**Поле загрузки (Разряды 00 — 03 конфигурационного регистра)**

Поле загрузки	Смысл	Использование
00	Режим монитора ROM	Для загрузки в режиме монитора ROM установите в конфигурационном регистре значение 2100. Необходимо запустить маршрутизатор командой <code>b</code> . Появится приглашение <code>rommon&gt;</code> .
01	Запуск из ROM образа загрузки	Для загрузки из ROM образа IOS установите в конфигурационном регистре значение 2101. Маршрутизатор выведет приглашение <code>router(boot)&gt;</code> .
02 — F	Определяет имя загрузочного файла по умолчанию,	Любое значение от 2102 до 210F предписывает маршрутизатору использовать команды загрузки, записанные в NVRAM.

## Проверка текущего значения конфигурационного регистра

Для вывода текущего значения конфигурационного регистра служит команда `show version` (краткая форма: `sh version` или `show ver`):

```
Router#sh version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.0(3)T3, RELEASE SOFTWARE (fc1)
[листинг сокращен]
Configuration register is 0x2102
(конфигурационный регистр равен 0x2102)
```

В последней строке указано текущее значение конфигурационного регистра. В нашем примере оно равно 0x2102, т.е. значению по умолчанию. Команда `show version` выводит также версию IOS. В нашем примере версия IOS равна 12 0(3)T3.

## Изменение конфигурационного регистра

Можно модифицировать значение в конфигурационном регистре для изменения способа запуска и загрузки маршрутизатора:

- Установить запуск системы в режиме монитора ROM
- Указать источник загрузки и имя загрузочного файла по умолчанию
- Разрешить или запретить действие прерывания (функция Break)
- Управлять адресом широковещательной рассылки
- Установить скорость обмена в бодах для консольного терминала
- Загрузить операционное программное обеспечение из ROM
- Разрешить загрузку с сервера TFTP (Trivial File Transfer Protocol — упрощенный протокол пересылки файлов)

**ВНИМАНИЕ** | Перед изменением значения в конфигурационном регистре нужно знать его текущее состояние. Для вывода текущего значения служит команда `show version`.

Для изменения значения в конфигурационном регистре используется команда `config-register`. Например, показанные ниже команды предписывают маршрутизатору загрузку в режиме монитора ROM с последующим выводом текущего значения конфигурационного регистра:

```
Router(config)#config-register 0x0101
Router(config)#^Z
Router#sh ver
[листинг сокращен]
Configuration register is 0x2102 (will be 0x0101 at next reload)
(конфигурационный регистр равен 0x2102, но получит значение 0x0101
при следующей перезагрузке)
```

Команда `show version` показала текущее значение, а также значение в конфигурационном регистре, которое будет установлено после перезагрузки маршрутизатора. Любые изменения конфигурационного регистра не действуют до перезагрузки (перезапуска) маршрутизатора.

## Восстановление пароля

Если маршрутизатор оказался заблокирован, поскольку администратор забыл пароль, то восстановить этот пароль поможет изменение конфигурационного регистра. Разряд 6 данного регистра указывает маршрутизатору на использование содержимого памяти NVRAM для загрузки конфигурации маршрутизатора.

По умолчанию в конфигурационном регистре записано значение 0x2102, т.е. разряд 6 выключен. При значении по умолчанию маршрутизатор будет искать и загружать конфигурацию из NVRAM (`startup-config`). Для восстановления пароля следует включить бит в шестом разряде, что укажет маршрутизатору на игнорирование содержимого NVRAM (в том числе и пароля. — *Прим. пер.*). После включения бита в разряде 6 значением конфигурационного регистра станет 0x2142.

Основные операции для восстановления пароля:

1. Загрузите маршрутизатор и прервите выполнение загрузочной последовательности операцией `Break`.
2. Измените значение в конфигурационном регистре для включения бита шестого разряда (т.е. установите значение 0x2142).
3. Перезагрузите маршрутизатор.
4. Войдите в привилегированный режим.
5. Скопируйте файл `startup-config` в исполняемую конфигурацию `running-config`.

6. Измените пароль.
7. Сбросьте конфигурационный регистр в значение по умолчанию.
8. Перезагрузите маршрутизатор.

Эти операции подробно рассмотрены в следующих разделах книги, где предложены примеры восстановления доступа к маршрутизаторам серий 2600 и 2500.

## Прерывание загрузочной последовательности маршрутизатора

Первой операцией является запуск загрузки маршрутизатора и ее прерывание. Обычно для прерывания (функция Break) используется клавиатурная комбинация Ctrl+Break, например в программе HyperTerminal.

**▼ОСТОРОЖНО** Программа HyperTerminal в Windows NT по умолчанию не выполняет прерывания. Необходимо обновить эту программу или перейти в операционную систему Windows 95/98.

Мы получим следующее:

```
System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
TAC:Home:SW:IOS:Specials for info
PC = 0xffff0a530, Vector = 0x500, SP = 0x680127b0
C2600 platform with 32768 Kbytes of main memory
PC = 0xffff0a530, Vector = 0x500, SP = 0x80004374
monitor: command "boot" aborted due to user interrupt
(монитор: отмена команды boot из-за прерывания пользователем)
rommon 1 >
```

Обратите внимание на строку "boot" aborted due to user interrupt. В этот момент на некоторых маршрутизаторах выводится приглашение rommon 1>.

## Изменение конфигурационного регистра

Для изменения конфигурационного регистра служит команда config-register. Чтобы включить шестой разряд, можно записать в конфигурационный регистр значение 0x2142.

### Команды для серии Cisco 2600

Для включения разряда в маршрутизаторе серии Cisco 2600 достаточно ввести команду в приглашении rommon 1>:

```
rommon 1 > confreg 0x2142
```

```
You must reset or power cycle for new config to take effect
(для использования новой конфигурации необходимо сбросить устройство
или выполнить цикл выключения/включения питания)
```

### Команды для серии Cisco 2500

Для изменения конфигурационного регистра в маршрутизаторе серии 2500 введите `o` после прерывания загрузочной последовательности. Откроется меню с параметрами настройки конфигурационного регистра. Для **изменения** этого регистра служит команда `o/r`, аргументом которой является новое значение. Пример включения бита шестого разряда в маршрутизаторе 2501:

```
System Bootstrap, Version 11.0(10c), SOFTWARE
Copyright (c) 1986-1996 by Cisco Systems
2500 processor with 14336 Kbytes of main memory
Abort at 0x1098FEC (PC) (прервано на инструкции ПК 0x1098FEC)
>o
Configuration register= 0x2102 at last boot
(значение конфигурационного регистра при последней загрузке = 0x2102)
Bit# Configuration register option settings:
 (Разряд Режим конфигурационного регистра)
15 Diagnostic mode disabled
 (отключен режим диагностики)
14 IP broadcasts do not have network numbers
 (широковещательные рассылки IP не имеют номера сети)
13 Boot default ROM software if network boot fails
 (загрузка программного обеспечения по умолчанию из ROM
 при отказе загрузки по сети)
12-11 Console speed is 9600 baud
 (скорость обмена с консолью равна 9600 бод)
10 IP broadcasts with ones
 (IP-адрес широковещательной рассылки со всеми единицами)
08 Break disabled
 (запрещено прерывание)
07 OEM disabled
 (запрещен режим OEM)
06 Ignore configuration disabled
 (запрещено игнорирование конфигурации)
03-00 Boot file is cisco2-2500 (or 'boot system' command)
 (файл загрузки cisco2-2500 или команда boot system)
>o/r 0x2142
```

### Перезагрузка маршрутизатора и вход в привилегированный режим

Далее следует сбросить маршрутизатор:

- В маршрутизаторе серии 2600 введите `reset`.
- » В маршрутизаторе серии 2500 введите `I` (т.е. `initialize` — инициализация).

Маршрутизатор выполнит перезагрузку и предложит перейти в режим установки (поскольку не используется `startup-config`). Введите `No` для

входа в режим установки, нажмите Enter для перехода в пользовательский режим, затем задайте **enable** для перехода в привилегированный режим.

### Просмотр и изменение конфигурации

Введите пароли пользовательского и привилегированного режимов. Скопируйте файл `startup-config` в файл `running-config`:

```
copy startup-config running-config
```

или в краткой форме:

```
copy start run
```

Теперь конфигурация выполняется в памяти RAM и мы находимся в привилегированном режиме, т.е. можем просмотреть и изменить конфигурацию. Хотя не допускается вывод разрешенного секрета, можно заменить пароль новым значением:

```
config t
```

```
enable secret todd
```

### Сброс конфигурационного регистра и перезагрузка маршрутизатора

Завершив изменение пароля, восстановите в конфигурационном регистре значение по умолчанию командой `config-register`:

```
config t
```

```
config-register 0x2102
```

Перезагрузите маршрутизатор.

## Резервное копирование и восстановление Cisco IOS

Перед обновлением или восстановлением операционной системы Cisco IOS необходимо иметь копию существующего файла на хосте TFTP для использования в виде резервной (архивной) в случае неправильной работы нового образа системы. Подойдет любой хост TFTP. По умолчанию для хранения Cisco IOS служит флэш-память маршрутизатора. Рассмотрим операции по проверке объема флэш-памяти, копирования Cisco IOS из флэш-памяти на хост TFTP, а также в обратном направлении.

### Проверка флэш-памяти

Перед обновлением Cisco IOS в маршрутизаторе новым образом файла IOS следует проверить, достаточен ли объем флэш-памяти для размещения нового образа системы. Команда `show flash` (краткая форма `sh flash`) выводит объем флэш-памяти и сведения о хранящемся в ней файле(ах):

```

Router#sh flash
System flash directory:
(системный флэш-каталог)
File Length Name/status
(Файл Длина Имя/статус)
1 8121000 c2500-js-l.112-18.bin
[8121064 bytes used, 8656152 available, 16777216 total]
(использовано 8121064 байтов, доступно 8656152 байтов, всего 16777216)
16384K bytes of processor board System flash (Read ONLY)
(16384Кбайтов системной памяти "только чтение" на процессорной плате)
Router#

```

Рассмотрим составные части имени файла (`c2500-js-l.112-18.bin`), которое отражает принадлежность к аппаратной платформе и другую информацию:

- C2500 — платформа Cisco серии 2500.
- j — файл является корпоративным образом.
- s — файл поддерживает улучшенные возможности.
- l — файл может быть при необходимости перемещен из флэш-памяти и не является сжатым.
- 11.2-18 — номер пересмотра (revision number).
- .bin — двоичный исполняемый файл Cisco IOS.

Последняя строка в листинге из маршрутизатора показывает, что объем флэш-памяти равен 16 384 Кбайтам (или 16 Мбайт). Следовательно, в эту память поместится образ объемом 10 Мбайт. После подтверждения того, что флэш-память способна хранить образ IOS, перейдем к операциям резервного копирования.

## Резервное копирование Cisco IOS

Для резервного копирования Cisco IOS на хост TFTP служит команда `copy flash tftp`. В ней нужно указать только имя файла-источника и IP-адрес хоста TFTP.

Успешность копирования во многом определяется надежностью соединения с хостом TFTP. Это можно проверить утилитой Ping из консольного приглашения маршрутизатора, например:

```

Router#ping 192.168.0.120
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.120, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

```

**▼ ВНИМАНИЕ** | Утилита Ping (Packet Internet Groper — посыльный пакетов Интернета) служит для проверки соединений в сети. Она используется в нескольких примерах и подробно рассмотрена в конце этой главы.

Проверив по Ping доступ по протоколу IP к хосту TFTP, можно использовать команду `copy flash tftp` для копирования IOS на хост TFTP (см. ниже). После ввода команды выводится имя файла из флэш-памяти, что позволяет копировать/вставить его в приглашение ввода имени файла источника.

```
Router#copy flash tftp
System flash directory:
File Length Name/status
1 8121000 c2500-js-l.112-18.bin
[8121064bytes used, 8656152available, 16777216total]
Address or name of remote host [255.255.255.255]? 192.168.0.120
(адрес или имя удаленного хоста)
Source file name? c2500-js-l.112-18.bin
(имя файла источника)
Destination file name [c2500-js-l.112-18.bin]? (press enter)
(имя файла назначения)
Verifying checksum for 'c2500-js-l.112-18.bin' file #1)...OK
(проверка контрольной суммы)
Copy '/c2500-js-l.112-18' from Flash to server as '/c2500-js-l.112-18'? [yes/no]
(копирование файла /c2500-js-l.112-18 из флэш на сервер имением
/c2500-js-l.112-18)
!!
!!!!!!!!!!!!!!!!!!!! [листинг сокращен]
Upload to server done
(загрузка на сервер завершена)
Flash copy took 00:02:30 [hh:mm:ss]
(копирование флэш занято)
Router#
```

В показанном примере флэш-память успешно скопирована на хост TFTP. В качестве адреса удаленного хоста используется IP-адрес хоста TFTP. Именем файла источника служило имя файла из флэш-памяти.

**▼ ОСТОРОЖНО** | Команда `copy flash tftp` не выводит приглашения для ввода местоположения файла и не запрашивает адрес для размещения копируемого файла. Сервер TFTP действует по принципу "взять и сохранить", поэтому на сервере должен быть определен каталог по умолчанию, иначе копирование становится невозможным.

## Восстановление и обновление Cisco IOS в маршрутизаторе

Иногда требуется восстановить Cisco IOS во флэш-памяти для замены исходного файла, который оказался испорченным, или во время обновления IOS. Можно загрузить во флэш-память файл с хоста TFTP командой `copy tftp flash`. Необходимо указать IP-адрес хоста TFTP и имя загружаемого во флэш-память файла.

Перед началом загрузки следует проверить, что загружаемый файл находится в каталоге по умолчанию хоста TFTP. После ввода команды не запрашивается местоположение файла на хосте TFTP. Если восстанавливаемый файл не находится в каталоге по умолчанию хоста TFTP, то копирование не выполняется.

**ОСТОРОЖНО** | Копирование IOS с хоста TFTP во флэш-память требует перезагрузки маршрутизатора. Поэтому операции обновления или восстановления IOS лучше перенести с 9 утра в понедельник на обеденный перерыв.

После ввода команды `copy tftp flash` появляется сообщение о необходимости перезагрузки маршрутизатора и запуска образа IOS из ROM:

```
Router#copy tftp flash
 **** NOTICE ****
```

```
Flash load helperv1.0
(вспомогательный загрузчик флэш v1.0)
```

```
This process will accept the copy options and then terminate the current system
image to use the ROM based image for the copy. Routing functionality will not be
available during that time. If you are logged in via telnet this connection will
terminate. Users with console access can see the results of the copy operation.
```

```
(Этот процесс принимает параметры копирования, а затем завершает
использование текущего системного образа из ROM для выполнения
копирования. В процессе копирования перестает действовать маршрутиза-
ция. Если пользователь был подключен по протоколу Telnet, соединение
завершается. Пользователи с консольным доступом смогут увидеть
результаты операции копирования)
```

```
_____*****_____
Proceed? [confirm](pressenter)
```

После нажатия клавиши Enter для подтверждения будущей перезагрузки маршрутизатора выводится показанный ниже листинг. Когда маршрутизатор начинает взаимодействовать с хостом TFTP, запоминается адрес этого хоста и выводится приглашение для нажатия клавиши Enter.

```
System flash directory:
File Length Name/status
1 8121000 /c2500-js-l.112-18
[8121064 bytes used, 8656152 available, 16777216 total]
```

Address or name of remote host [192.168.0.120]? (press enter)

Следующее приглашение служит для ввода имени файла, копируемого во флэш-память. Этот файл должен находиться в каталоге по умолчанию на хосте TFTP.

Source file name? **c2500-js56i-l.120-9.bin**

Destination file name [c2500-js56i-l.120-9.bin]? (press enter)

Accessing file 'c2500-js56i-l.120-9.bin' on 192.168.0.120...

Loading c2500-js56i-l.120-9.bin from 192.168.0.120 (via Ethernet0): ! [OK]

После указания маршрутизатору имени файла и его местоположения, выводится приглашение для подтверждения стирания флэш-памяти.

**▼ ВНИМАНИЕ**

Если объема флэш-памяти недостаточно для хранения обеих копий, либо используется новая ("чистая") флэш-память, маршрутизатор предложит стереть содержимое флэш-памяти перед записью в нее нового файла.

Подтверждение операции придется выполнить три раза, чтобы показать, что вы намерены стереть флэш-память. Если явно не указать команду `copy run start`, то выводится приглашение на ее исполнение, поскольку маршрутизатору необходимо перезагрузиться.

Erase flash device before writing? [confirm] (press enter)

(стереть устройство флэш перед записью)

Flash contains files. Are you sure you want to erase?

[confirm] (press enter)

(флэш содержит файлы, вы уверены в необходимости стирания)

System configuration has been modified. Save? [yes/no]:y

(системная конфигурация изменена, сохранить ее)

Building configuration..(построение конфигурации)

[OK]

Copy 'c2500-js56i-l.120-9.bin' from server

as 'c2500-js56i-l.120-9.bin' into Flash WITH erase? [yes/no] y

После выбора ответа "yes" для стирания флэш-памяти маршрутизатор должен перезапуститься для загрузки из памяти ROM небольшой специализированной версии IOS. Нельзя стереть флэш-память, которая используется.

После стирания содержимого флэш-памяти проводится доступ к файлу на хосте TFTP и копирование его во флэш-память.

%SYS-5-RELOAD: Reload requested

(запрошена перезагрузка)

%FLH: c2500-js56i-l.120-9.bin from 192.168.0.120 to flash ...

System flash directory:

File Length Name/status

1 8121000 /c2500-js-L.112-18

```
[8121064 bytes used, 8656152 available, 16777216 total]
Accessing file 'c2500-js56i-l.120-9.bin' on 192.168.0.120...
Loading c2500-js56i-l.120-9.bin from 192.168.0.120 (via Ethernet0): ! [OK]
(загрузка файла c2500-js56i-l.120-9.bin с адреса 192.168.0.120
через интерфейс Ethernet0)

Erasing device...
ee
(стирание устройства)
Loading c2500-js56i-l.120-9.bin from 192.168.0.120 (via Ethernet0):
!!
!!!!!!!!!!!!!!!!!!!! [листинг сокращен]
```

Строка символов `e` показывает процесс стирания флэш-памяти. Каждый восклицательный знак (!) означает успешную пересылку одного сегмента UDP.

После завершения копирования появится сообщение:

```
[OK - 10935532/16777216bytes]
Verifying checksum... OK (0x2E3A)
(проверка контрольной суммы)
Flash copy took 0:06:14 [hh:mm:ss]
%FLN: Re-booting system after download
(перезапуск системы после загрузки)
```

После загрузки файла во флэш-память и проверки контрольной суммы, маршрутизатор перезагружается для запуска нового файла IOS.

**▼ ВНИМАНИЕ** | Маршрутизатор Cisco может стать серверным хостом TFTP с образом системы, которая исполняется из флэш-памяти. Для этого служит команда глобального конфигурирования `tftp-server система имя_ios`.

## Резервное копирование и восстановление конфигурации в устройстве Cisco

Все изменения в конфигурации маршрутизатора записываются в файл `running-config`. Если не выполнить команду `copy run start` после изменения в файле `running-config`, то изменения будут применены после перезагрузки маршрутизатора или после цикла выключения/включения сетевого питания. Разрешено сделать дополнительную копию конфигурационной информации для непредвиденных обстоятельств, например, на случай отказа маршрутизатора или переключателя, либо для документирования текущей конфигурации устройства. Рассмотрим процедуры копирования конфигурации маршрутизатора и переключателя на хост TFTP, а также восстановление этой конфигурации.

## Резервное копирование конфигурации маршрутизатора Cisco

Для копирования конфигурации маршрутизатора на хост TFTP можно использовать команду `copy running-config tftp` или `copy startup-config tftp`. Любая из них выполнит резервное копирование текущей конфигурации маршрутизатора, запущенной из памяти DRAM, или хранящейся в памяти NVRAM.

### Проверка текущей конфигурации

Для проверки конфигурации в DRAM служит команда `show running-config` (краткая форма: `sh run`):

```
Router#sh run
Building configuration...

Current configuration:
!
version 12.0
```

Полученная информация о текущей конфигурации показывает, что маршрутизатор исполняет версию 12.0 операционной системы IOS.

### Проверка хранимой конфигурации

На следующем этапе необходимо проверить конфигурацию, хранящуюся в NVRAM. Для этого служит команда `show startup-config` (краткая форма: `sh start`):

```
Router#sh start
Using 366 out of 32762 bytes
!
version 11.2
```

Во второй строке листинга показан объем конфигурации. В нашем случае объем NVRAM равен 32 Кбайтам, но занято только 366 байт. Номер версии конфигурации в памяти NVRAM равен 11.2 (поскольку после обновления маршрутизатора не выполнялось копирование из `running-config` в `startup-config`).

Если нет уверенности в том, что оба файла одинаковы, причем необходимо использовать файл `running-config`, для согласования файлов следует выполнить команду `copy running-config startup-config` (см. ниже).

### Копирование в NVRAM текущей конфигурации

За счет копирования файла `running-config` в NVRAM мы формируем резервную копию этого файла и гарантируем, что файл `running-config` всегда будет перезагружаться при запуске маршрутизатора. В IOS версии 12.0 выводится приглашение для ввода имени файла, который должен использоваться. Кроме того, в показанном ниже примере версия IOS

равна 11.2. При последнем исполнении команды `copy run start` маршрутизатор рекомендует обновить этот файл на новую версию 12.0.

```
Router#copyrunstart
Destination filename [startup-config]? (press enter)
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
(внимание: попытка перезаписи конфигурации в NVRAM, ранее сохраненной
с иной версией системного образа)
Overwrite the previous NVRAM configuration?[confirm](press enter)
(перезаписать предыдущую конфигурацию в NVRAM)
Building configuration...
[OK]
```

Теперь, после запуска `show starting-config` мы увидим версию 12.0:

```
Router#sh start
Using 487 out of 32762 bytes
!
version 12.0
```

### Копирование конфигурации на хост TFTP

После копирования файла в NVRAM можно сделать вторую резервную копию на хосте TFTP командой `copy running-config tftp` (краткая форма: `copy run tftp`):

```
Router#copyrun tftp
Address or name of remote host []? 192.168.0.120
Destination filename [router-config]? todd1-config
!!
487 bytes copied in 12.236 secs (40 bytes/sec)
Router#
```

В листинге только два восклицательных знака (!!), отмечающих два подтверждения UDP. В нашем примере файл назван `todd1-config`, поскольку в маршрутизаторе не было установлено имя хоста. Если же имя хоста сконфигурировано, команда автоматически будет использовать это имя с расширением `-config` в качестве имени копируемого файла.

## Восстановление конфигурации маршрутизатора Cisco

После изменения файла `running-config` в маршрутизаторе иногда необходимо восстановить конфигурацию из файла `startup-config`. Проще всего использовать команду `copy startup-config running-config` (краткая форма: `copy start run`). Для восстановления конфигурации можно пользоваться устаревшей командой Cisco — `config mem`. Однако для этого следует предварительно (до начала любых изменений) скопировать файл `running-config` в NVRAM.

Если конфигурация маршрутизатора записана на хост TFTP в виде дополнительной резервной копии, можно пользоваться командами `copy tftp running-config` (краткая форма: `copy tftp run`) и `copy tftp startup-config` (краткая форма: `copy tftp start`). Для этого же существует устаревшая команда `config net`.

```
Router#copytftp run
Address or name of remote host []? 192.168.0.120
Source filename []? todd1-config
Destination filename [running-config]? (press enter)
Accessing tftp://192.168.0.120/todd1-config...
Loading todd1-config from 192.168.0.120 (via Ethernet0):
!!
[OK - 487/4096 bytes]
487 bytes copied in 5.400 secs (97 bytes/sec)
Router#
00:38:31: %SYS-5-CONFIG: Configured from tftp://
192.168.0.120/todd1-config
Router#
```

Файл конфигурации является текстовым файлом ASCII. Следовательно, перед копированием конфигурации с хоста TFTP обратно в маршрутизатор, можно изменить файл конфигурации в любом текстовом редакторе.

## Стирание конфигурации

Для удаления файла `startup-config` в маршрутизаторе Cisco служит команда `erase startup-config`:

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files!
Continue? [confirm](press enter)
(стирание файловой системы NVRAM приводит к удалению всех файлов.
Продолжить?)
[OK]
Erase of nvram: complete
(стирание NVRAM: завершено)
Router#
```

Показанная выше команда удаляет содержимое памяти NVRAM в маршрутизаторе. При следующей загрузке маршрутизатор перейдет в режим установки.

## Использование протокола Cisco Discovery Protocol

*Протокол CDP* (Cisco Discovery Protocol — протокол исследования компании Cisco) является лицензированным протоколом, разработанным Cisco для помощи сбора информации администраторами о локально подключенных и удаленных устройствах. Использование CDP позволяет собрать данные об оборудовании и протоколах соседнего устройства. Эта информация полезна для диагностики и документирования сети.

### Получение информации по протоколу CDP о таймере и времени удержания

Команда `show cdp` (краткая форма: `sh cdp`) показывает сведения о двух глобальных параметрах CDP, настраиваемых в устройствах Cisco:

- Таймер CDP определяет, как часто передаются пакеты CDP во все активные интерфейсы.
- Время удержания CDP определяет интервал хранения пакета, полученного от соседнего устройства.

Маршрутизаторы и переключатели Cisco используют одинаковые параметры.

Пример листинга из маршрутизатора:

```
Router#sh cdp
GlobalCDP information:
(глобальная информация CDP)
 Sending CDP packets every 60 seconds
 (отправка пакетов CDP каждые 60 с)
 Sending a holdtime value of 180 seconds
 (отправка значения времени удержания каждые 180 с)
Router#
```

Для настройки таймера и времени удержания CDP в маршрутизаторе служат глобальные команды `cdp holdtime` и `cdp timer`.

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#cdp?
 holdtime Specify the holdtime (in sec) to be sent in packets
 (время удержания определяет интервал удержания в секундах,
 сообщаемый в пакетах)
 timer Specify the rate at which CDP packets are sent(in sec)
 (таймер определяет периодичность отправки пакетов CDP в секундах)
Router(config)#cdp timer 90
Router(config)#cdp holdtime 240
Router(config)#^Z
```

Можно полностью выключить протокол CDP командой `no cdp run` в режиме глобального конфигурирования маршрутизатора. Для включения или выключения CDP в определенном интерфейсе маршрутизатора служат команды `no cdp enable` и `cdp enable` (см. ниже).

## Получение информации от соседних устройств

Команда `show cdp neighbor` (краткая форма: `sh cdp nei`) показывает информацию о непосредственно подключенных устройствах. Важно отметить, что пакеты CDP не проходят через переключатели Cisco, поэтому "видны" только непосредственно подключенные устройства. В соединенном с переключателем маршрутизаторе мы не "видим" других устройств, которые соединены с переключателем.

Пример листинга команды `show cdp neighbor` в маршрутизаторе 2509:

```
Todd2509#sh cdp nei
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
```

```
S - Switch, H - Host, I - IGMP, r - Repeater
```

(коды функциональных возможностей: R - маршрутизатор, T - транзитный мост, B - мост с маршрутизацией от источника, S - переключатель, H - хост, I - устройство с протоколом IGMP, r - повторитель)

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
1900Switch	Eth 0	238	TS	1900	2
2500B	Ser 0	138	R	2500	Ser 0

(Идентификатор устройства Локальный интерфейс Время удержания

Код возможностей Платформа Идентификатор порта)

```
Todd2501#
```

В таблице 7.5 перечислены сведения, выводимые командой `show cdp neighbor` для каждого типа устройств.

Еще одна команда для показа информации о соседях — `show cdp neighbor detail` (краткая форма: `show cdp nei de`) — может выполняться маршрутизатором или переключателем. Эта команда показывает подробную информацию обо всех соединенных устройствах. Пример листинга команды для маршрутизатора:

```
Todd2509#sh cdp neighbor detail
```

```

```

```
Device ID: 1900Switch
```

```
Entry address(es):
```

```
(входной адрес/адреса)
```

```
IPaddress:0.0.0.0
```

```
Platform: cisco 1900, Capabilities: Trans-Bridge Switch
```

```
Interface: Ethernet0, Port ID (outgoing port): 2
```

```
Holdtime : 166 sec
```

```
Version :
```

```
V9.00
```

```

```

```

Device ID: 2501B
Entry address(es):
 IP address: 172.16.10.2
Platform: cisco 2500, Capabilities: Router
Interface: Serial0, Port ID (outgoing port): Serial0
Holdtime : 154 sec
Version :
Cisco Internetwork Operating System Software
IOS(tm) 3000 Software (IGS-J-L), Version 11.1(5), RELEASE
SOFTWARE (fc1) Copyright (c) 1986-1996 by cisco Systems,
Inc. Compiled Mon 05-Aug-96 11:48 by mkamson
Todd2509#

```

### Таблица 7.5.

#### Содержимое листинга команды `show cdp neighbor`

Поле	Описание
Device ID (идентификатор устройства)	Имя хоста непосредственно подключенного устройства.
Local Interface (локальный интерфейс)	Порт или интерфейс, получающий пакеты CDP.
Holdtime (время удержания)	Интервал хранения информации в маршрутизаторе перед удалением при отсутствии следующих пакетов CDP.
Capability (возможности)	Роль соседнего устройства, например маршрутизатор, переключатель или повторитель. Коды функциональных возможностей расшифрованы в листинге команды.
Platform (платформа)	Тип устройства Cisco. В показанном выше листинге с переключателем соединены Cisco 2509, Cisco 2511 и Catalyst 5000. Устройство 2509 видит только переключатель и маршрутизатор 2501, соединенный с последовательным интерфейсом serial 0.
Port ID (идентификатор порта)	Порт или интерфейс соседнего устройства, в котором выполняются широковещательные рассылки пакетов CDP.

В представленном листинге отмечены имя хоста и IP-адрес для непосредственно подключенных устройств. Эта же информация выводится командой `show cdp neighbor` (см. таблицу 7.5). Однако команда `show cdp neighbor detail` дополнительно показывает версию IOS соседнего устройства.

Команда `show cdp entry *` выводит ту же информацию, что и `show cdp neighbor details`. Пример листинга `show cdp entry *` для маршрутизатора:

```
Todd2509#sh cdp entry *
```

```

Device ID: 1900Switch
Entry address(es):
 IP address: 0.0.0.0

```

```
Platform: dsc0 1900, Capabilities: Trans-Bridge Switch
Interface: Ethernet0, PortID (outgoing port): 2
Holdtime : 223 sec
Version :
V9.00
```

```

Device ID: 2501B
Entry address(es):
 IP address: 172.16.10.2
Platform: dsc0 2500, Capabilities: Router
Interface: Serial0, Port ID (outgoing port): Serial0
Holdtime : 151 sec
Version :
Cisco Internetwork Operating System Software
IOS(tm) 3000 Software (IGS-J-L), Version 11.1(5), RELEASE
SOFTWARE (fc1) Copyright (c) 1986-1996 by Cisco Systems,
Inc. Compiled Mon 05-Aug-96 11:48 by mkamson
Todd2509#
```

## Получение информации о трафике в интерфейсе

Команда `show cdp traffic` выводит данные о трафике интерфейса, включая количество полученных пакетов CDP, а также число ошибок для протокола CDP.

Пример команды `show cdp traffic` в маршрутизаторе:

```
Router#sh cdp traffic
CDP counters:
(счетчики CDP)
 Packets output: 13, Input: 8
 (вывод пакетов: 13, ввод: 8)
 Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
 (синтаксис заголовка: 0, ошибок контрольной суммы: 0, неудачных
 инкапсуляции: 0)
 No memory: 0, Invalid packet: 0, Fragmented: 0
 (ошибок "нет памяти": 0, неправильных пакетов: 0, фрагментации: 0)
Router#
```

## Получение информации о портах и об интерфейсах

Команда `show cdp interface` (краткая форма: `sh cdp inter`) показывает статус CDP в интерфейсе маршрутизатора или порту переключателя.

Можно полностью отключить CDP в маршрутизаторе командой по `cdp run`. CDP можно отключать в отдельных интерфейсах командой по `cdp enable`. Для разрешения порта служит команда `cdp enable`. Все порты и интерфейсы по умолчанию допускаются для протокола CDP.

В маршрутизаторе команда `show cdp interface` выведет сведения о всех интерфейсах, использующих CDP, включая информацию о инкапсуляции в линии связи, таймер и время удержания для каждого интерфейса. Пример листинга команды в маршрутизаторе:

```
Router#sh cdp interface
Ethernet0 is up, line protocol is up
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
Serial0 is administratively down, line protocol is down
 Encapsulation HDLC
 Sending CDP packet every 60 seconds
 Holdtime is 180 seconds
Serial1 is administratively down, line protocol is down
 Encapsulation HDLC
 Sending CDP packet every 60 seconds
 Holdtime is 180 seconds
```

Для выключения CDP в определенном интерфейсе маршрутизатора используется команда `no cdp enable` в режиме конфигурации интерфейса:

```
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s0
Router(config-if)#no cdp enable
Router(config-if)#^Z
```

Проверим внесенное изменение командой `show cdp interface`:

```
Router#sh cdp int
Ethernet0 is up, line protocol is up
 Encapsulation ARPA
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
Serial1 is administratively down, line protocol is down
 Encapsulation HDLC
 Sending CDP packets every 60 seconds
 Holdtime is 180 seconds
Router#
```

Интерфейс `serial 0` уже не показан в листинге команды.

## Использование Telnet

Telnet — это протокол виртуального терминала из стека TCP/IP. Telnet обеспечивает соединение с удаленными устройствами, сбор информации и запуск программ.

После настройки маршрутизатора или переключателя можно пользоваться программой Telnet для конфигурации и проверки этих устройств вместо использования подключения через консольный кабель. Для запуска программы Telnet следует ввести telnet в любой командной строке (DOS или Cisco). На маршрутизаторе должен быть установлен пароль VTU.

Протокол CDP не позволяет собирать информацию о маршрутизаторах и переключателях, которые не подключены к устройству. Однако программа Telnet поможет соединиться с соседним устройством и запустить на нем CDP для сбора информации по протоколу CDP об удаленном устройстве.

Команду telnet можно ввести в любом приглашении маршрутизатора, например:

```
Todd2509#telnet 172.16.10.2
Trying 172.16.10.2 ...Open
(попытка подключения к 172.16.10.2. Сеанс открыт)

Password required, but none set
(требуется пароль, но он не установлен)

[Connection to 172.16.10.2closed by foreign host]
(соединение с 172.16.10.2закрывается внешним хостом)
Todd2509#
```

В примере показано, что пароль не установлен! Порты VTU в маршрутизаторе всегда конфигурируются на вход в систему, т.е. необходимо использовать пароль VTU или отменить его действие командой no login (см. главу 4).

В маршрутизаторах Cisco необязательно пользоваться командой telnet. Если ввести в приглашении IP-адрес, маршрутизатор предполагает соединение с указанным устройством по Telnet, например:

```
Todd2509#172.16.10.2
Trying 172.16.10.2 ... Open
Password required, but none set

[Connection to 172.16.10.2closed by foreign host]
Todd2509#
```

Установим в маршрутизаторе пароль VTU, чтобы можно было подключаться к этому устройству по Telnet. Пример установки пароля:

```
2501B#config t
Enter configuration commands, one per line. End with CNTL/Z.
```

```

2501B(config)#line vty 0 4
2501B(config-line)#login
2501B(config-line)#password todd
2501B(config-line)#^Z
2501B#
%SYS-5-CONFIG_I: Configured from console by console
(конфигурация с консоли посредством консоли)

```

Теперь снова подключимся к маршрутизатору (с консоли маршрутизатора 2509).

```

Todd2509#172.16.10.2
Trying 172.16.10.2 ...Open
User Access Verification (проверка доступа пользователя)
Password: (пароль)
2501B>

```

Пароль VTY — это пароль **пользовательского** режима, но не режима разрешенного пароля. Посмотрим, что произойдет при переходе в привилегированный режим и после подключения по Telnet к маршрутизатору 2501B:

```

2501B>en
% No password set
2501B>

```

Это хорошее средство защиты. Никому не разрешайте обращение по Telnet к устройству для ввода команды `enable`, позволяющей перейти в привилегированный режим. Для конфигурации удаленного устройства по Telnet установите пароль разрешенного режима или пароль разрешенного секрета.

## Одновременный доступ по Telnet к нескольким устройствам

Во время доступа по Telnet к маршрутизатору или переключателю можно прекратить соединение, введя в любой момент команду `exit`! Однако если требуется сохранить соединение с удаленным устройством, но вернуться в исходный консольный режим доступа к маршрутизатору, то следует нажать `Ctrl+Shift+6`, отпустить все эти клавиши, а затем нажать `X`.

Пример подключения к нескольким устройствам с консоли маршрутизатора Todd2509:

```

Todd2509#telnet 172.16.10.2
Trying 172.16.10.2 ...Open
User Access Verification
Password:

```

```
2501B>
Todd2509#
```

В данном случае открыт доступ по Telnet к маршрутизатору 2501B. Введена команда password для перехода в пользовательский режим. Нажата клавиатурная комбинация Ctrl+Shift+6, затем — клавиша X (это не показано ни на экране, ни в листинге). **Заметим**, что приглашение для ввода команд опять стало приглашением маршрутизатора Todd2509.

Можно обращаться по Telnet к переключателям серии 1900. Однако необходимо установить пароль разрешенного режима на уровне 15 до того, как будет получен доступ к переключателю из программы Telnet (установка паролей в переключателях 1900 рассмотрена в приложении B).

Пример доступа по Telnet к переключателю серии 1900, причем с обеспечением консольного вывода из переключателя.

```
Todd2509#telnet 192.168.0.148
Trying 192.168.0.148 ... Open

Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc. 1993-1999
All rights reserved.
Enterprise Edition Software
Ethernet Address: 00-BO-64-75-6B-C0
PCA Number: 73-3122-04
PCA Serial Number: FAB040131E2
Model Number: WS-C1912-A
System Serial Number: FAB0401U0JQ
Power Supply S/N: PHI033108SD
PCB Serial Number: FAB040131E2,73-3122-04
```

```

1user(s) now active on Management Console.
(в управляющей консоли один активный пользователь)
```

```
User Interface Menu
(меню пользовательского интерфейса)
```

```
[M] Menus
(меню)
[K] Command Line
(командная строка)
```

```
Enter Selection:
(укажите выбранный вариант)
```

В данный момент нажата комбинация Ctrl+Shift+6, затем X, что вернет нас обратно в консоль маршрутизатора Todd2509.

```
Todd2509#
```

## Проверка подключения по Telnet

Для показа подключений из маршрутизатора к удаленным устройствам используется команда `show sessions`.

```
Todd2509#sh sessions
Conn Host Address Byte Idle Conn Name
1172.16.10.2 172.16.10.2 0 0 172.16.10.2
* 2 192.168.0.148 192.168.0.148 0 0 192.168.0.148
Todd2509#
```

Символ "звездочка" (\*) в строке второго подключения означает, что оно последнее. Можно вернуться в последнее подключение, дважды нажав Enter. Для возвращения в любое подключение следует ввести его номер и дважды нажать Enter.

## Проверка пользователей Telnet

Для вывода списка всех активных консолей и портов VTY маршрутизатора используется команда `show users`.

```
Todd2509#sh users
Line User Host(s) Idle Location
* 0 con 0 172.16.10.2 00:07:52
 192.168.0.148 00:07:18
```

В листинге команды `con` означает локальную консоль. В нашем примере консоль соединена с двумя удаленными IP-адресами (т.е. с двумя устройствами).

В следующем примере показан листинг команды `show users` в маршрутизаторе 2501B, к которому по Telnet обращается маршрутизатор Todd2509.

```
2501B>sh users
Line User Host(s) Idle Location
0 con 0 idle 9
* 2 vty 0
```

Листинг показывает, что консоль активна и для VTY используется порт 2. Звездочкой отмечен пользователь текущего терминального сеанса.

## Закрытие сеанса Telnet

Завершить сеанс Telnet можно несколькими способами. Проще и быстрее всего ввести `exit` или `disconnect`.

Для завершения сеанса с удаленного устройства служит команда `exit`.

```
2509# (здесь нужно дважды нажать Enter)
[Resuming connection 2 to 192.168.0.148 ...]
(восстановление подключения 2 к 192.168.0.148)
```

```
switch >exit
```

```
[Connection to 192.168.0.148 closed by foreign host]
(соединение 192.168.0.148 закрыто удаленным хостом)
```

```
Todd2509#
```

Для завершения сеанса с локального устройства применяется команда `disconnect`

```
Todd2509#disconnect ?
```

```
<1-2> The number of an active network connection
 (количество активных сетевых соединений)
WORD The name of an active network connection
 (имя активного сетевого соединения)
```

```
<cr>
```

```
Todd2509#disconnect 1
```

```
Closing connection to 172.16.10.2 [confirm]
```

```
Todd2509#
```

В показанном примере использовался номер сеанса 1, поскольку предполагалось завершить именно это соединение с маршрутизатором 2501B. Для просмотра номера соединений применяйте команду `show sessions`.

Если необходимо прервать сеанс устройства, подключенного к маршрутизатору по Telnet, сначала проверьте все подключенные к маршрутизатору устройства. Используйте команду `show users`.

```
2501B#sh users
```

Line	User	Host(s)	Idle	Location
* 0	con 0	idle	0	
1	aux 0	idle	0	
2	vtty 0	idle		0172.16.10.1

Листинг показывает, что VTY 2 имеет подключение к IP-адресу 172.16.10.1. Это маршрутизатор Todd2509.

Для очистки соединения используется команда `clear line`.

```
2501B#clear line 2
```

```
[подтверждение]
```

```
[OK]
```

Проверить успешность отключения пользователя позволит команда `show users`.

```
2501B#sh users
```

```

Line User Host(s) Idle Location
* 0 con 0 idle 0
 1 aux 0 idle 1
2501B#

```

Листинг показывает, что линия очищена.

## Разрешение имен хостов

Чтобы использовать имя хоста вместо IP-адреса при подключении к удаленному устройству, другое устройство, с которого выполняется подключение, должно обеспечить разрешение (определение) имен хостов в IP-адреса. Для этого существуют два способа: построение таблиц хостов на каждом маршрутизаторе или создание сервера DNS (Domain Name System — система доменных имен), который обеспечивает динамическую таблицу хостов.

### Построение таблицы хостов

Таблица хостов обеспечивает разрешение имен только в маршрутизаторе, на котором она находится. Команда для построения таблицы хостов в маршрутизаторе:

```
ip host имя_хоста номер_порта_TCP IP_адрес
```

По умолчанию для протокола TCP используется порт номер 23. Можно организовать сеанс по Telnet через другой номер порта TCP, причем разрешено присвоить имени хоста до восьми IP-адресов.

Пример настройки таблицы хостов с двумя записями для размещения имени маршрутизатора 2501B и имени переключателя:

```

Todd2509#config t
Enter configuration commands, one per line. End with CNTL/Z.
Todd2509(config)#ip host ?
WORD Name of host

Todd2509(config)#ip host 2501B ?
<0-65535> Default telnet port number
 (номер порта Telnet по умолчанию)
A.B.C.D Host IP address (maximum of 8)
 (IP-адреса хостов, не более восьми)

Todd2509(config)#ip host 2501B 172.16.10.2 ?
A.B.C.D Host IP address (maximum of 8)
<cr>

Todd2509(config)#ip host 2501B 172.16.10.2
Todd2509(config)#ip host переключатель 192.168.0.148
Todd2509(config)#^Z

```

Для вывода таблицы хостов служит команда `show hosts`.

**Todd2509#sh hosts**

Default domain is not set

Name/address lookup uses domain service

(просмотр имен и адресов с помощью службы доменов)

Name servers are 255.255.255.255

(сервер имен -255.255.255.255)

Host	Flags	Age	Type	Address(es)
(Хост	Флаги	Возраст	Тип	Адрес/адреса)
2501B	(perm, OK)	0	IP	172.16.10.2
switch	(perm, OK)	0	IP	192.168.0.148

Todd2509#

В показанном листинге маршрутизатора представлены два имени хоста и их IP-адреса. Слово perm в столбце Flags означает настройку этой записи вручную. Если же указано temp, значит элемент таблицы допускается службой DNS.

Для проверки разрешения имен через таблицу хостов вводится имя в приглашении маршрутизатора. Помните, что если команда не указана, маршрутизатор предполагает использование команды telnet. Ниже применялись имена хостов для доступа по Telnet к удаленным устройствам. Затем мы нажали **Ctrl+Shift+6** и **X** для возвращения в главную консоль маршрутизатора Todd2509.

**Todd2509#2501b**

Trying 2501B (172.16.10.2)... Open

User Access Verification

Password:

2501B&gt;

**Todd2509#(control+shift+6, then x)****Todd2509#switch**

Trying switch (192.168.0.148)... Open

Catalyst 1900 Management Console

Copyright (c) Cisco Systems, Inc. 1993-1999

All rights reserved.

Enterprise Edition Software

Ethernet Address: 00-BO-64-75-6B-C0

PCA Number: 73-3122-04

PCA Serial Number: FAB040131E2

Model Number: WS-C1912-A

System Serial Number: FAB0401U0JQ

Power Supply S/N: PHI033108SD

PCB Serial Number: FAB040131E2,73-3122-04

```
1 user(s) now active on Management Console.
```

```
User Interface Menu
```

```
[M] Menus
```

```
[K] Command Line
```

```
Enter Selection: (control+shift+6, then x)
```

```
Todd2509#
```

Мы использовали таблицу хостов для создания сеансов к двум устройствам. С помощью имен можно было по Telnet обратиться к обоим устройствам. Строки в листинге show session показывают, что имя хоста выведено вместо IP-адреса.

```
Todd2509#shsess
```

```
Conn Host Address Byte Idle Conn Name
(Хост подключения Адрес Байт свободно Имя подключения)
 1 switch 192.168.0.148 O O switch
* 2 2501b 172.16.10.2 O O 2501b
Todd2509#
```

Для удаления имени хоста из таблицы хостов служит команда по ip host:

```
RouterA(config)#no ip host routerb
```

Недостатком таблицы хостов является то, что необходимо создавать ее на каждом маршрутизаторе, в противном случае не будет полноценного разрешения имен. Если в сети много маршрутизаторов и стоит задача разрешения имен, советуем применить службу DNS.

## Использование DNS для разрешения имен

Если в сети много устройств и нет желания создавать таблицу хостов на каждом из устройств для разрешения имен хостов, используйте службу DNS.

Когда устройство Cisco получает непонятную команду, по умолчанию происходит попытка разрешения имени через службу DNS. Посмотрим, что произойдет после ввода в приглашении маршрутизатора Cisco специальной команды todd.

```
Todd2509#todd
```

```
Translating "todd"...domain server (255.255.255.255)
(трансляция todd на сервере домена)
```

```
% Unknown command or computer name, or unable to find computer address
(неизвестная команда или имя компьютера, либо невозможно найти адрес
компьютера)
```

```
Todd2509#
```

Маршрутизатор не знает имени todd или не понимает введенной команды, поэтому пытается разрешить проблему с помощью службы DNS. С этим связаны два недостатка. Во-первых, маршрутизатор так и не

запомнит имя todd. Во-вторых, придется некоторое время подождать, пока не закончится разрешение имени. Вполне допустимо запретить по умолчанию просмотр DNS командой `no ip domain-lookup`, которая вводится в глобальном конфигурационном режиме.

Если в сети присутствует сервер DNS, введите несколько команд для запуска процесса разрешения имен через DNS:

- Команда `ip domain-lookup` выполняется по умолчанию. Ее необходимо вводить, только если ранее команда была выключена (т.е. вводилась команда `no ip domain-lookup`).
- Командой `ip name-server` установите IP-адрес сервера DNS. Можно указать до шести IP-адресов разных серверов.
- Команда `ip domain-name` не является обязательной, но лучше ее использовать. Эта команда добавляет при вводе доменное имя к имени хоста. В службе DNS используется система FQDN (Fully Qualified Domain Name, полностью квалифицированное доменное имя), поэтому необходимо полное имя DNS в формате `имя_домена.com`.

Пример применения упомянутых команд:

```
Todd2509#config t
Enter configuration commands, one per line. End with CNTL/Z.
Todd2509(config)#ip domain-lookup
Todd2509(config)#ip name-server ?
 A.B.C.D Domain server IP address (maximum of 6)
Todd2509(config)#ip name-server 192.168.0.70
Todd2509(config)#ip domain-name lammle.com
Todd2509(config)#^Z
Todd2509#
```

После настройки конфигурации DNS следует проверить работу сервера DNS. Используйте имя хоста при обращении по Ping или Telnet к устройству.

```
Todd2509#ping 2501b
Translating "2501b"...domain server (192.168.0.70) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.10.2, timeout is
2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/31/32 ms
```

Заметим, что сервер DNS использовался маршрутизатором для разрешения имени.

После разрешения имени с помощью DNS следует проверить командой `show hosts` кэширование информации об устройстве в таблице хостов, например:

```
Todd2509#sh hosts
```

```
Default domain is lammlle.com
```

```
Name/address lookup uses domain service
```

```
Name servers are 192.168.0.70
```

Host	Flags	Age	Type	Address(es)
2501b.lammlle.com	(temp, OK)	0	IP	172.16.10.2
переключатель	(perm, OK)	0	IP	192.168.0.148

```
Todd2509#
```

Разрешенные имена отменены словом temp, но для переключателя указано perm (т.е. это статическая запись). Именем хоста является полное имя домена. Если не пользоваться командой ip domain-name lammlle.com, надо в приглашении ping ввести 2501b.lammlle.com, что несколько сложнее.

## Проверка сетевых подключений

Для проверки подключения к удаленным устройствам используйте команды ping и trace. Обе команды поддерживаются разными протоколами, а не только протоколом IP.

### Использование команды Ping

Мы уже видели в этой главе много примеров проверки устройств по Ping, чтобы протестировать подключение по протоколу IP или разрешение имен с помощью сервера DNS. Для вывода списка поддерживаемых протоколов воспользуемся командой ping ?.

```
Todd2509#ping ?
```

```
WORD Ping destination address or hostname
```

```
apollo Apollo echo
```

```
appletalk Appletalk echo
```

```
clns CLNS echo
```

```
decnet DECnet echo
```

```
ip IP echo
```

```
ipx Novell/IPX echo
```

```
srb srb echo
```

```
tag Tag encapsulated IP echo
```

```
vines Vines echo
```

```
xns XNS echo
```

```
<cr>
```

В листинге команды ping отмечены минимальное, среднее и максимальное времена передачи и возвращения пакета Ping от указанной системы, например:

```
Todd2509#pingtodd2509
```

```
Translating "todd2509"...domain server (192.168.0.70) [OK]
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.121, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
Todd2509#
```

Видно, что для разрешения имен используется сервер DNS, а проверка устройства по Ping заняла 32 мс (миллисекунды).

## Использование команды Trace

Команда trace показывает путь пакета к удаленному устройству. Для вывода списка поддерживаемых протоколов воспользуемся командой trace ?.

```
Todd2509#trace ?
WORD Trace route to destination address or hostname
appletalk AppteTalk Trace
clns - ISO CLNS Trace
ip IP Trace
ipx IPX Trace
oldvines Vines Trace (Cisco)
vines Vines Trace (Banyan)
<cr>
```

### ▼ ВНИМАНИЕ

Использование trace для протоколов IPX и AppleTalk приведет к сообщению об ошибке, уведомляющему о неподдерживаемой команде. Поддержку этих протоколов предполагается реализовать в ближайшем будущем.

Команда trace показывает количество участков, пройденных пакетом по пути к удаленному хосту. Пример использования команды:

```
Todd2509#trace2501b
Type escape sequence to abort.
(для прерывания введите escape-последовательность)
Tracing the route to 2501b.lammle.com (172.16.10.2)

 1 2501b.lammle.com (172.16.10.2) 16 msec * 16 msec
Todd2509#
```

В нашем примере пакет до точки назначения прошел один участок.

## Упражнение

---

Ответьте на следующие вопросы:

1. Какая команда копирует Cisco IOS на хост TFTP?
2. Какая команда копирует файл startup-config из устройства Cisco на хост TFTP?
3. Какая команда копирует файл startup-config в DRAM?
4. Какая устаревшая команда служит для копирования файла startup-config в DRAM?
5. Какая команда выводит IP-адрес соседнего маршрутизатора в приглашении ввода команд?
6. Какая команда выводит имя хоста, локальный интерфейс, платформу и удаленный порт соседнего маршрутизатора?
7. Какая клавиатурная комбинация служит для одновременного доступа по Telnet к нескольким устройствам?
8. Какая команда выводит сведения об активных соединениях по Telnet с соседними и удаленными устройствами?
9. Какая команда служит для обновления Cisco IOS?
10. Какая команда создаст в таблице хостов запись для имени Bob, которому присвоены IP-адреса 172.16.10.1 и 172.16.20.2?

## Лабораторные работы

---

Для выполнения лабораторных работ потребуется хотя бы один маршрутизатор (лучше иметь несколько) и хотя бы один ПК, действующий в режиме хоста TFTP.

### ▼ СОВЕТУЕМ

Продукт RouterSim, доступный по адресу [www.routersim.com](http://www.routersim.com), может выполнить все предложенные в этой главе лабораторные работы.

### О Лабораторная работа 7.1.

#### *Резервное копирование /OS маршрутизатора*

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, указав en или enable.
2. Проверьте сетевое соединение с хостом TFTP, протестировав его IP-адрес программой Ping с консоли маршрутизатора.
3. Введите show flash для показа содержимого флэш-памяти.

4. Введите **show version** в приглашении привилегированного режима маршрутизатора, чтобы получить имя исполняемой маршрутизатором текущей системы IOS. Если во флэш-памяти только один файл, команды **show flash** и **show version** покажут один и тот же файл. Команда **show version** демонстрирует текущий исполняемый файл, а команда **show flash** — все файлы во флэш-памяти.
5. Убедившись в хорошем соединении Ethernet с хостом TFTP и выяснив имя файла IOS, выполните архивирование IOS. Введите команду **copy flash tftp**. Команда предписывает маршрутизатору скопировать содержимое флэш-памяти (где по умолчанию хранится IOS) на хост TFTP.
6. Введите IP-адрес хоста TFTP и имя исходного файла IOS. Файл будет скопирован и сохранен в каталоге по умолчанию на хосте TFTP.

## О Лабораторная работа 7.2.

### *Обновление или восстановление IOS в маршрутизаторе*

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, указав **en** или **enable**.
2. Проверьте подключение к хосту TFTP тестированием программой Ping IP-адреса хоста с консоли маршрутизатора.
3. Проверив, что есть хорошее соединение Ethernet с хостом TFTP, введите команду **copy tftp flash**.
4. Подтвердите, что знаете об отключении маршрутизатора на время восстановления или обновления. Выберите нужный ответ в выведенном приглашении на консоли маршрутизатора.
5. Введите IP-адрес хоста TFTP.
6. Введите имя файла IOS, который обновляется или восстанавливается.
7. Подтвердите стирание содержимого флэш-памяти.
8. Не пугайтесь стирания IOS из флэш-памяти — в нее будет записана новая система IOS.

Если удалить файл из флэш-памяти и не скопировать в нее новую версию, маршрутизатор загрузится в режиме монитора ROM. Нужно будет выяснить причину того, почему не прошло копирование.

## О Лабораторная работа 7.3.

### *Резервное копирование конфигурации маршрутизатора*

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, указав **en** или **enable**.

2. Проверьте по Ping соединение с хостом TFTP, чтобы гарантировать успешность связи по протоколу IP.
3. В маршрутизаторе B введите `copy run tftp`.
4. Введите IP-адрес хоста TFTP (например, 172.16.30.2) и нажмите Enter.
5. Маршрутизатор запросит имя файла. Имя хоста маршрутизатора стоит после префикса `config` (но не `config`). Допускается любое имя.  
Name of configuration file to write [RouterB-config]?  
**Press enter to accept the default name**  
(имя файла конфигурации для записи.  
Нажмите Enter для использования имени по умолчанию)  
Write file RouterB-config on host 172.16.30.2? [confirm] Press enter  
(Нажмите Enter для записи файла RouterB-config на хост 172.16.30.2)  
Символы !! являются подтверждениями протокола UDP об успешной пересылке файла.

## О Лабораторная работа 7.4.

### Использование протокола CDP

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, указав `en` или `enable`.
2. В маршрутизаторе введите `sh cdp` и нажмите Enter. Нужна гарантия, что пакеты CDP будут посланы во все активные интерфейсы, причем через каждые 60 с при времени удержания 180 с (это значения по умолчанию).
3. Для установки частоты обновления CDP в значение 90 с, введите `cdp timer 90` в режиме глобального конфигурирования.  
RouterC#**config t**  
Enter configuration commands, one per line. End with CNTL/Z.  
RouterC(config)#**cdp timer ?**  
<5-900> Rate at which CDP packets are sent (in sec)  
RouterC(config)#**cdp timer 90**
4. Проверьте в привилегированном режиме изменение таймера частоты CDP командой `show cdp`.  
RouteC#**sh cdp**  
Global CDP information:  
Sending CDP packets every 90 seconds  
Sending a holdtime value of 180 seconds
5. Используйте CDP для сбора информации о соседних маршрутизаторах. Список доступных команд можно получить, введя `sh cdp ?`.  
RouterC#**sh cdp ?**  
entry Information for specific neighbor entry

```
interface CDP interface status and configuration
neighbors CDP neighbor entries
traffic CDP statistics
<cr>
```

6. Введите **sh cdp int** для вывода сведений об интерфейсе и используемом им методе инкапсуляции по умолчанию, а также информации о таймерах CDP.
7. Введите **sh cdp entry \*** для вывода сведений CDP, полученных от всех маршрутизаторов.
8. Задайте **show cdp neighbor** для сбора информации о всех подключенных соседях (следует знать о смысле отдельных полей листинга этой команды).
9. Введите **show cdp neighbor detail**. Будет получен тот же самый листинг, что и с помощью команды **show cdp entry \***.

## О Лабораторная работа 7.5.

### Использование Telnet

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, указав **en** или **enable**.
2. С маршрутизатора А подключитесь по Telnet к удаленному маршрутизатору, указав в командном приглашении **telnet ip\_address**.
3. Введите в маршрутизаторе В IP-адрес из командного приглашения маршрутизатора А. Маршрутизатор автоматически попытается подключиться по Telnet к указанному IP-адресу. Можно ввести команду **telnet** или сразу указать IP-адрес.
4. В маршрутизаторе В нажмите **Ctrl+Shift+6**, а затем **X** для возвращения в командное приглашение маршрутизатора А. Обратитесь по Telnet к третьему маршрутизатору с именем С. Нажмите **Ctrl+Shift+6**, а затем **X** для возвращения в маршрутизатор А.
5. В маршрутизаторе А введите **show sessions**. Будут показаны два сеанса. Для перехода в один из них следует ввести указанный слева номер сеанса и дважды нажать **Enter**. Звездочкой помечен сеанс по умолчанию. Для перехода в этот сеанс дважды нажмите **Enter**.
6. Перейдите в сеанс с маршрутизатором В. Введите **show user**. Будут показаны консольное и удаленное подключения. Команда **disconnect** позволит очистить сеанс. Кроме того, можно ввести **exit** в приглашении для закрытия сеанса с маршрутизатором В.
7. Перейдите в консольный порт маршрутизатора С, введя на первом маршрутизаторе команду **show sessions** и используя номер подключения для возвращения в сеанс с маршрутизатором С. Введите **show user** и убедитесь в подключении к первому маршрутизатору А.
8. Введите **clear line** для закрытия сеанса Telnet.

## О Лабораторная работа 7.6.

### Разрешение имен хостов

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, указав **en** или **enable**.
2. В маршрутизаторе А введите **todd** и нажмите Enter в командном приглашении. Обратите внимание на полученную ошибку и задержку перед ее выводом. Маршрутизатор попытался разрешить имя хоста в IP-адрес за счет обращения к серверу DNS. Можно отключить этот режим командой `no ip domain-lookup` в режиме глобального конфигурирования.
3. Для построения таблицы хостов воспользуйтесь командой `ip host`. В маршрутизаторе А добавьте элементы таблицы хостов для маршрутизаторов В и С, указав команды:

```
ip host routerb ip_address
ip host routerc ip_address
```

Например:

```
ip host routerb 172.16.20.2
ip host routerc 172.16.40.2
```

4. Проверьте таблицу хостов, введя **ping riuterb** в командном приглашении (но не приглашении `config`).

```
RouterA#pingrouterb
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.20.2,
```

```
timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/ avg/max = 4/4/4 ms
```

5. Проверьте таблицу хостов, введя **ping routerc**.

```
RouterA#pingrouterc
```

```
Введите escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.16.40.2,
```

```
timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/ avg/max = 4/6/8 ms
```

6. Сохранив открытым сеанс с маршрутизатором В, вернитесь в маршрутизатор А. Нажмите **Ctrl+Shift+6**, затем **X**.
7. Обратитесь по Telnet к маршрутизатору С, введя в командном приглашении `routerc`.
8. Вернитесь в маршрутизатор А и сохраните открытым сеанс с маршрутизатором С. Нажмите **Ctrl+Shift+6**, затем **X**.
9. Выведите таблицу хостов, указав **show hosts** и нажав Enter.

```
Default domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255
Host Flags Age Type
Address(es)
routerb (perm, OK) 0 IP
172.16.20.2
routerc (perm, OK) 0 IP
172.16.40.2
```

## Проверочные вопросы

1. Какая команда покажет имена хостов, разрешаемые в IP-адреса самим маршрутизатором?
  - A. sh router
  - B. sho hosts**
  - C. sh ip hosts
  - D. sho name resolution
2. Какая команда копирует IOS на резервный хост в сети?
  - A. transfer IOS to 172.16.10.1
  - B. copy run start**
  - C. copy tftp flash
  - D. copy start tftp
  - E. copy flash tftp
3. Какая команда копирует конфигурацию маршрутизатора с хоста TFTP в память NVRAM?
  - A. transfer IOS to 172.16.10.1
  - B. copy run start**
  - C. copy tftp startup
  - D. copy tftp run
  - E. copy flash tftp
4. Какие две команды позволят скопировать по сети конфигурацию с хоста TFTP в память DRAM маршрутизатора Cisco?
  - A. config netw**
  - B. config mem**
  - C. config term
  - D. copy tftp run
  - E. copy tftp start
5. Какая память маршрутизатора Cisco хранит буферы пакетов и таблицы маршрутизации?

- A.** Флэш
  - B.** RAM
  - C.** ROM
  - D.** NVRAM
6. Какая команда создает таблицу хостов в маршрутизаторе Cisco?
- A.** bob ip host 172.16.10.1
  - B.** host 172.16.10.1 bob
  - C.** ip host bob 172.16.10.1 172.16.10.2
  - D.** host bob 172.16.10.1
7. Какая команда покажет соединения маршрутизатора с удаленными устройствами?
- A.** sh sess
  - B.** sh users
  - C.** disconnect
  - D.** clear line
8. Какая команда покажет интерфейсы маршрутизатора, где разрешен протокол CDP?
- A.** sh cdp
  - B.** sh cdp interface
  - C.** sh interface
  - D.** sh cdp traffic
9. Каковы по умолчанию в протоколе CDP интервал таймера обновления и время удержания?
- A.** 240, 90
  - B.** 90, 240
  - C.** 180, 60
  - D.** 60, 180
10. Какая команда скопирует конфигурацию из памяти DRAM маршрутизатора Cisco на хост TFTP в сети?
- A.** config netw
  - B.** config mem
  - C.** config term
  - D.** copy run tftp
  - E.** copy start tftp
11. Какую клавиатурную комбинацию следует использовать для одновременного открытия нескольких сеансов Telnet?
- A.** Tab+пробел
  - B.** Ctrl+X, затем 6
  - C.** Ctrl+Shift+X, затем 6
  - D.** Ctrl+Shift+6, затем X

12. Какая команда выводит те же данные, что и show cdp neighbors detail?
  - A. show cdp
  - B. show cdp ?
  - C. sh cdp neigh
  - D. sh cdp entry \*
13. Что выполняется командой cdp timer 90 do?
  - A. Показ частоты обновления пакетов CDP
  - B. Изменение частоты обновления пакетов CDP
  - C. Установка для команды neighbor протокола CDP длины в 90 строк
  - D. Изменение времени удержания пакетов CDP
14. Какая команда запрещает CDP в определенном интерфейсе?
  - A. no cdp run
  - B. no cdp enable
  - C. no cdp
  - D. disable cdp
15. Какая команда служит для поиска пути пакетов через объединенную сеть?
  - A. ping
  - B. trace
  - C. RIP
  - D. SAP
16. Какие две команды используются для тестирования в сети соединений по протоколу IP?
  - A. ping
  - B. trace
  - C. RIP
  - D. SAP
17. Какая команда очистит подключение к удаленному маршрутизатору?
  - A. clear connection
  - B. clear line
  - C. disconnect
  - D. clear user
18. Какая команда очистит подключение VTU к данному маршрутизатору?
  - A. clear connection
  - B. clear line #
  - C. disconnect
  - D. clear user

19. Что покажет команда `show cdp neighbor` в маршрутизаторе Cisco? (Укажите все правильные ответы.)
- A. IP-адрес соседа
  - B. Локальный порт/интерфейс
  - C. Такую же информацию, что и команда `show version`
  - D. Возможности системы
  - E. Ту же информацию, что и команда `show cdp entry *`
  - F. Идентификатор удаленного порта
  - G. Идентификатор соседнего устройства
  - H. Время удержания
  - I. Аппаратную платформу
  - J. Скорость линии
20. Какая команда копирует новую IOS в маршрутизатор?
- A. `copy tftp run`
  - B. `copy tftp flash`
  - C. `copy tftp start`
  - D. `copy flash tftp`
  - E. `boot system flash IOS_name`

## Ответы к упражнению

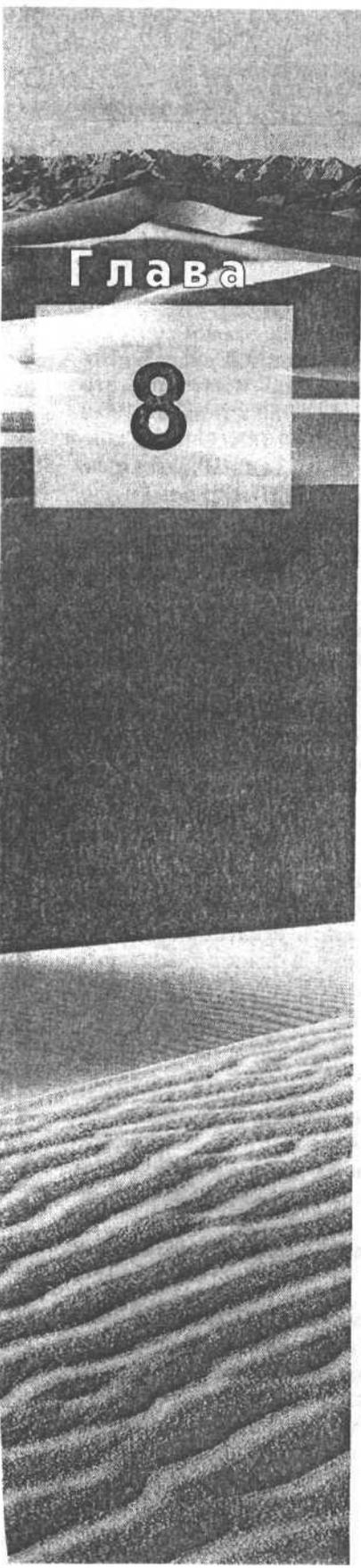
---

1. `copy flash tftp`
2. `copy start tftp`
3. `copy start run`
4. `config mem`
5. `show cdp neighbor detail` or `show cdp entry *`
6. `show cdp neighbor`
7. `Ctrl+Shift+6`, затем X
8. `show sessions`
9. `copy tftp flash`
10. `ip host bob 172.16.10.1 172.16.20.2`

## Ответы на проверочные вопросы

1. B
2. E
3. C
4. A, D
5. B
6. C
7. A
8. B
9. D
10. D
11. D
12. D
13. B
14. B
15. B
16. A, B
17. C
18. B
19. B, D, F, G, H, I
20. B





Глава

8

## Конфигурация сетей Novell IPX

**М**ногие сетевые администраторы когда-нибудь сталкиваются с IPX. На это есть две причины. Во-первых, в операционной системе Novell NetWare протокол IPX используется по умолчанию. Во-вторых, это был наиболее популярный сетевой протокол в конце 80-х и начале 90-х годов. В результате были установлены миллионы сетей IPX. Однако компания Novell в NetWare 5 перешла на протоколы стека TCP/IP, хотя и сохранила поддержку IPX. Зачем нужны два протокола? Нужно помнить о многочисленных установленных клиентах и серверах IPX. Было бы неправильным сразу удалить поддержку устаревшего коммуникационного протокола.

Учитывая широкое распространение IPX, не удивительно, что в Cisco IOS реализована полноценная поддержка крупных сетей IPX. Однако для полного использования всех возможностей и функций Novell IPX, нужно изменить обработку и управление адресами, поскольку в IPX это реализовано иначе, чем в TCP/IP. Рассмотрим основные концепции IPX, чтобы успешно конфигурировать этот протокол в Cisco IOS, а затем обсудим вопросы мониторинга трафика по протоколу IPX.

## Введение в Novell IPX

Протокол Novell IPX (Internetwork Packet Exchange — протокол межсетевого обмена пакетами) появился в начале 80-х годов. Он похож на протокол XNS (Xerox Network Systems), разработанный в исследовательском центре фирмы Хероx в Пало-Альто в 60-е годы, а имеет сходство с TCP/IP. В действительности IPX представляет собой семейство протоколов для связи по телефонным сетям.

## Стек протоколов Novell IPX

Стек протоколов IPX не полностью соответствует модели OSI, однако его протоколы подразделяются по уровням. Разработчики IPX уделяли основное внимание производительности, не заботясь о строгом соответствии существующим стандартам и моделям. Тем не менее можно провести некоторые параллели между IPX и моделью OSI.

На рис. 8.1 показано соответствие протоколов, уровней и функций в IPX и в модели OSI.

IPX Протокол IPX соответствует уровням 3 и 4 модели OSI. Он управляет присваиванием адресов IPX отдельным узлам (программная адресация), доставкой пакетов по сети, а также выбирает оптимальный маршрут на основании информации, полученной от протоколов маршрутизации (RIP или NLSP). IPX является протоколом без подключения (подобно протоколу UDP из семейства TCP/IP), т.е. в нем не требуется подтверждение



Рис. 8.1. Стек протоколов IPX и модель OSI

того, что переданные пакеты были приняты целевым узлом. Для связи с протоколами более высоких уровней в IPX применяются сокет. Они выполняют те же функции адресации нескольких независимых приложений, запущенных на одной машине, что и порты в TCP/IP.

**SPX** SPX (Sequence Packet eXchange — протокол последовательного обмена пакетами) добавляет к функциям протокола IPX ориентацию на подключение. С помощью него протоколы более высокого уровня могут проверять доставку данных от исходного узла целевому. SPX создает между машинами виртуальные соединения, при этом каждому из них присваивается идентификатор соединения, указываемый в заголовке IPX.

**RIP** RIP (Routing Information Protocol — протокол информации о маршрутизации) представляет собой протокол маршрутизации по алгоритму вектора расстояния, применяемый для выбора маршрутов IPX между сетями. При выборе оптимального маршрута применяются такие единицы времени, как "тики" (tick, 1 тик = 1/18 с), и такие показатели, как *число транзитных участков* (число маршрутизаторов между двумя узлами).

**SAP** SAP (Service Advertising Protocol — протокол объявления о службах) служит для объявления о службах и обращения к ним. Серверы применяют этот протокол для объявления о предоставляемых ими службах, а клиенты — для установки расположения сетевых служб.

**NLSP** NLSP (NetWare Link Services Protocol — протокол служб связи NetWare) — это разработанный фирмой Novell протокол маршрутизации по состоянию связи с дополнительными возможностями. Он предназначен для замены протоколов RIP и SAP.

**NCP** NCP (NetWare Core Protocol — основной протокол NetWare) обеспечивает клиентам доступ к ресурсам сервера и выполняет такие функции, как доступ к файлам, печать, синхронизация и безопасность.

Мы перечислили протоколы маршрутизации — транспортные, прикладные и прочие — с целью показать читателю, что IPX может поддерживать действительно большие сети, в которых выполняется много приложений. Понимание механизма работы протоколов облегчает администратору работу в сетях IPX с устройствами других фирм (такими, как маршрутизаторы Cisco).

## Связь между клиентом и сервером

Novell NetWare строго придерживается клиент/серверной модели (без совмещения этих функций): каждый узел NetWare является либо клиентом, либо сервером. В сетях NetWare нет машин, которые бы одновременно предоставляли и использовали сетевые ресурсы, т. е. нет одноранговых связей. Клиентами NetWare могут быть машины, работающие под управлением операционных систем MacOS, DOS, MS Windows, Windows NT, OS/2, Unix и VMS. Серверы работают под управлением Novell NetWare. Серверы NetWare выступают по отношению к клиентам как:

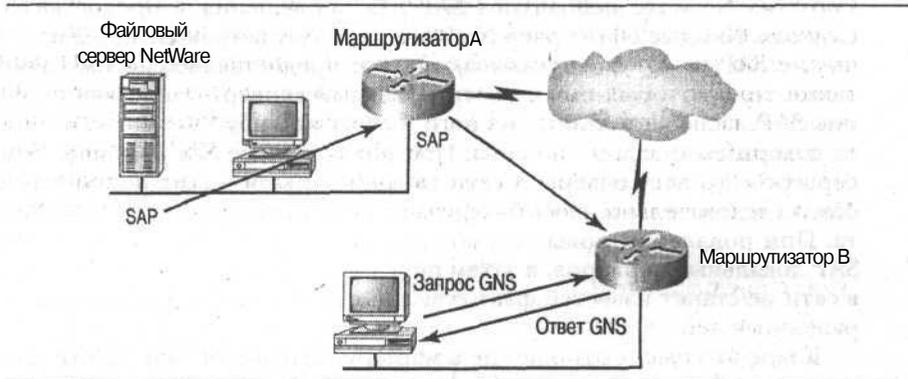
- серверы файлов
- серверы печати
- серверы сообщений
- серверы приложений
- серверы баз данных

Клиенты NetWare определяют расположение всех сетевых ресурсов с помощью серверов. Каждый сервер NetWare генерирует таблицу SAP, в которой перечисляются все сетевые ресурсы, известные серверу (способ создания такой таблицы описан ниже). Когда клиенту требуется доступ к тому или иному ресурсу, он выдает широковещательное сообщение IPX, называемое GNS (запрос GetNearestServer — найти ближайший сервер). С помощью этого запроса клиент определяет местоположение сервера NetWare, который и предоставляет ему нужный ресурс. В свою очередь сервер, получивший запрос GNS, ищет в своей таблице SAP сервер NetWare, удовлетворяющий запросу, а затем посылает клиенту другое сообщение GNS (ответное сообщение GetNearestServer). В нем указывается сервер, к которому следует обратиться для предоставления нужного ресурса. Если ни один из серверов, получивших GNS клиента, не предоставляет запрошенную службу сам и не содержит в таблице SAP информацию о сервере, который может это сделать, то серверы просто не отвечают на запрос, так что клиент не может получить доступ к ресурсу.

Это важно знать, потому что маршрутизаторы Cisco тоже генерируют таблицы SAP и могут отвечать на запросы клиентов точно так же, как и серверы NetWare. Это не означает, что маршрутизаторы Cisco *предоставляют* клиентам ресурсы, как серверы NetWare, — просто ответы маршрутизаторов Cisco на запросы GNS идентичны ответам серверов NetWare.

Клиент может получить ответное сообщение **GetNearestServer** от локального сервера NetWare, удаленного сервера NetWare или от маршрутизатора Cisco, причем локальные серверы NetWare, если они есть, должны ответить на запрос.

Если же их нет, на запрос GNS клиента может ответить локальный маршрутизатор Cisco, соединяющий сегмент, в котором находится клиент, с другими сегментами сети IPX. В этом случае клиенту не приходится ждать ответа от удаленных серверов NetWare. Есть и еще одно преимущество: пропадает необходимость в обмене сообщениями GNS между клиентами сегмента без локального сервера NetWare и удаленными серверами NetWare, снижающем пропускную способность сети (см. рис. 8.2).



**РИС. 8.2.** Удаленные клиенты IPX в сети без сервера

На рисунке изображены клиентские рабочие станции в удаленном офисе фирмы: для работы этим станциям необходим доступ к ресурсам серверов, расположенных в главном офисе. В этом случае маршрутизатор А может отвечать на запросы GNS клиентов сам, пользуясь своей таблицей SAP, а не пересылать их серверам в главный офис по глобальной сети. При этом клиенты никогда не обнаружат отсутствия сервера NetWare в своей локальной сети и не почувствуют от этого неудобств.

Этот способ связи освобождает клиента от таких задач, как определение расположения доступных сетевых ресурсов и их отслеживание — их выполнение возложено на сервер. Клиент просто посылает широковещательное сообщение GNS и ждет ответа. Для клиента все ресурсы сети выглядят локальными независимо от их физического расположения в сети.

## Связь между серверами

Связь между двумя серверами NetWare немного сложнее, чем связь между клиентом и сервером. Как уже отмечалось, серверы хранят таблицы всех доступных ресурсов сети независимо от того, являются ли эти ресурсы

локальными или удаленными для сервера. Кроме того, учтите, что любой сервер должен уметь определять расположение любого ресурса в сети.

Серверы обмениваются информацией двух типов, для каждого из которых предусмотрен отдельный протокол: информация о службах передается по протоколу SAP (Service Advertising Protocol), а информация о маршрутизации — по протоколу RIP (Routing Information Protocol).

#### ▼ ОСТОРОЖНО

Не следует смешивать протокол RIP из семейства IPX с протоколом RIP из семейства TCP/IP. Это два различных протокола маршрутизации с одинаковыми названиями.

## Протокол SAP

Серверы NetWare используют SAP для оповещения о предоставляемых службах. Каждые 60 с сервер NetWare передает широковещательное сообщение SAP, в котором указываются все предоставляемые им службы, а также те, о которых ему известно. Каждый сервер, получивший сообщение SAP, включает данные из него в свою таблицу SAP, а затем передает ее содержимое дальше по сети. Поскольку данные SAP — общие для всех серверов, то все серверы в сети осведомлены обо всех доступных службах, а следовательно, любой сервер может ответить на запрос GNS клиента. При появлении новых служб сведения о них добавляются в таблицы SAP локальных серверов, а затем передаются дальше, пока всем серверам в сети не станет известен факт существования новой службы и способ обращения к ней.

Какое это имеет отношение к маршрутизаторам Cisco? С SAP маршрутизатор работает точно так же, как серверы NetWare. По умолчанию широковещательное сообщение SAP не передается дальше маршрутизатора Cisco. Маршрутизатор заносит в свою таблицу SAP все сообщения SAP, принятые любыми его интерфейсами IPX, а затем передает ее по сети через все интерфейсы с 60-секундным интервалом до тех пор, пока администратор не изменит параметры настройки — точно так же, как и серверы NetWare. Это очень важно особенно для глобальных сетей. Маршрутизатор изолирует широковещательные сообщения SAP от других сегментов сети и передает вовне только сообщения, содержащие полную информацию о сегменте. Рассмотрим вид широковещательного сообщения SAP в анализаторе Etherpeek.

```

Flags: 0x00
Status: 0x00
Packet Length: 306
Timestamp: 23:48:36.362000 06/28/1998
Ethernet Header
Destination: ff:ff:ff:ff:ff:ff Ethernet Brdcast
Source: 00:80:5f:ad:14:e4
Protocol Type: 81-37 NetWare
IPX - NetWare Protocol
Checksum: 0xffff

```

```

Length: 288
Transport Control:
 Reserved: %0000
 Hop Count: %0000
Packet Type: 4 PEP
Destination Network: 0xcc715b00
Destination Node: ff:ff:ff:ff:ff:ff Ethernet Brdcast
Destination Socket: 0x0452 Service Advertising Protocol
Source Network: 0xcc715b00
Source Node: 00:80:5f:ad:14:e4
Source Socket: 0x0452 Service Advertising Protocol
SAP - Service Advertising Protocol
Operation: 2 NetWare General Service Response
Service Advertising Set #1
 Service Type: 263 NetWare 386
 Service Name:
BORDER3.....
 Network Number: 0x12db8494
 Node Number: 00:00:00:00:00:01
 Socket Number: 0x8104
 Hops to Server: 1
Service Advertising Set #2
 Service Type: 4 File Server
 Service Name:
BORDER3.....
 Network Number: 0x12db8494
 Node Number: 00:00:00:00:00:01
 Socket Number: 0x0451
 Hops to Server: 1
Service Advertising Set #3
 Service Type: 632
 Service Name: BORDER_____
R.S.I@@@@@D.PJ..
 Network Number: 0x12db8494
 Node Number: 00:00:00:00:00:01
 Socket Number: 0x4006
 Hops to Server: 1

```

Это сообщение SAP поступило с сервера NetWare с именем **BORDER3**. Обратите внимание, что в сообщении объявляются четыре различные службы, предоставляемые сервером. Эти службы — т.е. их адреса и данные о сокетах — будут добавлены в таблицы SAP всех устройств этой сети, работающих с IPX (в том числе и наших маршрутизаторов), а затем информация будет передана дальше по объединенной сети.

## Протокол RIP

Обмен информацией RIP между серверами в общих чертах осуществляется так же, как и обмен информацией SAP. Каждый сервер составляет таблицу маршрутизации, в которой перечислены сети, с которыми данный сервер соединен непосредственно, и передает ее по сети в виде широко-вещательного сообщения через все интерфейсы, поддерживающие IPX. Другие серверы получают сообщения RIP и передают в сеть через интерфейсы IPX таблицы RIP для своих сегментов. Информация RIP распространяется по сети до тех пор, пока все серверы и маршрутизаторы не будут осведомлены о межсетевых маршрутах. Сообщения RIP, как и сообщения SAP, генерируются с 60-секундным интервалом. Рассмотрим, как выглядит пакет IPX RIP в анализаторе Etherpeek.

```

Flags: 0x80802.3
Status: 0x00
Packet Length: 94
Timestamp: 15:23:05.642000 06/28/1998
802.3 Header
Destination: ff:ff:ff:ff:ff:ff Ethernet Brdcast
Source: 00:00:0c:8d:5c:9d
LLC Length: 76
802.2 Logical Link Control (LLC) Header
Dest. SAP: 0xe0 NetWare
Source SAP: 0xe0 NetWare Null LSAP
Command: 0x03 Unnumbered Information
IPX - NetWare Protocol
Checksum: 0xffff
Length: 72
Transport Control:
 Reserved: %0000
 Hop Count: %0000
 Packet Type: 1 RIP
Destination Network: 0x00002300
Destination Node: ff:ff:ff:ff:ff:ff Ethernet Brdcast
Destination Socket: 0x0453 Routing Information Protocol
Source Network: 0x00002300
Source Node: 00:00:0c:8d:5c:9d
Source Socket: 0x0453 Routing Information Protocol
RIP - Routing Information Protocol
Operation: 2 Response
Network Number Set #1
Network Number: 0x00005200
Number of Hops: 3
Number of Ticks: 14

```

```
Network Number Set #2
 Network Number: 0x00004100
 Number of Hops: 2
 Number of Ticks: 8
Network Number Set #3
 Network Number: 0x00003200
 Number of Hops: 1
 Number of Ticks: 2
Network Number Set #4
 Network Number: 0x00002200
 Number of Hops: 1
 Number of Ticks: 2
Network Number Set #5
 Network Number: 0x00002100
 Number of Hops: 1
 Number of Ticks: 2
Extra bytes (Padding):
r 72
```

Это очень похоже на пакет IP RIP, только отсутствуют IP-адреса. Вместо них указаны IPX-адреса и номера сетей. В сообщении обновления присутствуют сведения о тиках и участках. Тики определяют количество интервалов времени длиной  $1/18$  секунды, которое потребовалось для достижения удаленной сети. Таким способом протокол IPX оценивает задержку в линии для выбора наилучшего пути.

Маршрутизаторов только три, и этот пакет передается в сеть каждые 60 с — это происходит в большой сети, где число маршрутизаторов измеряется сотнями!

## IPX-адресация

После сложной системы адресации в IP адресация в IPX может показаться очень простой. Схема адресации в IPX отличается рядом свойств, значительно облегчающих понимание и администрирование по сравнению с адресацией в TCP/IP.

IPX-адреса занимают 80 бит данных, или 10 байт. Как и адреса в TCP/IP, они имеют иерархическую структуру и подразделяются на две части: адрес сети и адрес узла. 4 старших *байта* всегда обозначают адрес сети, а 6 младших — адрес узла. В системе адресации IPX нет аналогов классов А, В и С из системы адресации TCP/IP — адрес сети и адрес узла всегда имеют одну и ту же длину. И никаких масок подсети!

Как и адреса сети IP, адреса сети IPX присваиваются администраторами и должны быть уникальными в рамках всей глобальной сети IPX. Адрес узла присваивается автоматически. В большинстве случаев в качестве адреса сети используется MAC-адрес машины. Такая система обладает рядом значительных преимуществ по сравнению с TCP/IP. Во-первых,

поскольку адресация клиентов выполняется динамически (автоматически), администратору не нужно запускать DHCP или вручную устанавливать IPX-адрес каждой отдельной рабочей станции. Во-вторых, так как аппаратный адрес (уровень 2) является частью программного адреса (уровень 3), в IPX отпадает необходимость в эквиваленте протокола ARP из стека TCP/IP.

Как и адреса в TCP/IP, IPX-адреса можно записывать в нескольких форматах. Чаще всего их записывают в шестнадцатеричной форме: например, 00007C80.0000.8609.33E9.

Первые восемь шестнадцатеричных цифр (00007C80) представляют собой адрес сети, а оставшиеся двенадцать (0000.8609.33E9) — адрес узла, который совпадает с MAC-адресом рабочей станции. В сетях IPX принято отбрасывать ведущие нули. Таким образом, приведенный выше адрес сети есть просто адрес IPX-сети 7C80.

Оставшиеся двенадцать шестнадцатеричных разрядов (0000.8609.33E9) представляют собой часть адреса. Здесь определяется узел. Эта часть обычно разделяется на три секции по четыре шестнадцатеричных цифры, которые разделяются точками. Это MAC-адрес рабочей станции.

## Инкапсуляция

*Инкапсуляция, или кадрование*, — это процесс формирования кадров из пакетов, поступающих от протоколов более высокого уровня, для передачи их по сети. Напомним, что кадры относятся к уровню 2 модели OSI. В IPX инкапсуляция — это процесс преобразования датаграмм IPX (уровень 3) в кадры (уровень 2) для передачи по одному из поддерживаемых носителей. Мы рассмотрим инкапсуляцию IPX для следующих типов физических сетей:

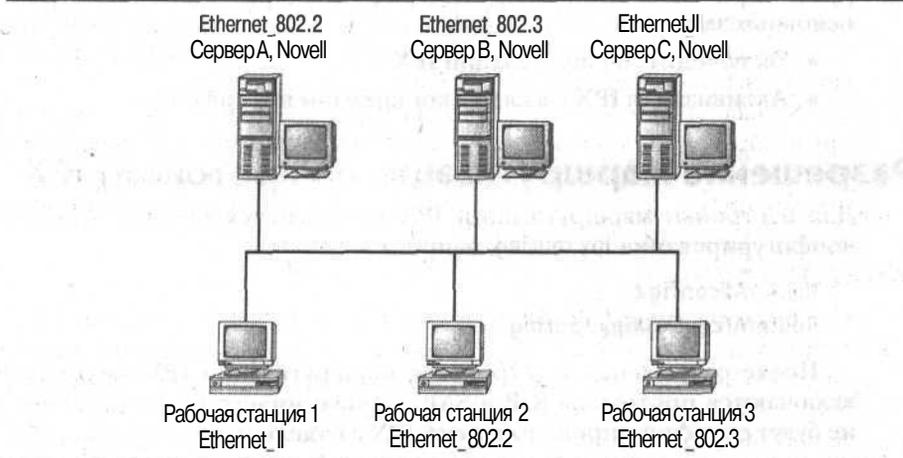
- Ethernet
- Token Ring
- FDDI

Почему это важно? Потому что NetWare поддерживает для одного и того же носителя несколько различных методов инкапсуляции, *несовместимых* между собой. Например, для Ethernet в NetWare существует четыре различных *типа кадров*, из которых можно выбрать наиболее подходящий (см. табл. 8.1), и ни один из этих типов несовместим с другими. Предположим, что на серверах сети применяется Ethernet\_802.2, а на клиентских машинах — Ethernet\_II. Если клиенты и серверы обмениваются данными через маршрутизатор, поддерживающий оба типа кадров, то все работает нормально. Если же это не так, то обмен информацией невозможен. При настройке любых сетевых устройств IPX (в том числе и маршрутизаторов) к выбору типа кадра следует подойти со всей ответственностью.

В некоторых случаях — но далеко не всегда — целесообразно поддерживать несколько типов кадров в рамках одной и той же сети. Пример такой конфигурации приведен на рис. 8.3.

**Таблица 8.1.**  
**Типы кадров Novell для Ethernet**

Тип кадра NetWare	Характеристики
Ethernet_802.3	Принят по умолчанию в NetWare версии 3.11 и более ранних
Ethernet_802.2	Принят по умолчанию в NetWare начиная с версии 3.12
Ethernet_II	Поддерживает TCP/IP и IPX
Ethernet_SNAP	AppleTalk, IPX и TCP/IP



**Рис. 8.3.** Несколько типов кадров в одном сегменте Ethernet

Заметим, что каждому типу кадра на рис. 8.3 соответствует уникальный адрес сети IPX. Даже если все компьютеры относятся к одному сегменту Ethernet, в этом примере существуют три *виртуальных* сети IPX и, следовательно, три уникальных адреса сети IPX. Каждая сеть выполняет через 60 секунд широковещательные рассылки по всей объединенной сети.

Рабочая станция 1 может обмениваться данными только с сервером С, на котором также установлен тип кадра Ethernet II. Рабочая станция 2 может обмениваться данными только с сервером А, а рабочая станция 3 — только с сервером В. Для того чтобы *любая* рабочая станция могла обращаться к любому серверу, следует просто установить маршрутизатор, поддерживающий все три типа кадров. При этом любая станция сможет работать со всеми тремя серверами, но маршрутизатор должен будет выполнять маршрутизацию всех пакетов для серверов и клиентов с различными типами кадров. Конечно, лучше иметь в объединенной сети один тип кадров (802.2). Однако NetWare 5 исполняет "родной" протокол IP, поэтому все наши рассуждения верны только для случая, когда в сети необходимо поддерживать устаревшие серверы.

При настройке маршрутизатора администратор должен знать тип кадра и адрес сети IPX для каждого сегмента, который будет подключен к маршрутизатору. Для получения этой информации после регистрации введите **config** с консоли сервера NetWare.

## Активизация IPX в маршрутизаторах Cisco

После усвоения основ IPX перейдем к вопросам настройки IPX на маршрутизаторе. Активизация IPX в маршрутизаторах Cisco состоит из двух основных задач:

- Включение маршрутизации IPX
- Активизация IPX в каждом конкретном интерфейсе

### Разрешение маршрутизации по протоколу IPX

Для настройки маршрутизации IPX используется команда глобального конфигурирования `ipx routing`, например:

```
RouterA#config t
RouterA(config)#ipx routing
```

После разрешения в устройстве маршрутизации IPX автоматически включаются протоколы RIP и SAP. Однако ничего не произойдет, пока не будут сконфигурированы адреса IPX в отдельных интерфейсах.

### Разрешение IPX в определенном интерфейсе

После разрешения в устройстве маршрутизации IPX следует включить IPX в интерфейсах. Для этого необходимо перейти в режим настройки и ввести команду:

```
ipx network номер [encapsulation тип-инкапсуляции] [secondary]
```

Параметры команды:

**номер** Сетевой адрес IPX.

**[encapsulation тип инкапсуляции]** Необязателен. В таблице 8.2 показаны типы инкапсуляции по умолчанию для различных носителей.

**[secondary]** Указывает дополнительную инкапсуляцию (тип кадра) и сетевой адрес в том же интерфейсе.

Пример настройки IPX в маршрутизаторе 2501A:

```
2501A#config t
2501A(config)#ipx routing
2501A(config)#int e0
2501A(config-if)#ipx network 10
```

Достаточно указать сетевой номер — остальное выполняется автоматически. IPX — жизнеспособный протокол маршрутизации, поскольку все данные отправляет в широковещательных **рассылках**. Однако это создает проблемы в крупных объединенных сетях.

Какой же тип кадра будет использован в интерфейсе Ethernet 0 маршрутизатора 2501A? По умолчанию установлен тип кадра Novell-Ether (802.3). Для изменения типа кадра или добавления другого типа во время настройки интерфейса используется команда `encapsulation`. В таблице 8.2 показаны типы инкапсуляции (типы кадров), поддерживаемые IPX.

**Таблица 8.2.**  
**Типы кадров Novell IPX**

Тип интерфейса	Тип кадра Novell	Ключевое слово Cisco
Ethernet	Ethernet_802.3	novell-ether (по умолчанию)
	Ethernet_802.2	sap
	Ethernet_II	arpa
	Ethernet_snap	snap
Token Ring	Token-Ring	sap (по умолчанию)
	Token-Ring_snap	snap
FDDI	Fddi_snap	snap (по умолчанию)
	Fddi_802.2	sap
	Fddi_raw	novell-fddi

Для установки в Ethernet 0 устройства 2501A типа кадра IPX, равного `sap(802.2)`, введите команду `encapsulation` со следующими параметрами:

```
2501A#config t
2501A(config)#int e0
2501A(config-if)#ipxnetwork 10 encapsulationsap
```

Изменится текущий номер сети и установленная ранее инкапсуляция с типом кадра 802.2. Если требуется добавить несколько типов кадров, следует применить команду `secondary`, указав ее в конце командной строки, либо сформировать подинтерфейс (`subinterface`). Оба способа рассмотрены ниже.

Для настройки маршрутизатора Cisco в существующей объединенной сети IPX необходимо знать сетевой адрес IPX и тип кадра. Эти сведения выводятся на экране "config" сервера NetWare. При установке типа инкапсуляции в маршрутизаторе проверьте, что указано ключевое слово Cisco, а не тип кадра Novell.

## Настройка объединенной сети на протокол IPX

Перед началом настройки устройств Cisco на маршрутизацию IPX рекомендуется еще раз проанализировать объединенную сеть. На рис. 8.4 показаны четыре маршрутизатора, а также используемые схемы адресации IP и IPX.

Для всех сегментов сети установлены сетевые номера IPX. Сетевые номера IP совпадают с номерами подсетей IP. Помните, что адресация IPX никак не связана с адресацией IP, а номера подсетей IP используются в качестве номеров сетей IPX только для упрощения работы администратора.

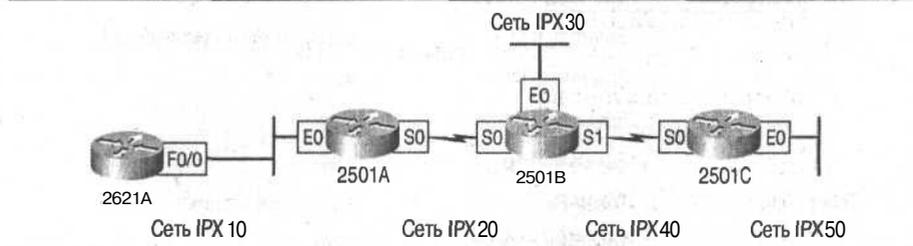


Рис. 8.4. Объединенная сеть

Начнем настройку сети с добавления типа кадра Novell-Ether (802.3) во все сети объединенной сети Ethernet. Это инкапсуляция по умолчанию, поэтому настройка не будет сложной. Инкапсуляцией по умолчанию для последовательных линий связи является HDLC (см. главу 10).

### Настройка IPX в маршрутизаторе 2621A

Для настройки IPX в маршрутизаторе 2621A нужно сначала включить маршрутизацию IPX командой глобального конфигурирования `ipx routing`, а затем указать интерфейсу FastEthernet 0/0 сеть IPX с номером 10.

Пример настройки 2621A:

```
2621A(config)#ipxrouting
2621A(config)#int f0/0
2621A(config-if)#ipxnetwork 10
```

Теперь маршрутизатор 2621A будет перенаправлять трафик IPX через интерфейс FastEthernet 0/0 с помощью сети IPX номер 10.

### Настройка IPX в маршрутизаторе 2501A

В маршрутизаторе 2501A нужна та же команда, что и в маршрутизаторе 2621A. Однако маршрутизатор 2501A имеет два подключения к объединенной сети: интерфейс Ethernet 0 для сети IPX номер 10 и интерфейс serial 0 для сети IPX номер 20.

Пример настройки маршрутизатора 2501A:

```
2501A(config)#ipx routing
2501A(config)#int e0
2501A(config-if)#ipxnetwork 10
2501A(config-if)#int s0
2501A(config-if)#ipxnetwork 20
```

Настройка IPX в маршрутизаторе 2501A оказалась проще настройки IP.

## Настройка IPX в маршрутизаторе 2501B

Для настройки маршрутизации IPX в устройстве 2501B нужно сконфигурировать три интерфейса: Ethernet 0 в сети 30, serial 0 в сети IPX номер 20 и int serial 1 в сети 40.

Пример настройки маршрутизатора 2501B:

```
2501B(config)#ipx routing
2501B(config)#int e0
2501B(config-if)#ipxnetwork 30
2501B(config-if)#int s0
2501B(config-if)#ipxnetwork 20
2501B(config-if)#int s1
2501B(config-if)#ipxnetwork 40
```

Этого хватает для настройки IPX в маршрутизаторе 2501B.

## Настройка IPX в маршрутизаторе 2501C

Для настройки маршрутизации IPX в устройстве 2501C нужно сконфигурировать два интерфейса: Ethernet 0 в сети IPX номер 50 и serial 0 в сети IPX номер 40.

Пример настройки в маршрутизаторе 2501C:

```
2501C(config)#ipx routing
2501C(config)#int e0
2501C(config-if)#ipxnetwork 50
2501C(config-if)#int s0
2501C(config-if)#ipxnetwork 40
```

Настроены и работают все четыре маршрутизатора. Проверить это позволит команда `show ipx route`.

## Проверка таблиц маршрутизации IPX

Для просмотра таблицы маршрутизации IPX служит команда `show ipx route`. Как и для протокола IP, маршрутизатор IPX по умолчанию "знает" только о непосредственно подключенных сетях. Однако после включения

маршрутизации IPX (как в показанном выше примере настройки), во всех маршрутизаторах автоматически запускается протокол RIP стека IPX.

Протокол RIP стека IPX найдет в объединенной сети все сети IPX и обновит таблицы маршрутизаторов. Посмотрим, что произойдет с таблицами маршрутизации IPX во всех устройствах нашего примера.

## 2621A

Маршрутизатор 2621A подключен только к сети IPX номер 10, поэтому IPX RIP добавит в таблицу маршрутизации четыре других сети IPX.

Таблица маршрутизации устройства 2621A:

```
2621A#sh ipx route
```

Codes: C - Connected primary network, c - Connected secondary network  
(коды: C - подключенная основная сеть, c - подключенная дополнительная сеть)

[листинг сокращен]

5 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

(всего 5 путей IPX. Допускается до 1 параллельного пути и до 16 участков)

No default route known.

(пути по умолчанию неизвестны)

```
C 10 (NOVELL-ETHER), Fa0/0
R 20 [07/01] via 10.0000.0c8d.3a7b, 16s, Fa0/0
R 30 [07/02] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 40 [07/02] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 50 [13/03] via 10.0000.0c8d.3a7c, 17s, Fa0/0
```

```
2621A#
```

Буква C означает непосредственно подключенную сеть IPX, а R — сети IPX, найденные по протоколу RIP. Значение [07/01] указывает тики и участки для достижения удаленной сети.

## 2501A

Маршрутизатор 2501A "знает" только о сетях IPX номер 10 и 20, которые подключены непосредственно. IPX RIP уведомит маршрутизатор 2501A о сетях 30, 40 и 50. Таблица маршрутизации в устройстве 2501A:

```
2501A#sh ipx route
```

Codes: C - Connected primary network, c - Connected secondary network

[листинг сокращен]

5 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

```
C 20 (HDLC), Se0
C 10 (NOVELL-ETHER), Et0
R 30 [13/02] via 20.0000.0c8d.2b8c, 16s, Se0
R 40 [07/02] via 20.0000.0c8d.2b8c, 17s, Se0
R 50 [07/03] via 20.0000.0c8d.2b8c, 17s, Se0
```

```
2501A#
```

В показанной таблице маршрутизации отмечены две непосредственно подключенные сети и три сети, найденные RIP. В таблице маршрутизации записаны адреса IPX интерфейсов соседей, а также интерфейсов самого маршрутизатора, которые используются для обращения к удаленной сети.

## 2501B

Пути, найденные IPX RIP для маршрутизатора 2501B, ведут к сетям 10 и 20. Пример листинга из маршрутизатора 2501B:

```
2501B#sh ipx route
```

```
Codes: C - Connected primary network, c - Connected secondary network
```

```
[листинг сокращен]
```

```
5 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.
```

```
No default route known.
```

```
C 20 (HDLC), Se0
C 40 (HDLC), Se1
C 30 (NOVELL-ETHER), Et0
R 10 [07/01] via 20.0000.0c8d.3d8e, 16s, Se0
R 50 [07/01] via 40.0000.0c8d.5c9d, 17s, Se1
```

```
2501B#
```

## 2501C

Для маршрутизатора 2501C протокол RIP стека IPX найдет сети 10, 20 и 30. Пример листинга из маршрутизатора 2501C:

```
2501C#sh ipx route
```

```
Codes: C - Connected primary network, c - Connected secondary network
```

```
[листинг сокращен]
```

```
5 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.
```

```
No default route known.
```

```
C 40 (HDLC), Se0
C 50 (NOVELL-ETHER), Et0
R 10 [13/02] via 40.0000.0c8d.5c9d, 16s, Se0
R 20 [07/01] via 40.0000.0c8d.5c9d, 17s, Se0
R 30 [07/01] via 40.0000.0c8d.5c9d, 17s, Se0
```

```
2501C#
```

## Добавление дополнительных адресов

В примере нашей объединенной сети типом кадра Ethernet является Novell-Ether (802.3). Мы не использовали команду encapsulation, поэтому применяется тип кадра по умолчанию.

Обсудим, как настроить три остальные типа кадра, поддерживаемые в сетях Ethernet. Эту операцию не обязательно выполнять в производственной сетевой среде. Более того, лучше вообще этого не делать. Однако

вам следует знать о такой настройке, поскольку она необходима в определенных сетевых конфигурациях.

Для настройки нескольких типов кадров в одной локальной сети можно использовать команду `secondary` или создать подинтерфейс. Не существует никаких функциональных отличий между этими двумя способами. Единственное связано только с самим процессом администрирования сети.

## Настройка дополнительного адреса

Для настройки дополнительного адреса в локальной сети Ethernet и поддержки нескольких типов кадров служит команда `ipx network` с параметром `secondary`, находящимся в конце этой команды.

Пример добавления дополнительной сети для подключения Ethernet в устройстве 2501A:

```
2501A#config t
Enter configuration commands, one per line. End with CNTL/Z.
2501A(config)#int e0
2501A(config-if)#ipxnetwork 10a encaps sap sec
```

Если не указать в конце команды `ipx network` параметр `secondary`, то будет заменена существующая запись о сети (можно пользоваться краткой формой `епсар` или `sec` вместо `encapsulation` и `secondary`).

Важно понять, что каждый тип кадра обязан иметь отличающийся номер сети IPX. Обратите внимание на 10a в показанном выше примере. Тип кадра 802.3 уже использует сеть 10, поэтому этот номер нельзя указать для типа кадра 802.2.

## Подинтерфейс

Для определения номеров сетей IPX в интерфейсе маршрутизатора, поддерживающего несколько сетей, вместо команды `secondary` можно пользоваться подинтерфейсом. Таким образом с помощью одного физического интерфейса можно поддерживать работу нескольких логических сетей IPX. Каждый подинтерфейс, как и дополнительный интерфейс, обязан иметь уникальный сетевой номер IPX и уникальный тип инкапсуляции.

Для определения интерфейса служит команда `interface ethernet port.number`. Можно использовать номера из диапазона от e0.0 до e0.4292967295. Рассмотрим пример добавления типа кадра 802.2:

```
2621A(config)#int e0.10
2621A(config-subif)#ipxnetwork 10a encaps sap
2621A(config-subif)#^Z
2621A#
```

Как уже упомянуто выше, в объединенной IPX сети не существует функциональных отличий между командами `secondary` и `subinterface`. Их выбор определяется администратором сети. Можно создать подинтерфейс вместо дополнительного интерфейса для усиления

административного контроля. В подинтерфейсе можно вводить команды, а это усиливает точность управления подинтерфейсом и его сетью. Если же пользоваться дополнительным интерфейсом, то сеть стоит "выше" физического интерфейса, поэтому любое изменение в нем действует на все подключенные к интерфейсу сети.

## Настройка в объединенной сети нескольких типов кадров Ethernet

Этот процесс обычно не требуется проводить в производственных сетях, кроме случаев, когда необходима поддержка клиентов, не способных работать с типом кадров 802.2, и необходимо обеспечить поддержку кадров 802.3. Помните, что в хороших сетях IPX используется только один тип кадров.

Однако администратору нужно знать о различных типах кадров и способах их настройки. В этом разделе книги рассматривается процесс настройки объединенной сети на все допустимые типы кадров локальных сетей Ethernet. Однако такая конфигурация в производственной сети будет неэффективной.

Важно понять, что настройка такого рода выполняется только в интерфейсах локальной сети и не используется для кадров локальной сети в интерфейсах региональных сетей.

## Настройка нескольких типов кадров в маршрутизаторе 2621A

Для настройки в маршрутизаторе 2621A нескольких типов кадров следует добавить три новых сетевых номера IPX, по одному для каждого добавляемого типа кадра. Во время настройки на режим поддержки нескольких типов кадров рекомендуется дополнить номер сети буквой. В нашем примере используется номер 10a для 802.2, 10b для Ethernet\_II и 10c для SNAP.

В показанной ниже конфигурации мы создадим в каждом маршрутизаторе один дополнительный адрес и два подинтерфейса. Сделать это можно любым способом.

Рассмотрим конфигурацию устройства 2621A. При вводе команды `ipx network 10a encaps` с вопросительным знаком мы увидим все поддерживаемые типы инкапсуляции и ключевые слова Cisco.

```
2621A(config)#int f0/0
2621A(config-if)#ipxnetwork 10a encaps ?
 arpa Novell Ethernet_II
 hdlc . HDLC on serial links
 novell-ether Novell Ethernet_802.3
 novell-fdi Novell FDDI RAW
 sap IEEE 802.2 on Ethernet FDDI, Token Ring
```

```

snap IEEE 802.2 SNAP on Ethernet Token Ring, and FDDI
RouterA(config-if)#ipx network 10a encaps sap sec

```

После настройки дополнительного адреса нужно добавить два подинтерфейса. Если создавать такую конфигурацию для производственной сети, где необходима поддержка нескольких типов кадров, следует использовать только подинтерфейсы без дополнительных сетей. Cisco не собирается в будущем поддерживать команду `secondary`. Эта команда показана в примерах только для того, чтобы продемонстрировать дополнительные возможности настройки.

Номер подинтерфейса может быть любым числом, что и показано ниже на экране справки (`int fO/0.?`). Номер подинтерфейса действует локально и никак не влияет на работу IPX в объединенной сети.

```

2621A(config)#int f0/0.?
<0-4294967295> Ethernet interface number
2621A(config)#int f0/0.10
2621A(config-subif)#ipx network 10b encaps arpa
2621A(config)#int f0/0.100
2621A(config-subif)#ipx network 10c encaps snap

```

В интерфейсе FastEthernet O/O маршрутизатора 2621 сконфигурированы все четыре типа кадров. Любое устройство, взаимодействующее с маршрутизатором 2621A по протоколу IPX, обязано пользоваться теми же самыми номерами сетей для каждого установленного типа кадра.

## Настройка нескольких типов кадров в маршрутизаторе 2501A

Чтобы маршрутизатор 2501A смог обратиться по IPX к 2621A, необходимы одинаковые номера сетей IPX для каждого настроенного типа кадров.

Пример конфигурации маршрутизатора 2501A:

```

2501A(config)#int e0
2501A(config-if)#ipx network 10a encaps sap sec
2501A(config-if)#int e0.10
2501A(config-if)#ipx network 10b encaps arpa
2501A(config-if)#int e0.100
2501A(config-if)#ipx network 10c encaps snap

```

В примере использовались одинаковые номера подинтерфейсов, но можно выбрать любые числа. Ниже показан файл `running-config` после настройки маршрутизатора на все четыре типа кадров IPX Ethernet:

```

hostname RouterA
!
ipx маршрутизация 0060.7015.63d6
!

```

```
interface Ethernet0
ipaddress 172.16.10.1 255.255.255.0
ipx network 10
ipx network 10A encapsulation SAP secondary
!
interface Ethernet0.10
ipx network 10B encapsulation ARPA
!
interface Ethernet0.100
ipx network 10C encapsulation SNAP
!
interface Serial0
ip address 172.16.20.1 255.255.255.0
ipx network 20
```

Ниже основного интерфейса Ethernet указаны два сетевых номера IPX: один для типа кадров Novell-Ether (802.3) и один - для SAP (802.2). Типы кадров EthernetII (arpa) и SNAP имеют собственные подинтерфейсы, поэтому не нужно использовать команду secondary.

## Настройка нескольких типов кадров в маршрутизаторе 2501B

Настройка маршрутизатора 2501B выполняется только в интерфейсе Ethernet 0. Сеть IPX номер 30 использует тип кадра 802.3 в основном интерфейсе. Три остальные типа кадра просто добавлены в интерфейс Ethernet 0. Пример конфигурации маршрутизатора 2501B:

```
2501B(config)#int e0
2501B(config-if)#ipxnetwork30aencapsapsec
2501B(config-if)#int e0.30
2501B(config-subif)#ipxnetwork 30b encap arpa
2501B(config-subif)#int e0.300
2501B(config-subif)#ipxnetwork 30c encap snap
```

Теперь маршрутизатор 2501B поддерживает в интерфейсе Ethernet 0 все четыре типа кадров IPX Ethernet. Большая часть полосы пропускания Ethernet будет использоваться впустую.

## Настройка нескольких типов кадров в маршрутизаторе 2501C

Маршрутизатор 2501C имеет только одно подключение к локальной сети — сети IPX номер 50. В ней используется тип кадра 802.3. Настроим в интерфейсе Ethernet 0 три остальные номера сетей IPX.

Пример конфигурации маршрутизатора 2501C:

```

2501C(config)#int e0
2501C(config-if)#ipxnetwork50a encapsap sec
2501C(config-if)#int e0.50
2501C(config-subif)#ipxnetwork 50b encap arpa
2501C(config-subif)#inte0.500
2501C(config-subif)#ipxnetwork50c encapsnap

```

Настроены все четыре маршрутизатора, которые теперь должны работать и поддерживать допустимые типы кадров IPX Ethernet.

Так чем же плохо использование в объединенной сети нескольких типов кадров? Воспользуемся командой `show ipx route`, чтобы найти ответ на поставленный вопрос.

## Проверка таблицы маршрутизации IPX

В предыдущем примере при проверке таблиц маршрутизации IPX мы видели только одно подключение к каждой сети IPX во всех таблицах всех маршрутизаторов. Снова введем команду и сравним результаты (проверьте таблицу маршрутизации IPX в устройстве 2621A, поскольку она совпадает с таблицами остальных маршрутизаторов),

```

2621A#sh ipx route
Codes: C - Connected primary network, c - Connected secondary network
[листинг сокращен]
14 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.
No default route known.
C 10 (NOVELL-ETHER), Fa0/0
C 10A(SAP), Fa0/0
C 10B(ARPA), Fa0/0.10
C 10C(SNAP), Fa0/0.100
R 20 [07/01] via 10.0000.0c8d.3a7b, 16s, Fa0/0
R 30A[07/02] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 30B[07/02] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 30C[07/02] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 30D[07/02] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 40 [07/02] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 50A[13/03] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 50B[13/03] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 50C[13/03] via 10.0000.0c8d.3a7c, 17s, Fa0/0
R 50D[13/03] via 10.0000.0c8d.3a7c, 17s, Fa0/0
2621A#

```

Теперь в таблице маршрутизации присутствуют 14 путей IPX вместо пяти в предыдущем примере. Мы не добавляли новые физические сети. Они появились из-за новой инкапсуляции, добавленной в каждую физическую сеть. Три локальные сети каждые 60 с рассылают уведомления

IPX во все активные интерфейсы. Что же будет, если добавить все типы кадров в 20 маршрутизаторов?

Существует еще одно предостережение при добавлении в локальную сеть нескольких типов кадров — действие протокола SAP. Протокол Service Advertisement Protocol (SAP) каждые 60 с выводит широковещательные рассылки во все активные интерфейсы. Если в локальной сети сконфигурировано несколько типов кадров, такие рассылки отправляются для каждого типа. Вместо одного пакета SAP, мы получим четыре одинаковых пакета. Если же пакетов SAP много, то каждые 60 с будет отправляться по четыре дубля каждого пакета.

## Мониторинг IPX в маршрутизаторе Cisco

После настройки и запуска протокола IPX существует несколько способов проверки и отслеживания работы маршрутизатора. Для этого используются разные команды.

### Show IPX Servers

Эта команда похожа на команду `display servers` операционной системы NetWare. Она выводит на экран содержимое таблицы SAP маршрутизатора Cisco, т.е. в полученном списке должны быть имена всех служб SAP. Помните, что, если в таблице SAP маршрутизатора нет записей об удаленных серверах, локальные клиенты не смогут обратиться к этим серверам. Поэтому, если вы не обнаружили в таблице нужных серверов, тщательно проверьте адреса сети IPX и параметры инкапсуляции.

```
2501A#sho ipx servers
```

```
Codes: S - Static, P - Periodic, E - EIGRP, N - NLSP, H - Holddown, += detail
```

```
9 Total IPX Servers
```

```
Table ordering is based on routing and server info
```

Type	Name	Net	Address	Port	Route	Hops	Itf
P	4 BORDER1	350ED6D2.0000.0000.0001	0001:0451	2/01	1	EtO	
P	4 BORDER3	12DB8494.0000.0000.0001	0001:0451	2/01	1	EtO	
P	107 BORDER1	350ED6D2.0000.0000.0001	8104	2/01	1	EtO	
P	107 BORDER3	12DB8494.0000.0000.0001	8104	2/01	1	EtO	
P	26B BORDER	350ED6D2.0000.0000.0001	0005	2/01	1	EtO	
P	278 BORDER	12DB8494.0000.0000.0001	4006	2/01	1	EtO	
P	278 BORDER	350ED6D2.0000.0000.0001	4006	2/01	1	EtO	
P	3E1 BORDER1	350ED6D2.0000.0000.0001	9056	2/01	1	EtO	
P	3E1 BORDER3	12DB8494.0000.0000.0001	9056	2/01	1	EtO	

В листинге из маршрутизатора показаны все серверы IPX, найденные по объявлениям SAP.

Поле `Type` — это поле типа объявляемой службы SAP (4 для файловой службы и 7 для службы печати). Номера других служб специфичны для приложений, исполняемых сервером NetWare. Поля `Net` и `Address`

определяют внутренние сетевые номера IPX, установленные на каждом сервере. Поле Port идентифицирует приложение верхнего уровня. Номер сокета для протокола NetWare Core Protocol (NCP) равен 451.

## Show IPX Route

Эта команда выводит на экран записи таблицы маршрутизации IPX, известные данному маршрутизатору. Сначала маршрутизатор перечисляет сети, с которыми он соединен непосредственно, а затем сети, о которых он получил информацию после подключения.

```
2501A#sh ipxroute
Codes: C - Connected primary network, c - Connected secondary network,
S - Static, F - Floating static, L - Local (internal), W - IPXWAN, R - RIP, E - EIGRP,
N - NLSP, X - External, A - Aggregate, s - seconds, u - uses
6 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.
No default route known.
C 10 (NOVELL-ETHER), EtO
C 20 (HDLC), SeO
c 10a (sap), EtO
C 10b (ARPA), Et0.10
R 40 [07/01] via 20.00e0.lea9.c418, 13s, SeO
R 50 [13/02] via 20.00e0.lea9.c418, 13s, SeO
RouterA#
```

Строчная буква с в таблице маршрутизации указывает на дополнительную сеть IPX.

## Балансировка нагрузки по протоколу IPX

Если между маршрутизаторами нужно настроить параллельные пути IPX, следует иметь в виду, что по умолчанию Cisco IOS о них не знает. Маршрутизатор знает один путь к целевой точке и отбрасывает информацию об альтернативных параллельных путях с одинаковой стоимостью. В приведенном выше примере это отражено во фразе "up to 1 parallel paths and 16 hops allowed" (допускается до 1 параллельного пути и до 16 участков). Чтобы маршрутизатор "смирился" с тем фактом, что к одной цели может вести несколько путей, следует добавить команду `ipx maximum-paths 2` (можно указать любое число до 512).

Теперь Cisco IOS будет по умолчанию распределять пакеты по параллельным путям. Они будут распределяться по всем равнозначным маршрутам по принципу карусели, вне зависимости от цели. Если же нужно, чтобы все пакеты, пересылаемые на тот или иной целевой компьютер или хост, всегда передавались по одному и тому же пути, используйте команду `IPX per-host-load-share`.

Ниже показан пример команды `ipx maximum-paths`, которая предписывает протоколу IPX RIP выполнять карусельную балансировку нагрузки между двумя путями с одинаковой стоимостью.

```
Router#config t
Router(config)#ipxmaximum-paths 2
Router(config)#^Z
Router#sh ipxroute
Codes: C - Connected primary network, c - Connected
[листинг сокращен]
5 Total IPX routes. Up to 2 parallel paths and 16 hops allowed.
[листинг сокращен]
```

Команда show ipx route показывает, что теперь поддерживаются два параллельных пути.

## Show IPX Traffic

Эта команда выводит на экран обобщенную информацию о количестве и типах пакетов IPX, принятых и отправленных маршрутизатором. Обратите внимание, что она выводит данные о пакетах обновления IPX RIP и SAP.

```
2501A#sh ipx traffic
System Traffic for 0.0000.0000.0001 System-Name: RouterA
Rcvd: 15 total, 0 format errors, 0 checksum errors, 0
bad hop count 0 packets pitched, 15 local destination, 0
multicast
Beast: 10 received, 249 sent
Sent: 255 generated, 0 forwarded
 0 encapsulation failed, 0 no route
SAP: 1 SAP requests, 0 SAP replies, 0 servers
 0 SAP Nearest Name requests, 0 replies
 0 SAP General Name requests, 0 replies
 0 SAP advertisements received, 0 sent
 0 SAP flash updates sent, 0 SAP format errors
RIP: 1 RIP requests, 0 RIP replies, 6 routes
 8 RIP advertisements received, 230 sent
 12 RIP flash updates sent, 0 RIP format errors
Echo: Rcvd 0 requests, 5 replies
 Sent 5 requests, 0 replies
 0 unknown: 0 no socket, 0 filtered, 0 no helper
 0 SAPs throttled, freed NDB len 0
Watchdog:
 0 packets received, 0 replies spoofed
Queue lengths:
 IPX input: 0, SAP 0, RIP 0, GNS 0
 SAP throttling length: 0/(no limit), 0 nets
```

```
pending lost route reply
--More --
```

Команда `show ipx traffic` выводит статистику о получаемой маршрутизатором информации протоколов RIP и SAP стека IPX. Если нужна статистика RIP или SAP, полученная в определенном интерфейсе, используйте команду `show ipx interface` (см. ниже).

## Show IPX Interfaces

Команда `show ipx interfaces` выводит статус интерфейса IPX и сконфигурированные в каждом интерфейсе параметры. Т.е. команда `show ipx interface e0` покажет адрес и тип инкапсуляции IPX для указанного интерфейса. Помните, что эта команда не выводит адрес IPX, хотя показывает адрес IP.

```
2501A#sh ipx int e0
Ethernet0 is up, line protocol is up
 IPX address is 10.0000.0c8d.5c9d, NOVELL-ETHER [up]
 Delay of this IPX network, in ticks is 1 throughput 0 link delay 0
 IPXWAN processing not enabled on this interface.
 IPX SAP update interval is 1 minute(s)
 IPXtype 20 propagation packet forwarding is disabled
 Incoming access list is not set
 Outgoing access list is not set
 IPX helper access list is not set
 SAP GNS processing enabled, delay 0 ms, output filter list is not set
 SAP Input filter list is not set
 SAP Output filter list is not set
 SAP Router filter list is not set
 Input filter list is not set
 Output filter list is not set
 Router filter list is not set
 Netbios Input host access list is not set
 Netbios Input bytes access list is not set
 Netbios Output host access list is not set
 Netbios Output bytes access list is not set
 Updates each 60 seconds, aging multiples RIP: 3 SAP: 3
 SAP interpacket delay is 55 ms, maximum size is 480 bytes
 RIP interpacket delay is 55 ms, maximum size is 432 bytes
--More --
```

В листинге представлена информация протоколов RIP и SAP в определенном интерфейсе. Заметим, что команда `show ipx traffic` выводит информацию RIP и SAP для всего маршрутизатора,

## Show Protocols

Существует еще одна команда для вывода адресов IPX и типов инкапсуляции каждого интерфейса — `show protocols`. Эта команда показывает настроенные в устройстве протоколы маршрутизации и адреса интерфейсов.

Пример `show protocol` в маршрутизаторе 2501A:

```
2501A#sh protocols
```

```
Global values:
```

```
Internet Protocol routing is enabled
```

```
IPX routing is enabled
```

```
Ethernet0 is up, line protocol is up
```

```
Internet address is 172.16.10.1/24
```

```
IPX address is 10.0060.7015.63d6 (NOVELL-ETHER)
```

```
IPX address is 10A.0060.7015.63d6 (SAP)
```

```
Ethernet0.10 is up, line protocol is up
```

```
IPX address is 10B.0060.7015.63d6
```

```
Ethernet0.100 is up, line protocol is up
```

```
IPX address is 10C.0060.7015.63d6
```

```
Serial0 is up, line protocol is up
```

```
Internet address is 172.16.20.1/24
```

```
IPX address is 20.0060.7015.63d6
```

Выведены все адреса сконфигурированных интерфейсов, включая подинтерфейсы. Однако показаны адреса для основного и дополнительного интерфейсов, а также подинтерфейсов. Однако для подинтерфейсов не выводится тип инкапсуляции.

Существуют только две команды для просмотра адресов IPX интерфейса: `show ipx interface` и `show protocols`.

## Debug IPX

Команда `debug ipx` выводит сведения о работе IPX в объединенной сети. Особенность команды состоит в выводе обновлений RIP и SAP стека IPX, но пользоваться командой следует осторожно — она сильно загружает процессор.

Существуют еще две команды для отладки работы IPX: `debug ipx routing activity` и `debug ipx sap activity`:

```
RouterA#debug ipx routing?
```

```
activity IPX RIP routing activity
```

```
events IPX RIP routing events
```

Рассмотрим каждую из них отдельно.

## Debug IPX Routing Activity

Команда `debug ipx routing activity` выводит информацию об обновлениях маршрутизации IPX, которые передаются или принимаются маршрутизатором.

```
RouterA#debug ipx routing act
IPXroutingdebuggingis on
RouterA#
IPXRIP: update from 20.00e0.lea9.c418
 50 in 2 hops, delay 13
 40 in 1 hops, delay 7
IPXRIP: positing full update to 10.ffff.ffff.ffff via
EthernetO (broadcast)
IPXRIP: src=10.0000.0c8d.5c9d, dst=20.ffff.ffff.ffff,
packet sent
 network 50, hops 3, delay 14
 network 40, hops 2, delay 8
 network 30, hops 1, delay 2
 network 20, hops 1, delay 2
 network 10, hops 1, delay 2
```

Для выключения команды следует ввести `undebug all` (краткая форма: `un al`), либо ввести полную команду:

```
RouterA#undebugipx routing act
IPXrouting debugging is off
RouterA#
```

## Debug IPX SAP Activity

Команда `debug ipx sap activity` показывает пакеты SAP стека IPX, которые передаются или принимаются маршрутизатором. Широковещательные рассылки SAP выполняются через 60 с в каждом активном интерфейсе (как и рассылки RIP стека IPX). Каждый пакет SAP выведен в нескольких строках листинга.

В показанном ниже примере две первые строки соответствуют IPX SAP, а четыре остальные строки показывают итоговые сведения о пакетах и подробное описание служб.

```
RouterA#debug ipx sap activity
05:31:18: IPXSAP: positing update to 1111.ffff.ffff.ffff
via EthernetO (broadcast) (full)
02:31:18: IPXSAP: Update type 0x2 len 288 src:1111.00e0.2f5d.bf2e
dest:1111.ffff.ffff.ffff(452)
02:31:18: type 0x7, " MarketingPrint ",
10.0000.0000.0001(451), 2 hops
02:31:18: type 0x4, "SalesFS", 30.0000.0000.0001(451), 2 hops
```

```
02:31:18: type 0x4, "MarketingFS",
30.0000.0000.0001(451), 2 hops
02:31:18: type 0x7, "SalesFS", 50.0000.0000.0001(451), 2 hops
```

Отключить команду debug можно с помощью `undebug all` (краткая форма: `un al`). Либо рекомендуется ввести полную команду:

```
RouterA#undebug ipx sap activity
IPX routing debugging is off
```

## RouterA#IPX Ping

Обратившись по Telnet к удаленному маршрутизатору, либо воспользовавшись командами `show cdp neighbor detail` или `show cdp entry *`, можно узнать IPX адреса соседнего маршрутизатора. Вы сможете проверить его адрес по Ping во время тестирования объединенной сети IPX.

Для проверки из маршрутизатора IPX-адреса по Ping можно использовать обычную или улучшенную программу Ping. Показанная ниже команда введена в маршрутизаторе C и позволяет определить сетевой адрес IPX маршрутизатора B.

```
RouterC#sh cdp entry *
```

```

Device ID: RouterB
Entry address(es):
 IP address: 172.16.40.1
 Novell address: 40.0000.0c8d.5c9d
Platform: cisco 2500, Capabilities: Router
Interface: Serial0, Port ID (outgoing port): Serial1
Holdtime: 155sec
```

Получив адрес IPX маршрутизатора B, можно проверить этот маршрутизатор по Ping. Воспользуемся командой `ping ipx [адрес]`, введенной в приглашении маршрутизатора:

```
RouterC#ping ipx 40.0000.0c8d.5c9d
Sending 5, 100-byte IPX Novell Echoes to 40.0000.0c8d.5c9d, timeout
is 2 seconds:
!!!!
```

Можно использовать улучшенную версию Ping, которая имеет дополнительные возможности в сравнении со стандартной версией.

```
RouterC#ping
Protocol [ip]: ipx
Target IPX address: 40.0000.0c8d.5c9d
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
```

```

Verbose [n]:
NovellStandard Echo [n]:y
Введите escape sequence to abort.
Sending 5, 100-byte IPX Novell Echoes to 40.0000.0c8d.5c9d, timeout
is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max=4/7/12 ms

```

## Упражнение

Ответьте на вопросы о сетях IPX.

1. Напишите команду для просмотра протоколов маршрутизации, сконфигурированных в маршрутизаторе.
2. Напишите команду для разрешения протоколов маршрутизации IPX.
3. Напишите команду для разрешения IPX в отдельном интерфейсе. Настройте в интерфейсе Ethernet 0 сеть IPX номер 11, Token Ring по сети IPX номер 15 и интерфейс serial 0 для сети IPX номер 20.
4. Напишите команду для вывода таблицы маршрутизации IPX.
5. Напишите две команды для вывода адреса IPX интерфейса.
6. Напишите две команды для поиска адреса IPX соседнего устройства.
7. Добавьте тип кадра Ethernet\_II в интерфейс Ethernet 0, но не пользуйтесь подинтерфейсом. Укажите для сети IPX номер На.
8. Добавьте типы кадров 802.2 и SNAP в интерфейс Ethernet 0 с помощью подинтерфейса. Укажите для сетей IPX номер 11b и 11c.
9. Напишите команду для проверки конфигурации IPX.

## Лабораторные работы

В этом разделе книги мы настроим три маршрутизатора 2501 для маршрутизации IPX. В первой лабораторной работе нужно сконфигурировать IPX с типом кадра 802.3, а во второй — настроить несколько типов кадров в одной физической локальной сети. В обеих лабораторных работах используется сеть, показанная на рис. 8.5.

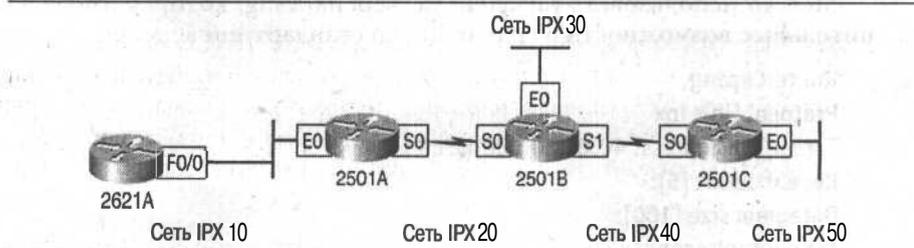


Рис. 8.5. Пример сети IPX

## О Лабораторная работа 8.1. Настройка протокола *Internetworking Packet Exchange (IPX)*

1. Войдите в систему маршрутизатора и перейдите в привилегированный режим, указав команду `en` или `enable`.
2. Введите `show protocol` или `sh prot` для просмотра сконфигурированных протоколов маршрутизации. Будет показан и протокол IP, который настроен в каждом интерфейсе.
3. Разрешите действие протокола маршрутизации IPX командами:

```
RouterA#config t
RouterA(config)#ipx routing
RouterA(config)#^Z
```

4. Еще раз проверьте протоколы маршрутизации, чтобы подтвердить разрешение использования IPX. Для этого введите `sh prot` или `show protocol`. Маршрутизация по IPX разрешена, но интерфейсы пока не имеют адресов IPX — только IP-адреса.
5. Разрешите IPX в отдельных интерфейсах командой `ipx network`. Можно использовать любой номер, длиной до восьми шестнадцатеричных символов (от А до F и от 0 до 9). Пример для маршрутизатора 2501A:

```
2501A#config t
2501A(config)#int e0
2501A(config-if)#ipx network 11
2501A(config-if)#int to0
2501A(config-if)#ipx network 15
2501A(config-if)#int s0
2501A(config-if)#ipx network 20
```

6. Настройте другие маршрутизаторы в лабораторной сети IPX.
7. Проверьте конфигурацию. Лучше всего это сделать командой `show ipx route`.
8. Командами `show protocol command` и `show ipx interface` выведите адреса IPX интерфейса.
9. Узнав адреса IPX соседних маршрутизаторов, проверьте доступ к ним по Ping с помощью протокола IPX (можно перейти в консольный порт соседнего маршрутизатора и использовать команды `show protocol` или `show ipx interface`, либо собрать информацию с помощью протокола CDP и соответствующей команды, например `sh cdp entry *`).

face и `show protocol`

7. Самостоятельно настройте дополнительный интерфейс и подинтерфейсы во всех остальных маршрутизаторах.

10. Командой `ipx maximum-paths` укажите маршрутизатору Cisco на возможность существования нескольких связей с удаленной сетью (по умолчанию протокол IPX ищет только один путь к удаленной сети; если он будет обнаружен, то остальные пути не анализируются, даже если существует второй путь к той же сети).
11. Проверьте введенную команду с помощью `show ipx route`.

## О Лабораторная работа 8.2.

### Добавление в сети IPX дополнительного сетевого

## Проверочные вопросы

- Какой протокол обеспечивает ориентированный на соединения транспорт для протоколов верхнего уровня?
  - IP
  - NLSP
  - SPX
  - NCP
- Кто отвечает на клиентские запросы GNS? (Укажите все правильные ответы)
  - Локальный сервер NetWare
  - Удаленный сервер NetWare
  - Локальный клиент
  - Маршрутизатор Cisco
- Как часто серверы обмениваются информацией RIP и SAP, если явно не указан иной промежуток?
  - Каждые 15 с
  - Каждые 30 с
  - Каждые 60 с
  - Каждые 120 с
- Как сконфигурировать второй подинтерфейс в интерфейсе Ethernet?
  - `Config t, int e0.24010`
  - `Config t, int e0.0`
  - `config t, 24000e0`
  - `config t, 24000 e100`
- Каковы будут сеть и адрес узла IPX для IPX-адреса 71.00A0.2494.E939?
  - Сеть 00a0. Узел 2494 E9S9
  - Сеть 71. Узел 00a0.2494.e939
  - Сеть 00A0.2494. Узел E939
  - Сеть 71 00a0. Узел 2494.e939
- В чем причина того, что клиенты Novell не могут увидеть установленный в сети новый сервер NetWare?
  - Необходимо обновить клиентское программное обеспечение.
  - Необходимо загрузить заплатки для NetWare.
  - Несовпадение типов кадров.
  - Новый сервер NetWare не поддерживает IPX.
- Какой метод допустим для создания нескольких способов инкапсуляции в одном интерфейсе? (Укажите все правильные ответы)

- A. Дополнительные сети.
  - B. Подинтерфейсы.
  - C. Дополнительные физические интерфейсы.
  - D. Невозможно создать несколько способов инкапсуляции в одном интерфейсе.
8. Какая команда покажет полученную в интерфейсе информацию SAP и RIP?
- A. sho ipx route
  - B. sho ipx traffic
  - C. sho ipx interface
  - D. sho ipx servers
9. Какая команда проверяет прослушивание маршрутизатором сервера SAP?
- A. sho ipx route
  - B. sho ipx traffic
  - C. sho ipx interface
  - D. sho ipx servers
10. Какая команда позволяет показать адреса IPX интерфейса? (Укажите все правильные ответы)
- A. sh ipx route
  - B. sh int
  - C. sh prot
  - D. debug ipx int
  - E. show ipx inter
11. Какая команда позволит послать пакеты IPX по нескольким путям?
- A. ipx forward maximum-paths
  - B. ipx maximum-paths
  - C. ipx forward
  - D. ipx forward-paths
12. Какие допустимы имена для инкапсуляции Cisco? (Укажите все правильные ответы)
- A. arpa = IPX Ethernet
  - B. hdlc = HDLC в последовательных линиях
  - C. novell-ether = IPX Ethernet\_802.3
  - D. novell-fddi = IPX Fddi\_Raw
  - E. sap = IEEE 802.2 в Ethernet, FDDI и Token Ring
  - F. snap = IEEE 802.2 SNAP в Ethernet, FDDI и Token Ring
13. Какую команду необходимо ввести для разрешения работы сети IPX?
- A. IPX routing, IPX number, network 790
  - B. IPX routing, int e0, IPX network number 980

- C.** IPX routing, inteO, IPX network 77790 encapsulation arpa  
**D.** IPXrouting, IPXencapsulationSAP, inteO, network789
14. Каков метод инкапсуляции по умолчанию в интерфейсе Ethernet после разрешения поддержки сетей Novell?
- A.** SAP  
**B.** 802.2  
**C.** SNAP  
**D.** Token\_SNAP  
**E.** 802.3  
**F.** Ethernet\_II
15. Какая команда покажет количество тиков для достижения пакетом IPX удаленной сети?
- A.** show ticks  
**B.** show ip route  
**C.** show ipx route  
**D.** show ipx traffic
16. Какой тип инкапсуляции следует выбрать для использования типа кадров 802.2 в интерфейсе Ethernet?
- A.** SNAP  
**B.** 802.2  
**C.** Ethernet\_II  
**D.** SAP  
**E.** Novell-Ether
17. Какую инкапсуляцию следует выбрать для поддержки типа кадров Ethernet\_IIв интерфейсе Ethernet?
- A.** arpa  
**B.** rarpa  
**C.** sap  
**D.** rip  
**E.** snap  
**F.** novell-ether
18. Какая команда покажет протоколы маршрутизации, исполняемые маршрутизатором Cisco ?
- A.** show ipx traffic  
**B.** show ip route  
**C.** show protocols  
**D.** show ipx protocols
19. Какая команда покажет объявления сетевого сервера в сети?
- A.** sh novell  
**B.** sh ipx sap

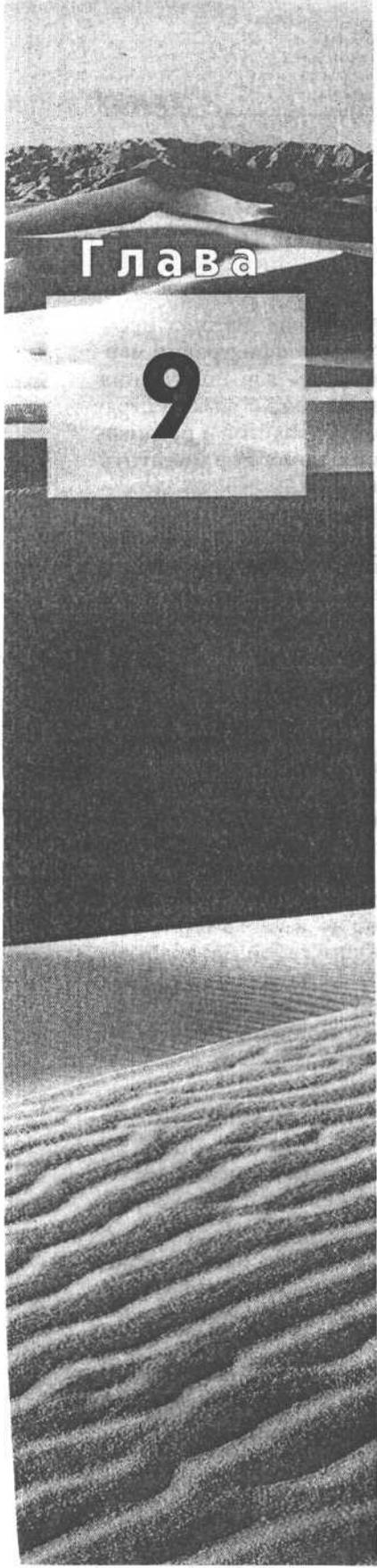
- C. sh ipx servers  
D. sh servers
20. Какая команда установит в маршрутизаторе отправку и получение пакетов RIP в стеке IPX?  
Л. show ip rip  
В. sh ipx int  
С. debug ipx маршрутизация activity  
D. debug ipx interface

## Ответы к упражнению

1. show protocol
2. Config t lpx routing
3. RouterA#**config t**  
Enter configuration commands, one per line  
  
EndwithCNTL/Z.  
RouterA(config)#**int e0**  
RouterA(config-if)#**ipx network 11**  
RouterA(config-if)#**intto0**  
RouterA(config-if)#**ipx network 15**  
RouterA(config-if)#**ints0**  
RouterA(config-if)#**ipx network 20**
4. show ipx route
5. show proto and show ipx int
6. sh cdp nei detail and show cdp entry \*
7. RouterA#**config t**  
RouterA(config)#**inte0**  
RotuerA(config-if)#**ipx network 11a encap arpa sec**
8. RouterA#**config t**  
RouterA(config)#**int e0.10**  
RouterA(config-subif)#**ipx network 11b encap sap**  
RouterA(config-subif)#**int e0.11**  
RouterA(config-subif)#**ipx network 11c encap snap**
9. Sh ipx route  
Sh protocol  
Sh ipx int

## Ответы на проверочные вопросы

- |          |                      |
|----------|----------------------|
| 1. C     | 11. B                |
| 2. A, D  | 12. A, B, C, D, E, F |
| 3. C     | 13. C                |
| 4. A     | 14. E                |
| 5. B     | 15. C                |
| 6. C     | 16. D                |
| 7. A, B  | 17. A                |
| 8. C     | 18. C                |
| 9. D     | 19. C                |
| 10. C, E | 20. C                |



Глава

9

# Управление трафиком с помощью списков доступа

**П**равильное использование и настройка списков доступа несомненно является одной из важнейших задач во время конфигурации маршрутизаторов. В основном эти списки предназначены для повышения эффективности и оптимизации работы сети. С их помощью администратор получает возможность сбора статистики о потоке пакетов и реализованных политиках безопасности. Кроме того, они помогают защитить важные устройства от неавторизованного доступа.

Списки доступа позволяют разрешить (permit) или запретить (deny) движение пакетов через маршрутизатор, доступ по Telnet (VTY) к или из маршрутизатора, а также создавать трафик типа DDR (dial-on demand, вызов по запросу), переключающий обращение к удаленным областям сети.

## Список доступа

Список доступа (access list) — это список условий для управления доступом. Списки управляют доступом к или из сетевого сегмента. Они способны фильтровать пакеты и формировать политики безопасности. При согласованной комбинации списков доступа сетевой администратор получает мощное средство реализации практически любой политики, которую можно вообразить.

Списки доступа IP и IPX действуют одинаково — они фильтруют пакеты, сравнивают их между собой, классифицируют по категориям и воздействуют на обработку пакетов. После создания списка, он может быть применен как к входному, так и к выходному трафику любого интерфейса. Применение списка доступа приводит к началу анализа маршрутизатором каждого пакета, проходящего через соответствующий интерфейс в определенном направлении, и к выполнению установленных списком действий над пакетами.

Существует несколько важных правил, используемых во время сравнения пакета со списком доступа:

- Сравнение выполняется последовательно со всеми строками списка, т.е. начинается со строки 1, затем пакет сравнивается со строкой 2, затем со строкой 3 и т.д.
- Сравнение выполняется до первого совпадения. Если пакет совпадает с условием в одной из строк списка доступа, над ним выполняется указанное в строке действие, а дальнейшее сравнение прекращается.
- Существует неявное условие "deny" в конце каждого списка доступа — если пакет не совпал со всеми предыдущими строками, этот пакет отбрасывается.

Каждое из правил имеет большое влияние на фильтрацию пакетов IP и IPX.

Для протоколов IP и IPX существуют два типа списков доступа:

**Стандартный список доступа (Standard access list)** Использует для фильтрации пакетов IP только IP-адрес источника. Обычно этот список полностью разрешает или запрещает весь стек протоколов. Стандартные списки IPX допускают фильтрацию по IPX-адресам источника и назначения.

**Улучшенный список доступа (Extended access list)** Проверяются IP-адреса источника и назначения, поле протокола в заголовке сетевого уровня и номер порта в заголовке транспортного уровня. Улучшенный список доступа IPX использует IPX-адреса источника и назначения, поле протокола в заголовке сетевого уровня и номер сокета в заголовке транспортного уровня.

После создания список доступа можно применить к интерфейсу в виде входного (inbound) или выходного (outbound) списка доступа:

**Входной список доступа (Inbound access list)** Пакеты обрабатываются перед маршрутизацией в выходной интерфейс.

**Выходной список доступа (Outbound access list)** Пакеты маршрутизируются в выходной интерфейс, а затем обрабатываются с помощью списка доступа.

Существует несколько рекомендаций по созданию и реализации списков доступа в маршрутизаторе:

- Разрешается присвоить интерфейсу, протоколу или направлению движения пакетов только один список доступа. Следовательно, если созданы списки доступа IP, то в интерфейсе можно иметь только один входной и один выходной список.
- В начало списка лучше помещать наиболее специализированные условия.
- Любая добавляемая строка всегда помещается в конец списка доступа.
- Нельзя удалить из списка доступа одну строку, поскольку будет удален весь список. Рекомендуется скопировать список доступа в текстовый редактор для изменения отдельной строки. Единственным исключением из этого правила являются именованные списки доступа (named access list).
- Если только список доступа не завершится командой permit any, отбрасываются все пакеты, не отвечающие ни одному условию в строках списка доступа. Любой список должен иметь хотя бы один оператор permit, иначе будет полностью блокирован весь интерфейс.
- Созданные списки доступа применяются к интерфейсам. Если к интерфейсу применен не существующий список доступа, то трафик в интерфейсе не фильтруется.

- Списки доступа предназначены для фильтрации трафика, проходящего через маршрутизатор. Они не фильтруют трафик, генерируемый маршрутизатором.
- Стандартный список доступа IP следует размещать по возможности ближе к точке назначения.
- Улучшенный список доступа IP следует размещать по возможности ближе к источнику.

## Стандартный список доступа IP

Стандартный список доступа IP фильтрует сетевой трафик по IP-адресам источника в пакетах протокола IP. Для создания этого списка нужно использовать номера 1 — 99.

Ниже перечислены номера списков доступа для фильтрации в сети. Состав поддерживаемых протоколов зависит от используемой версии IOS.

```
RouterA(config)#access-list?
<1-99> IP standard access list
<100-199> IP extended access list
 (стандартный список доступа IP)
<1000-1099> IPX SAP access list
 (список доступа IPX SAP)
<1100-1199> Extended 48-bit MAC address access list
 (улучшенный список доступа по 48-разрядным
 MAC-адресам)
<1200-1299> IPX summary address access list
 (список доступа по итоговым адресам IPX)
<200-299> Protocol type-code access list
 (список доступа по коду типа протокола)
<300-399> DECnet access list
 (список доступа DECnet)
<400-499> XNS standard access list
 (стандартный список доступа XNS)
<500-599> XNS extended access list
 (улучшенный список доступа XNS)
<600-699> Appletalk access list
 (список доступа AppleTalk)
<700-799> 48-bit MAC address access list
 (Список доступа по 48-разрядным MAC-адресам)
<800-899> IPX Standard access list
 (стандартный список доступа IPX)
<900-999> IPX extended access list
 (улучшенный список доступа IPX)
```

Используя для списка доступа номера из диапазона 1 — 99, мы указываем маршрутизатору на создание стандартного списка доступа IP.

```
RouterA(config)#access-list 10 ?
```

deny	Specify packets to reject (указывает отбрасываемые пакеты)
permit	Specify packets to forward (указывает перенаправляемые пакеты)

После выбора номера для списка доступа нужно определить тип списка: you permit или deny. Пример создания оператора deny:

```
RouterA(config)#access-list 10 deny ?
 Hostname or A.B.C.D Address to match
 any Any source host
 (любой хост-источник)
 host A single host address
 (определенный адрес хоста)
```

Опишем подробно следующую операцию. Вы можете выбрать один из трех вариантов. Команда any запрещает/разрешает любой хост, можно указать IP-адрес для сравнения с определенной сетью или хостом IP, либо применить команду host для указания определенного хоста.

Пример использования команды host:

```
RouterA(config)#access-list 10 deny host 172.16.30.2
```

Мы запретили все пакеты от хоста 172.16.30.2. Командой по умолчанию является host. Для команды access-list 10 deny 172.16.30.2 маршрутизатор предполагает сравнение с адресом хоста 172.16.30.2.

Однако существует иной путь указания хоста — использование заменителей (wildcard, подстановочных символов). По сути, это единственный способ указания в списке доступа сети или подсети.

## Заменители

Заменители служат для указания хоста, сети или части сети в списке доступа. Чтобы понять действие заменителей, нужно разобраться с размером блоков. Размер блока позволяет указать диапазон адресов. Ниже перечислены доступные размеры блоков.

### Размер блока

64  
32  
16  
8  
4

Для указания диапазона адресов выберите ближайший по размерам блок. Например, для указания 34 сетей следует выбрать размер блока 64. Если нужно указать 18 хостов, используйте размер блока 32. Если же определяются только две подсети, подходит размер блока 4.

Заменители используются в адресах хостов и сетей для указания маршрутизатору на диапазон доступных адресов в фильтре. Чтобы определить хост, адрес должен выглядеть так:

```
172.16.30.50.0.0.0
```

Четыре нуля представляют четыре октета в адресе. Если указан ноль, то должно быть точное соответствие с этим октетом в адресе. Для указания произвольного значения в октете служит число 255. Пример определения заменителем всей подсети:

```
172.16.30.00.0.0.255
```

Маршрутизатор будет сравнивать только первые три октета, а в четвертом октете допускается любое значение.

Перейдем к более сложным задачам. Как установить только небольшой диапазон подсетей? Нам поможет размер блока, который позволит указать диапазон значений. Не обязательно указывать 20 сетей по отдельности, достаточно воспользоваться подходящим размером блока. Например, диапазон может быть равен 16 или 32, но не 20.

Предположим, нужен доступ к части сети в диапазоне от 172.16.8.0 до 172.16.15.0. Это блок с размером 8. Номером сети станет 172.16.8.0, а заменителем 0.0.7.255. Значение 7.255 будет использоваться маршрутизатором для определения размера блока. Номер сети и заменитель указывают маршрутизатору начать от 172.16.8.0 и просмотреть в пределах блока из восьми адресов до сети 172.16.15.0.

Вы должны помнить, что заменитель всегда на один номер меньше размера блока. В нашем примере для размера блока 8 потребуется заменитель 7. Для размера блока 16 заменителем станет 15.

Приведем несколько примеров. Ниже показан пример, где маршрутизатор точно сравнивает три первых октета, но четвертый октет может быть произвольным.

```
RouterA(config)#access-list 10 deny 172.16.10.0 0.0.0.255
```

Далее показан маршрутизатор, сравнивающий первые два октета, причем в двух последних октетах могут быть любые значения.

```
RouterA(config)#access-list 10 deny 172.16.0.0 0.0.255.255
```

Теперь обсудим такую строку:

```
RouterA(config)#access-list 10 deny 172.16.16.0 0.0.3.255
```

Маршрутизатор должен начать от сети 172.16.16.0 и использовать размер блока, равный 4. Диапазон адресов: от 172.16.16.0 до 172.16.19.0.

Следующий пример демонстрирует список доступа, начинающий сравнение от 172.16.16.0 и использующий размер блока 8 для получения конца диапазона, равного 172.16.23.0.

```
RouterA(config)#access-list 10 deny 172.16.16.0 0.0.7.255
```

Начнем от сети 172.16.32.0 с размером блока 32 и дойдем до 172.16.63.0:

```
RouterA(config)#access-list 10 deny 172.16.32.0 0.0.31.255
```

Теперь начнем от сети 172.16.64.0 с размером блока 64 и дойдем до 172.16.127.0:

```
RouterA(config)#access-list 10 deny 172.16.64.0 0.0.63.255
```

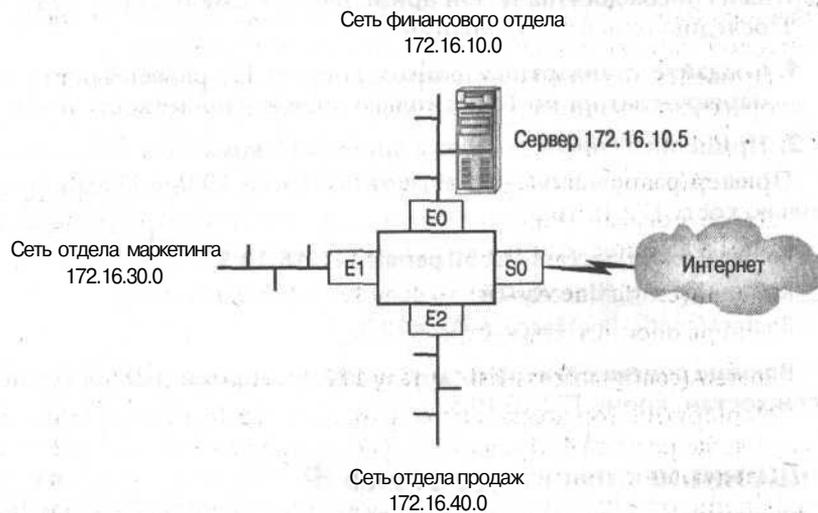
Во время использования заменителей и размеров блока следует помнить о двух правилах:

- Любой блок начинается от 0. Например, нельзя иметь размер блока 8 и начать от 12. Следует использовать 0 — 7, 8 — 15, 16 — 23 и т.д. Для размера блока 32 диапазонами будут 0 — 31, 32 — 63, 64 — 95 и т.д.
- Команда `any` соответствует заменителю 0.0.0.0 255.255.255.255.

### Пример стандартного списка доступа IP

Рассмотрим использование стандартного списка доступа IP для запрещения пользователям доступа к локальной сети финансового отдела компании.

На рис. 9.1 маршрутизатор имеет три подключения к локальным сетям и одно по региональной сети к Интернету. Пользователи локальной сети отдела продаж не должны иметь доступ к локальной сети финансового отдела. Однако у них должен быть доступ к Интернету и сети отдела маркетинга. В сети отдела маркетинга необходимо иметь возможность обращаться к серверу приложений в сети финансового отдела.



**Рис. 9.1.** Пример списка доступа IP для трех локальных и одной региональной сети

К маршрутизатору Асме следует применить стандартный список доступа IP:

```
Асме#config t
Асме(config)#access-list 10 deny 172.16.40.0 0.0.0.255
Асме(config)#access-list 10 permit any
```

Важно понять, что команда `any` аналогична следующей строке:

```
Acme(config)#access-list 10 permit 0.0.0.0 255.255.255.255
```

В данном случае список доступа запрещает локальную сеть Отдела продаж и все остальное. Однако в какое место списка нужно вставить эту строку? Если поместить ее во входной список для E2, то возможно запрещение интерфейса Ethernet, поскольку всем устройствам локальной сети отдела продаж запрещен доступ ко всем сетям, подключенным к маршрутизатору. Лучше вставить нашу строку в выходной список маршрутизатора для интерфейса E0.

```
Acme(config)#inte0
Acme(config-if)#access-group 10 out
```

Сеть 172.16.40.0 не будет доступна вне Ethernet 0, но сможет обращаться к локальной сети отдела маркетинга и к Интернету.

## Управление доступом VTU (Telnet)

Если стоит задача по запрещению доступа пользователей по протоколу Telnet к любому активному порту маршрутизатора, то пришло время заняться управлением VTU. Для решения этой проблемы используется стандартный список доступа IP. Он применяется к самой линии VTU.

Последовательность операций:

1. Создайте стандартный список доступа IP, разрешающий доступ к маршрутизатору по Telnet только определенному хосту или хостам.
2. Примените список доступа к линии VTU командой `access-class`.

Пример разрешения доступа по протоколу Telnet к маршрутизатору только хосту 172.16.10.3:

```
RouterA(config)#access-list 50 permit 172.16.10.3
RouterA(config)#line vty 0 4
RouterA(config-line)#access-class 50 in
```

В конце списка стоит `deny any`, поэтому запрещается доступ по Telnet всем хостам, кроме 172.16.10.3.

## Улучшенные списки доступа IP

В показанном выше примере стандартного списка доступа IP обратите внимание на то, как одним блоком определена вся подсеть для доступа к финансовому отделу. Но что делать, если нужен доступ только к определенному серверу этого отдела, но не ко всем службам сети финансового отдела? Стандартные списки доступа IP не смогут обеспечить доступ пользователей только к определенной сетевой службе, запретив подход к остальным ресурсам. Однако улучшенные списки доступа IP позволяют указать IP-адрес источника или назначения, а также протокол или номер порта, который определяет приложение, либо протокол верхнего уровня.

Рассмотрим пример улучшенного списка доступа IP. Первая из используемых нами команд выведет доступные для списка номера. Для улучшенных списков выделены номера от 100 до 199.

```
RouterA(config)#access-list?
<1-99> IP standard access list
<100-199> IP extended access list
<1000-1099> IPX SAP access list
<1100-1199> Extended 48-bit MAC address access list
<1200-1299> IPX summary address access list
<200-299> Protocol type-code access list
<300-399> DECnet access list
<400-499> XNS standard access list
<500-599> XNS extended access list
<600-699> Appletalk access list
<700-799> 48-bit MAC address access list
<800-899> IPX standard access list
<900-999> IPX extended access list
```

Выберем в улучшенном списке доступа запись deny.

```
RouterA(config)#access-list 110 ?
deny Specify packet
 (определяет пакет)
dynamic Specify a DYNAMIC list of PERMITS or DENYS
 (определяет динамический список для условий PERMIT
 или DENY)
permit Specify packets to forward
 (разрешает перенаправление указанных пакетов)
```

Выбрав тип списка доступа, нужно определиться с полем протокола сетевого уровня. Важно понимать, что если фильтровать сеть на уровне приложений, то можно ввести запись для прохода по всей модели OSI. Например, для фильтрации по Telnet или FTP укажите TCP. Если же выбрать IP, то мы не выйдем за пределы сетевого уровня и не сможем фильтровать данные на уровне приложений.

```
RouterA(config)#access-list 110 deny ?
<0-255> An IP protocol number
eigrp Cisco's EIGRP routing protocol
 (протокол маршрутизации EIGRP от Cisco)
gre Cisco's GRE tunneling
 (туннель GRE от Cisco)
icmp Internet Control Message Protocol
 (протокол управляющих сообщений Интернета)
igmp Internet Gateway Message Protocol
 (протокол сообщений шлюза Интернета)
```

igrp	Cisco's <b>IGRP</b> routing protocol (протокол маршрутизации IGRP от Cisco)
ip	Any Internet Protocol (любой протокол Интернета)
ipinip	<b>IP in IP tunneling</b> (туннель "IP в IP")
nos	<b>KA9Q NOS compatible IP over IP tunneling</b> (туннель KA9Q NOS, совместимый с "IP поверх IP")
ospf	<b>OSPF routing protocol</b> (протокол маршрутизации OSPF)
tcp	Transmission Control Protocol (протокол управления передачей)
udp	User Datagram Protocol (протокол пользовательских датаграмм)

Выбрав фильтрацию на уровне приложений через TCP, мы получим приглашение для ввода IP-адреса источника для хоста или сети. Команда `any` допускает указание любого адреса источника.

**RouterA(config)#access-list 110 deny tcp ?**

A.B.C.D Source address  
 any Any source host  
 host A single source host

Установив адрес источника, следует указать адрес назначения.

**RouterA(config)#access-list 110 deny tcp any ?**

A.B.C.D Destination address  
 any Any destination host  
 (любой адрес назначения)  
 eq Match only packets on a given port number  
 (только пакеты для указанного номера порта)  
 gt Match only packets with a greater port number  
 (только пакеты для порта с номером, большим указанного)  
 host A single destination host  
 (отдельный хост назначения)  
 lt Match only packets with a lower port number  
 (только пакеты для порта с номером, меньшим указанного)  
 neq Match only packets not on a given port number  
 (только пакеты с любым другим номером порта)  
 range Match only packets in the range of port numbers  
 (только пакеты для диапазона портов)

В нашем примере мы запретим любые IP-адреса источника, кроме пакетов с IP-адресом назначения 172.16.30.2.

**RouterA(config)#access-list 110 deny tcp any host 172.16.30.2 ?**

eq Match only packets on a given port number  
 (только пакеты для указанного номера порта)

established	Match established connections (только для установленных подключений)
fragments	Check fragments (проверка фрагментации)
gt	Match only packets with a greater port number (только пакеты для порта с номером, большим указанного)
log	Log matches against this entry (регистрация согласно данной записи)
log-input	Log matches against this entry, including input interface (регистрация согласно данной записи, включая входной интерфейс)
lt	Match only packets with a lower port number (только пакеты для порта с номером, меньшим указанного)
neq	Match only packets not on a given port number (только пакеты для любого другого номера порта)
precedence	Match packets with given precedence value (только пакеты с указанным значением приоритета)
range	Match only packets in the range of port numbers (только пакеты для указанного диапазона номеров портов)
tos	Match packets with given TOS value (только пакеты с указанным значением типа службы)
<cr>	

Нажмем Enter, чтобы не менять список доступа. Однако можно было бы сделать его более специализированным: укажите адрес хоста, дополните его запрещаемым типом службы. Ниже показан пример указания номера порта, приложения и даже имени программы.

```
RouterA(config)#access-list 110 deny tcp any host 172.16.30.2 eq ?
```

<0-65535>	Port number
bgp Border	Gateway Protocol (179) (протокол граничного шлюза)
chargen	Character generator (19) (генератор символов)
and	Remote commands (rcmd, 514) (удаленная команда)
daytime	Daytime (13) (дневное время)
discard	Discard (9) (отменить)
domain	Domain Name Service (53) (служба доменных имен)
echo	Echo (7) (эхо)
exec	Exec (rsh, 512) (исполнение)
finger	Finger (79) (программа Finger)

ftp	File Transfer Protocol (21) (протокол передачи файлов)
ftp-data	FTP data connections (20,21) (подключение данных по FTP)
gopher	Gopher (70) (служба Gopher)
hostname	NIC hostname server (101) (сервер имен хостов сетевого информационного центра)
ident	<b>Ident Protocol</b> (113) (протокол идентификации)
irc	Internet Relay Chat (194) (служба динамического обмена сообщениями Интернета)
klogin	Kerberos login (543) (регистрация по протоколу Kerberos)
kshell	Kerberos shell (544) (оболочка Kerberos)
login	Login ( <b>rlogin</b> , 513) (регистрация, программа rlogin)
lpd	Printer service (515) (служба печати)
nntp	Network News Transport Protocol (119) (транспортный протокол сетевых новостей)
pop2	Post Office Protocol v2 (109) (протокол почтового офиса версии 2)
pop3	Post Office Protocol v3 (110) (протокол почтового офиса версии 3)
smtp	Simple Mail Transport Protocol (25) (упрощенный почтовый транспортный протокол)
sunrpc	Sun Remote Procedure Call (111) (вызов удаленной процедуры по спецификации Sun)
syslog	Syslog (514) (системный журнал)
tacacs	TAC Access Control System (49) (система управления доступом TAC)
talk	Talk (517) (программа Talk)
telnet	Telnet (23) (программа Telnet)
time	Time (37) (программа Time)
uucp	<b>Unix-to-Unix Copy Program</b> (540) (программа копирования Unix-Unix)
whois	<b>Nickname</b> (43) (псевдоним в службе Whois)
www	World Wide Web (HTTP, 80) (служба World Wide Web с протоколом HTTP)

Заблокируйте Telnet (порт 23) только для хоста 172.16.30.2. Если пользователям нужен протокол FTP, то он разрешен. Команда `log` позволит послать сообщение в консоль при любом обращении к списку доступа. Это неудобно в загруженной сетевой среде, но хорошо подходит для управления сетью в школе или дома.

```
RouterA(config)#access-list 110 deny tcp any host 172.16.30.2 eq 23 log
```

Помните, что по умолчанию последней строкой списка является неявная операция `deny any`. Если применить наш список к интерфейсу, он может полностью отключиться, поскольку в конце предполагается неявный оператор `deny all`. Следует завершить список доступа такой командой:

```
RouterA(config)#access-list 110 permit ip any 0.0.0.0 255.255.255.255
```

Помните, что `0.0.0.0 255.255.255.255` аналогичен команде `any`.

Создав список доступа, применим его к интерфейсу. Команда применения не отличается от аналогичной команды для стандартных списков доступа IP:

```
RouterA(config-if)#ip access-group 110 in
```

или

```
RouterA(config-if)#ip access-group 110 out
```

### Пример улучшенного списка доступа IP

Для рис. 9.1 мы уже создали стандартный список доступа IP, но теперь запретим доступ по Telnet и FTP к серверу 172.16.10.5 финансового отдела. Все остальные службы этой локальной сети должны быть открыты для отделов продаж и маркетинга.

Потребуется такой список доступа:

```
Acme#config t
```

```
Acme(config)#access-list 110 deny tcp any host 172.16.10.5 eq 21
```

```
Acme(config)#access-list 110 deny tcp any host 172.16.10.5 eq 23
```

```
Acme(config)#access-list 110 permit ip any any
```

Важно понять, почему запрещение помещено в начало списка. Если сначала установить разрешение, а потом запрещение, то локальная сеть финансового отдела не сможет обращаться к другим локальным сетям и Интернету, поскольку предполагается неявное `deny` в конце списка. Очень трудно создать нужный нам список не так, как показано в примере.

Создав список, применим его к порту Ethernet 0. Дело в том, что трем другим интерфейсам маршрутизатора необходим доступ к локальной сети. Однако если список создавался только для блокирования отдела продаж, то его следует поместить ближе к источнику, либо применить к интерфейсу Ethernet 2.

```
Acme(config-if)#ip access-group 110 out
```

## Мониторинг списков доступа IP

Проверьте конфигурацию маршрутизатора. Для этого используйте команды:

**show access-list** Выводит все списки доступа и их параметры, сконфигурированные в маршрутизаторе. Команда не показывает, для какого интерфейса установлен список.

**show access-list 110** Выводит только параметры для списка доступа 110. Команда не показывает, для какого интерфейса установлен список.

**show ip access-list** Выводит только списки доступа IP, сконфигурированные в маршрутизаторе.

**show ip interface** Показывает, какие интерфейсы имеют списки доступа.

**show running-config** Выводит только списки доступа и интерфейсы, к которым применены эти списки.

## Списки доступа IPX

Списки доступа IPX настраиваются подобно другим спискам доступа. Командой `access-list` формируется список доступа для тестирования пакетов, затем он применяется к интерфейсу с помощью команды `access-group`.

Обсудим такие списки доступа IPX:

**Стандартный список доступа IPX** Фильтрует по IPX-адресам источника и назначения хостов или номерам сетей. Использует номера списков доступа 800 — 899. Стандартный список доступа IPX похож на стандартный список IP, но во втором случае выполняется фильтрация только по IP-адресам источника. Стандартный же список доступа IPX фильтрует по IPX-адресам источника и назначения.

**Улучшенный список доступа IPX** Фильтрует по IPX-адресам источника и назначения хостов или номерам сетей, полю протокола IPX в заголовке сетевого уровня и номеру сокета в заголовке транспортного уровня. Использует номера списков доступа 900 — 999.

**Фильтр SAP стека IPX** Служит для управления трафиком SAP в локальных и региональных сетях. Фильтр SAP стека IPX помечен номерами списков доступа 1000 — 1099. Сетевой администратор может установить список доступа IPX для управления объемом трафика IPX, включая трафик IPX SAP по медленным линиям региональных сетей.

### Стандартный список доступа IPX

Стандартный список доступа IPX устанавливает фильтрацию по адресам источника и назначения хостов IPX или сетевым адресам. Этот список формируется подобно стандартному списку доступа IP. Параметры настройки стандартного списка доступа IPX:

```
access-list 800-899 deny или permit адрес_источника адрес_назначения
```

Заменители могут использоваться в IPX-адресах источника и назначения, однако заменитель \* означает любой хост или любую сеть.

На рис. 9.2 показан пример сети IPX и настройка в ней стандартного списка доступа IPX.

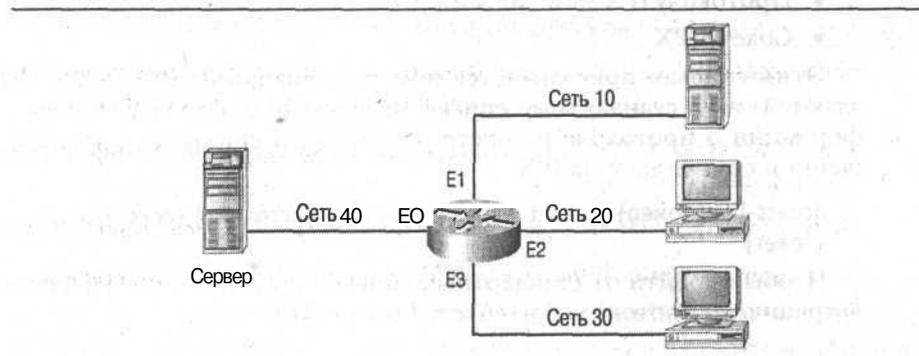


Рис. 9.2. Пример списка доступа IPX

На рис. 9.2 предполагается следующая конфигурация: интерфейс Ethernet 0 к сети 40, интерфейс Ethernet 1 к сети 10, интерфейс Ethernet 2 к сети 20 и интерфейс Ethernet 3 к сети 30.

Покажем создание и применение списка доступа. Список IPX разрешает прохождение пакетов из сети 20 по интерфейсу Ethernet 0 в сеть 40.

```
Router(config)#access-list810 permit 20 40
Router(config)#inte0
Router(config-if)#ipxaccess-group810out
```

Рассмотрим действие этой конфигурации подробнее. Прежде всего любое устройство IPX из сети IPX номер 20 через интерфейс Ethernet 2 может обратиться к серверу сети 40, который подключен к интерфейсу Ethernet 0. Однако далее вы увидите, что сделано одной строкой (но помните о неявном deny all в конце списка):

- Хосты сети 10 не могут обращаться к серверу в сети 40.
- Хосты сети 40 могут обращаться к сети 10, но пакеты не возвращаются обратно.
- Хосты сети 30 могут обращаться к сети 10, а сеть 10 — к сети 30.
- Хосты сети 30 не могут обращаться к серверу в сети 40.
- Хосты сети 40 могут обращаться к хостам сети 30, но ответные пакеты из сети 30 не возвращаются обратно.
- Хосты сети 20 могут обращаться ко всем устройствам объединенной сети.

```
Router filter list is not set
Netbios Input host access list is not set
Netbios Input bytes access list is not set
Netbios Output host access list is not set
Netbios Output bytes access list is not set
```

## Улучшенные списки доступа IPX

336

Глава 9

```
Updates each 60 seconds, aging multiples RIP: 3 SAP: 3
SAP interpacket delay is 55 ms, maximum size is 480 bytes
RIP interpacket delay is 55 ms, maximum size is 432 bytes
```

—More—

Команда `show ipx access-list` показывает два списка доступа IPX из маршрутизатора.

```
Router#sh ipx access-list
IPX access list 810
 permit FFFFFFFF 30
IPXSAP access list 1010
 permit FFFFFFFF 4Sales
Router#
```

Шестнадцатеричные значения F соответствуют всем единицам, т.е. операции `permit any`. Мы использовали -1 в команде IPX, поэтому `run-ning-config` представлена одними F.

## Упражнение

Напишите ответы на следующие вопросы:

1. Настройте стандартный список доступа IP на предотвращение обращений любых компьютеров из сети 172.16.0.0 в сеть Ethernet.
2. Примените список доступа к интерфейсу Ethernet.
3. Создайте список доступа, разрешающий хосту 196.22.15.5 обращение в сеть Ethernet.
4. Напишите команду проверки правильности ввода списка доступа.
5. Напишите две команды для проверки правильности применения списка доступа к интерфейсу Ethernet.
6. Создайте улучшенный список доступа, запрещающий хосту 172.16.10.1 обращение по Telnet через интерфейс Ethernet 0 к хосту 172.16.30.5 в Ethernet 1.
7. Примените список доступа к определенному интерфейсу.
8. Настройте список доступа протокола SAP стека IPX для предотвращения отправки вне Ethernet 0 сообщений SAP из любой файловой службы, кроме службы с IPX-адресом 45.0000.0000.0001.
9. Примените список доступа протокола SAP стека IPX к интерфейсу Ethernet.

## Лабораторные работы

В этом разделе нам предстоит выполнить три лабораторные работы, причем понадобится не менее трех маршрутизаторов серии 2500, либо программный продукт RouterSim.

Все лабораторные работы выполняются в сети, показанной на рис. 9.3.

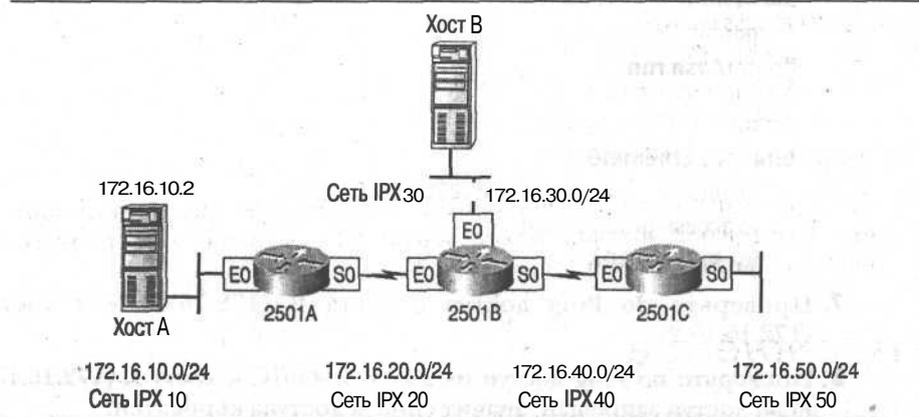


Рис. 9.3. Сеть для работы со списками доступа

### О Лабораторная работа 9.1.

#### Стандартные списки доступа IP

Установите доступ к сети 172.16.10.0 только для хоста В из сети 172.16.30.0.

1. В маршрутизаторе 2501A командой **config t** перейдите в режим глобального конфигурирования.
2. В режиме глобального конфигурирования введите **access-list ?** для получения справки о возможностях списков доступа.
3. Выберите номер для создания стандартного списка доступа IP (число из диапазона от 1 до 99).
4. Разрешите хост 172.16.30.2:

```
2501A(config)#access-list 10 permit 172.16.30.2 ?
A.B.C.D Wildcard bits
<cr>
```

Для указания только хоста 172.16.30.2 используйте заменитель 0.0.0.0:

```
RouterA(config)#access-list 10 permit 172.16.30.2 0.0.0.0
```

5. Создав список доступа, примените его к интерфейсу для активизации:

```
2501A(config)#int e0
2501A(config-if)#ip access-group 10 out
```

6. Проверьте работу списка доступа:

```
RouterA#sh access-list
Standard IP access list 10
 permit 172.16.30.2
RouterA#sh run
-cut-
interface Ethernet0
 ip address 172.16.10.1 255.255.255.0
 ip access-group 10 out
 ipx network 10A
```

7. Проверьте по Ping доступ с хоста В (172.16.30.2) к хосту А (172.16.10.2).
8. Проверьте по Ping доступ из 2501В и 2501С к хосту А (172.16.10.2). Если доступ запрещен, значит список доступа корректен.

## О Лабораторная работа 9.2.

### *Улучшенный список доступа IP*

Воспользуемся улучшенным списком доступа IP для запрещения хосту 172.16.10.2 создания сеанса Telnet с маршрутизатором 2501В (172.16.20.2). Однако этот хост должен обращаться по Ping к маршрутизатору 2501В. Улучшенный список доступа IP следует поместить как можно ближе к источнику, поэтому добавим список в маршрутизатор 2501А.

1. Удалите все списки доступа в 2501А и добавьте улучшенный список в маршрутизатор 2501А.
2. Укажите номер для создания улучшенного списка доступа IP, выбрав число в диапазоне 100 — 199.
3. Воспользуйтесь оператором deny (оператор permit мы добавим в п. 7, чтобы сохранить перенаправление другого трафика).

```
2501A(config)#access-list 110 deny ?
<0-255> An IP protocol number
ahp Authentication Header Protocol
eigrp Cisco's EIGRP routing protocol
esp Encapsulation Security Payload
gre Cisco's GRE tunneling
icmp Internet Control Message Protocol
igmp Internet Gateway Message Protocol
```

igrp	Cisco's IGRP routing protocol
ip	Any Internet Protocol
ipinip	IP in IP tunneling
nos	KA9Q NOS compatible IP over IP tunneling
ospf	OSPF routing protocol
pcp	Payload Compression Protocol
tcp	Transmission Control Protocol
udp	User Datagram Protocol

4. Мы хотим заблокировать Telnet, поэтому выбираем TCP в качестве протокола транспортного уровня:

```
2501A(config)#access-list 110 deny tcp ?
```

A.B.C.D	Source address
any	Any source host
host	A single source host

5. Добавьте фильтруемый IP-адрес источника, а затем IP-адрес назначения для хоста. Используйте команду host вместо заменителя.

```
2501A(config)#access-list 110 deny tcp host 172.16.10.2 host 172.16.20.2 ?
```

ack	Match on the ACK bit
eq	Match only packets on a given port number
established	Match established connections
fin	Match on the FIN bit
fragments	Check fragments
gt	Match only packets with a greater port number
log	Log matches against this entry
log-input	Log matches against this entry, including input interface
lt	Match only packets with a lower port number
neq	Match only packets not on a given port number
precedence	Match packets with given precedence value
psh	Match on the PSH bit
range	Match only packets in the range of port numbers
rst	Match on the RST bit
syn	Match on the SYN bit
tos	Match packets with given TOS value
urg	Match on the URG bit
<cr>	

6. Добавьте команду eq telnet. Включите в конец и команду log, чтобы при любом обращении к строке списка доступа на консоль вывело уведомление.

```
2501A(config)#access-list 110 deny tcp host 172.16.10.2 host 172.16.20.2 eq telnet log
```

7. Не забудьте добавить следующую строку с оператором permit:

```
2501A(config)#access-list 110 permit ip any 0.0.0.0
255.255.255.255
```

8. Создайте оператор permit, поскольку был добавлен оператор deny. Команда permit рассмотрена в предыдущей лабораторной работе.
9. Примените список доступа к интерфейсу Ethernet 0 маршрутизатора 2501A для блокирования трафика Telnet на входе в первый интерфейс маршрутизатора.

```
RouterB(config)#inteO
RouterB(config-if)#ipaccess-group 110in
RouterB(config-if)#^Z
```

10. Проверьте по Telnet доступ с хоста 172.16.10.2 к маршрутизатору B, используя IP-адрес назначения 172.16.20.2. На консоли 2501A генерируется показанное ниже сообщение, однако команда ping должна работать.

```
From host 172.16.10.2:>telnet 172.16.20.2
```

На консоли маршрутизатора B появится сообщение:

```
01:11:48: %SEC-6-IPACCESSLOGP: list 110 denied tcp
172.16.10.2(1030)->172.16.20.2(23), 1 packet
01:13:04: %SEC-6-IPACCESSLOGP: list 110 denied tcp
172.16.10.2(1030)->172.16.20.2(23), 3 packets
```

## О Лабораторная работа 9.3.

### Стандартный список доступа IPX

Настроим IPX для разрешения только трафика IPX из сети IPX с номером 30, но не из сети IPX 50.

1. Удалите все существующие списки доступа в маршрутизаторе 2501A. Стандартный список доступа IPX можно поместить в любое место сети, поскольку фильтрация выполняется как по IPX-адресам источника, так и назначения.
2. Проверьте, что сеть IPX работает согласно рис. 9.3. Командой show ipx route выведите все сети маршрутизатора.
3. Настройте список доступа в 2501A для разрешения только трафика IPX из сети 30 и запрещения доступа из сети IPX номер 50. Для стандартных списков доступа IPX используются номера 800 — 899.

```
2501A#config t
RouterC(config)#access-list 810 ?
deny Specify packets to reject
permit Specify packets to permit
```

4. Сначала запретите сеть IPX номер 50, затем разрешите все остальное. В IPX используется заменитель -1.

```
2501A(config)#access-list 810 deny ?
-1 Any IPX net
<0-FFFFFF> Source net
N.H.H.H Source net.host address
```

5. Укажите сеть 50 в качестве адреса источника:

```
2501A(config)#access-list 810 deny 50
-1 Any IPX net
<0-FFFFFF> Destination net
N.H.H.H Destination net.host address
<cr>
```

6. Укажите сеть 10 в качестве сети назначения:

```
2501A(config)#access-list 810 deny 50 10
```

7. Разрешите все остальное заменителем для IPX:

```
2501A(config)#access-list 810 permit -1 -1
```

8. Примените список к последовательному интерфейсу устройства 2501A для блокирования пакетов, достигших этого маршрутизатора:

```
2501A(config)#int s0
2501A(config-if)#ipx access-group 810 in
2501A(config-if)#^Z
```

9. Проверьте список, проанализировав таблицу маршрутизации IPX. Сеть 50 не должна присутствовать в таблице маршрутизации IPX устройства 2501A. Кроме того, используйте команды `show access-list` и `show ipx access-list` для изменения списка.

## Проверочные вопросы

- По каким критериям запрещается или разрешается пересылка пакетов в стандартном списке доступа IP?
  - Адрес источника
  - Адрес назначения
  - Протокол
  - Порт
- По каким критериям запрещается или разрешается пересылка пакетов в улучшенном списке доступа IP?
  - Адрес источника
  - Адрес назначения
  - Протокол
  - Порт
  - Все перечисленное выше

3. Какой заменитель в маске списка доступа следует использовать для указания всех хостов в сети IP 172.16.0.0 класса B?
  - A. 255.255.0.0
  - B. 255.255.255.0
  - C. 0.0.255.255
  - D. 0.255.255.255
  - E. 0.0.0.255
4. Как правильно указать только хост 172.16.30.55 в списке доступа IP?
  - A. 172.16.30.55 0.0.0.255
  - B. 172.16.30.55 0.0.0.0
  - C. any 172.16.30.55
  - D. host 172.16.30.55
  - E. 0.0.0.0 172.16.30.55
  - F. ip any 172.16.30.55
5. Какой список доступа разрешает только трафик WWW в сеть 196.15.7.0?
  - A. access-list 100 permit tcp any 196.15.7.0 0.0.0.255 eq www
  - B. access-list 10 deny tcp any 196.15.7.0 eq www
  - C. access-list 100 permit 196.15.7.0 0.0.0.255 eq www
  - D. access-list 110 permit ip any 196.15.7.0 0.0.0.255
  - E. access-list 110 permit www 196.15.7.0 0.0.0.255
6. Какая команда покажет порты, к которым применены списки доступа IP?
  - A. show ip port
  - B. show access-list
  - C. show ip interface
  - D. show access-list interface
  - E. show running-config
7. Какой заменитель позволит отфильтровать сети от 172.16.16.0 до 172.16.23.0?
  - A. 172.16.16.0 0.0.255
  - B. 172.16.255.255 255.255.0.0
  - C. 172.16.0.0 0.255.255
  - D. 172.16.16.0 0.8.255
  - E. 172.16.16.0 0.7.255
  - F. 172.16.16.0 0.15.255
8. Каков правильный стандартный список доступа IPX?
  - A. access-list 800 permit 30 50
  - B. access-list 900 permit 30 50

- C. access-list permit all 30 50
  - D. access-list 800 permit 30 50 eq SAP
  - E. access-list 900 permit -1 50
9. Какой заменитель позволит указать сети от 172.16.32.0 до 172.16.63.0?
- A. 172.16.0.0.0.0.255
  - B. 172.16.255.255 0.0.0.0
  - C. 0.0.0.0 255.255.255.255
  - D. 172.16.32.0.0.0.255
  - E. 172.16.32.0.0.0.31
  - F. 172.16.32.0.0.31.255
  - G. 172.16.32.0.31.255.255
  - H. 172.16.32.0 0.0.63.255
10. Какая команда применит список доступа IPX SAP с номером 1050 к входящему трафику, предполагая, что уже сконфигурирован интерфейс?
- A. ipx access-group 1050 in
  - B. ipx input-sap-filter 1050
  - C. ipx access-list 1050 in
  - D. ipx input-sap-filter 1050 in
  - E. ipx access-group 1050
11. Какая команда покажет улучшенный список доступа 187?
- A. sh ip int
  - B. sh ip access-list
  - C. sh access-list 187
  - D. sh access-list 187 extended
12. Каков диапазон номеров для улучшенных списков доступа IP?
- A. 1 – 99
  - B. 200 – 299
  - C. 1000 – 1999
  - D. 100 – 199
13. Какая команда создаст улучшенный список доступа IP?
- A. access-list 101 permit ip host 172.16.30.0 any eq 21
  - B. access-list 101 permit tcp host 172.16.30.0 any eq 21 log
  - C. access-list 101 permit icmp host 172.16.30.0 any ftp log
  - D. access-list 101 permit ip any eq 172.16.30.0 21 log
14. Каков диапазон номеров для улучшенных списков доступа IPX?
- A. 100 – 199
  - B. 900 – 999

**C.** 1000 – 1999

**D.** 700 – 799

- 15.** Что означает -1 в улучшенном списке доступа IPX?
- A.** Запрещение данного хоста
  - B.** Запрещение всех сетей или хостов
  - C.** Локальная сеть без участков
  - D.** Любой хост или любая сеть
- 16.** Какая команда выполняет мониторинг списков доступа IP?
- A.** sh int
  - B.** sh ip interface
  - C.** sh run
  - D.** sh access-list
- 17.** Какая команда должна следовать после команды access-list 110 deny tcp any any eq ftp?
- A.** access-list 110 deny ip any any
  - B.** access-list 110 permit tcp any any
  - C.** access-list 110 permit ip any
  - D.** access-list 110 permit ip any 0.0.0.0 255.255.255.255
- 18.** Какая конфигурация доступа разрешает только трафик из сети 172.16.0.0 в интерфейс int s0?
- A.** Access-list 10 permit 172.16.0.0 0.0.255.255, int s0, ip access-list 10 in
  - B.** Access-group 10 permit 172.16.0.0 0.0.255.255, int s0, ip access-list 10 out
  - C.** Access-list 10 permit 172.16.0.0 0.0.255.255, int s0, ip access-group 10 in
  - D.** Access-list 10 permit 172.16.0.0 0.0.255.255, int s0, ip access-group 10 out
- 19.** Где следует поместить в сети стандартный список доступа?
- A.** Ближе к переключателю
  - B.** Ближе к источнику
  - C.** Ближе к точке назначения
  - D.** В Интернете
- 20.** Где следует поместить в сети улучшенный список доступа?
- A.** Ближе к переключателю
  - B.** Ближе к источнику
  - C.** Ближе к точке назначения
  - D.** В Интернете

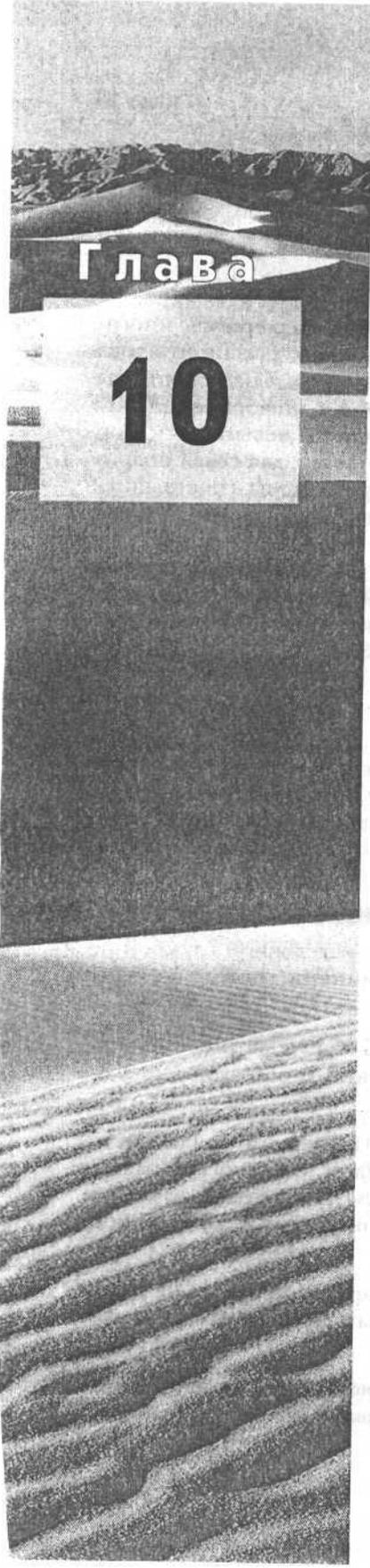
## Ответы к упражнению \_\_\_\_\_

1. access-list 10 deny 172.16.0.0.0.255.255  
access-list 10 permit ip any
2. ip access-group 10 out
3. access-list 10 deny host 196.22.15.5  
access-list 10 permit any
4. show access-list
5. show running-config sh ip interface
6. access-list 110 deny tcp host 172.16.10.1 host 172.16.30.5  
eq 23 access-list 110 permit ip any any
7. Int eO  
IP Access-group 110 in
8. Access-list 1010 permit 45.0000.0000.0001 4
9. Int eO  
ipx input-sap-filter 1010

## Ответы на проверочные вопросы \_\_\_\_\_

- |         |             |
|---------|-------------|
| 1. A    | 11. B, C    |
| 2. E    | 12. D       |
| 3. C    | 13. B       |
| 4. B, D | 14. B       |
| 5. A    | 15. D       |
| 6. C, E | 16. B, C, D |
| 7. E    | 17. D       |
| 8. A    | 18. C       |
| 9. F    | 19. C       |
| 10. B   | 20. B       |





Глава

10

## *Протоколы региональных сетей*

**О**перационная система Cisco IOS способна поддерживать многие протоколы региональных сетей (WAN), что позволяет расширить локальную сеть до сетей в географически удаленных местах. Соединение удаленных подразделений компаний обеспечит обмен информацией, что необходимо в современном бизнесе. Однако было бы невыгодным формировать собственные кабельные сети и подключения для связи подразделений компании. Телекоммуникационные провайдеры (поставщики услуг) предлагают арендовать или совместно использовать уже готовые линии связи, что сохранит время и деньги.

Необходимо понимать типы региональных сетей, поддерживаемые оборудованием Cisco. В этой главе мы не сможем обсудить все типы региональных сетей, поддерживаемые оборудованием Cisco. Подробно рассмотрим протоколы HDLC, PPP, Frame Relay и ISDN.

## Региональные сети

При знакомстве с технологиями региональных сетей нужно знать терминологию и типы подключений отдельных сетей. В этом разделе книги мы расскажем о терминах региональных сетей и типах подключений, обычно предоставляемых провайдерами.

### Определения из области региональных сетей

Перед заключением договора на пользование определенной службой региональной сети важно разобраться с терминами, применяемыми провайдерами.

Оборудование в помещении потребителя (CPE, Customer premises equipment) Оборудование, находящееся в помещении и обслуживаемое самим клиентом.

Демаркационная точка (Demarcation, demarc) *Последняя* точка системы, ответственность за которую несет провайдер. Обычно это разъем RJ-45, находящийся вблизи CPE. Оборудованием CPE в такой точке может быть CSU/DSU или интерфейс ISDN, подключаемый к демаркационной точке.

Локальный отвод (Local loop) Соединение демаркационной точки с ближайшим коммутационным шкафом, обычно называемым центральным офисом.

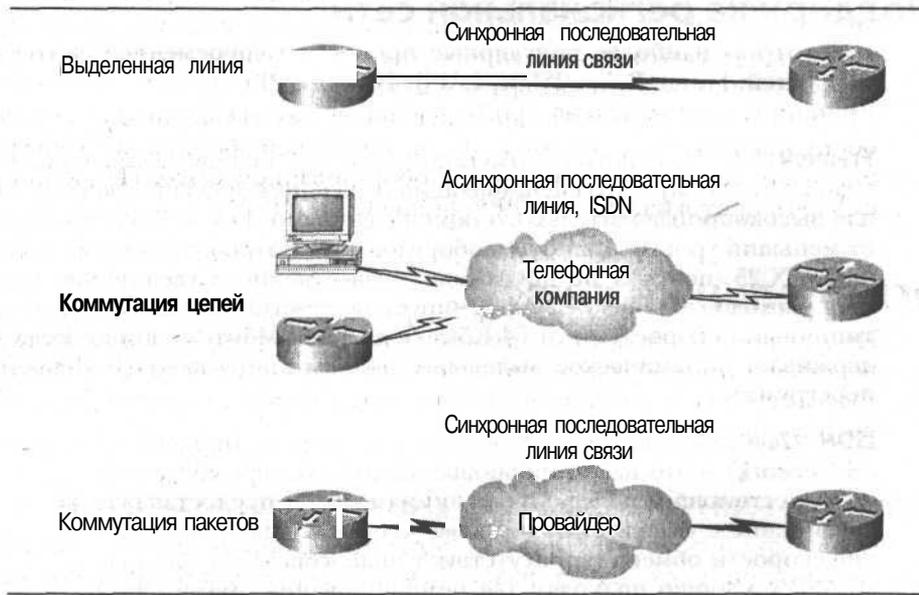
Центральный офис (CO, Central office) Соединяет потребителя с коммутационной сетью провайдера. Иногда CO называют точкой присутствия (POP, point of presence).

**Магистральная сеть (Toll network)** Магистральные линии внутри региональной сети провайдера. Объединяют переключатели и ресурсы.

Понимание смысла этих терминов необходимо для использования технологий региональных сетей.

### Типы подключения региональных сетей

На рис. 10.1 показаны разные типы подключения региональных сетей для соединения между собой локальных сетей по сети DCE.



**Рис. 10.1.** Типы подключения региональных сетей

Характеристики типов подключения по региональным сетям:

**Арендуемая линия (Leased line)** Обычно называется линией "точка-точка" или выделенной линией. Является предустановленным коммуникационным путем региональной сети от CPE через переключатель VSE к CPE в удаленной области. Такой путь позволяет взаимодействовать через сеть VTE в любое время без процедуры установки связи перед передачей данных. Основаны на синхронных последовательных линиях связи со скоростями до 45 Мбит/с.

**Коммутация цепей (Circuit switching)** Установка соединения подобно телефонному вызову. Данные не передаются до установки соединения между конечными точками. Основана на телефонных модемах и линиях ISDN. Служит для низкоскоростной передачи данных.

**Коммутация пакетов (Packet switching)** Метод коммутации в региональной сети, позволяющий нескольким компаниям совместно использовать общую полосу пропускания для сокращения затрат. Коммутацию пакетов можно считать сетью по отдельной части линии связи. Если не требуется постоянное подключение (т.е. не нужен режим объединения данных в блоки), коммутация пакетов позволит экономить затраты. Однако для постоянной передачи данных лучше перейти на арендуемую линию связи. Примером коммутации пакетов могут служить протоколы Frame Relay и X.25. Скорость обмена меняется от 56 Кбит/с до 2.048 Мбит/с.

## Поддержка региональной сети

Рассмотрим наиболее популярные протоколы современных региональных сетей: Frame Relay, ISDN, LAPB, HDLC и PPP. Кроме того, покажем принципы их работы и настройку в маршрутизаторах Cisco.

**Frame Relay** Технология коммутации пакетов, появившаяся в начале 90-х годов. *Frame Relay* — это спецификация канального и физического уровней для высокопроизводительного обмена данными. Frame Relay предполагает меньший уровень ошибок в оборудовании потребителя, чем спецификация X.25, поэтому не происходит существенного увеличения накладных расходов. Frame Relay формирует недорогие линии "точка-точка" с типичными скоростями от 64 Кбит/с до 1.544 Мбит/с. Frame Relay поддерживает динамическое выделение полосы пропускания и управление перегрузками.

**ISDN** *Цифровые сети с интегрированными службами (Integrated Services Digital Network)* — это набор цифровых служб для передачи голоса и данных по существующим телефонным линиям. ISDN предоставляет недорогое соединение с удаленными пользователями, когда требуются более высокие скорости обмена и присутствуют аналоговые телефонные линии связи. ISDN хорошо подходит для резервирования линий связи других типов, например Frame Relay или T-1.

**LAPB** *Протокол LAPB (Link Access Procedure, Balanced* — сбалансированная процедура доступа к линии) создан в качестве ориентированного на установление соединений протокола канального уровня для использования совместно с X.25. Протокол LAPB можно применять в виде простого транспорта канального уровня. Для LAPB характерны чрезмерные накладные расходы, поскольку протокол четко придерживается тайм-аутов и оконных технологий. Можно использовать LAPB вместо менее требовательного к ресурсам HDLC, если используются надежные линии связи с небольшим уровнем ошибок. Однако таких проблем уже почти не существует.

**HDLC** *Протокол HDLC (High-Level Data Link Control* — высокоуровневое управление связью данных) унаследован из протокола SDLC (Synchronous Data Link Control — управление синхронными связями данных), который был создан компанией IBM как коммуникационный протокол канального уровня. HDLC ориентирован на установление соединений канального уровня, но имеет небольшие накладные расходы по сравнению с LAPB.

Протокол HDLC не предназначен для инкапсуляции в одной связи нескольких протоколов сетевого уровня. В заголовке HDLC не указан тип протокола, транспортируемого "внутри" HDLC. Поэтому каждый разработчик коммуникационного оборудования использует в HDLC собственный способ идентификации протокола сетевого уровня. Т.е. реализация HDLC в оборудовании является лицензированной.

**Протокол PPP** Протокол PPP (Point-to-Point Protocol - протокол "точка-точка") является промышленным стандартом. Учитывая, что многие версии HDLC являются лицензированными, протокол PPP успешно используется для создания связей "точка-точка" между оборудованием разных компаний. В PPP использовано поле Network Control Protocol в заголовке канального уровня для идентификации протокола сетевого уровня. Обеспечивается аутентификация и одновременное создание нескольких подключений по синхронным или асинхронным линиям связи.

## Протокол HDLC

Протокол HDLC (High-Level Data-Link Control) — это популярный стандарт ISO для побитовой передачи данных протоколом канального уровня. Специфицирован метод инкапсуляции данных для синхронных последовательных линий связи на основе кадрирующих символов и контрольной суммы. HDLC является протоколом "точка-точка" для арендуемых линий связи. В нем не реализована аутентификация.

В побайтовых протоколах кодирование информации происходит в целые байты, но в побитовых протоколах для указания управляющей информации можно использовать отдельные разряды данных. К побитовым протоколам относятся SDLC, LLC, HDLC, TCP, IP и т.д.

В маршрутизаторах Cisco для синхронных последовательных линий по умолчанию используется инкапсуляция HDLC. Протокол HDLC от Cisco является лицензированным, поэтому не может взаимодействовать с другими реализациями HDLC. Не следует винить компанию Cisco — все реализации HDLC являются лицензированными. Рис. 10.2 показывает формат Cisco HDLC.



**Рис. 10.2.** Формат кадра Cisco HDLC

Причина появления лицензированного поля HDLC для метода инкапсуляции состоит в том, что каждый разработчик предлагает собственный способ взаимодействия протокола HDLC с протоколами сетевого уровня. Если не будет возможности взаимодействовать HDLC с разными протоколами уровня 3, то протокол HDLC сможет переносить информацию только одного другого протокола. Лицензированный заголовок (поле) вставляется в поле данных во время инкапсуляции по HDLC.

Если нужно подключаться только к одному маршрутизатору Cisco (например, к устройству Bay), когда в сети присутствует один маршрутизатор Cisco, не следует применять установленную в HDLC по умолчанию инкапсуляцию для последовательной линии связи. Лучше пользоваться чем-нибудь похожим на протокол PPP, который является стандартом ISO для идентификации протоколов верхних уровней.

## Протокол PPP

Протокол PPP (Point-to-Point Protocol) — это протокол связи данных, используемый в асинхронных последовательных (коммутируемых, телефонных) или синхронных последовательных (ISDN) линиях связи с применением LCP (Link Control Protocol) для построения и обслуживания соединений связи данных.

Основное предназначение PPP — транспорт пакетов уровня 3 через канальный уровень по линии "точка-точка". Рис. 10.3 показывает стек протоколов в сравнении с уровнями модели OSI.

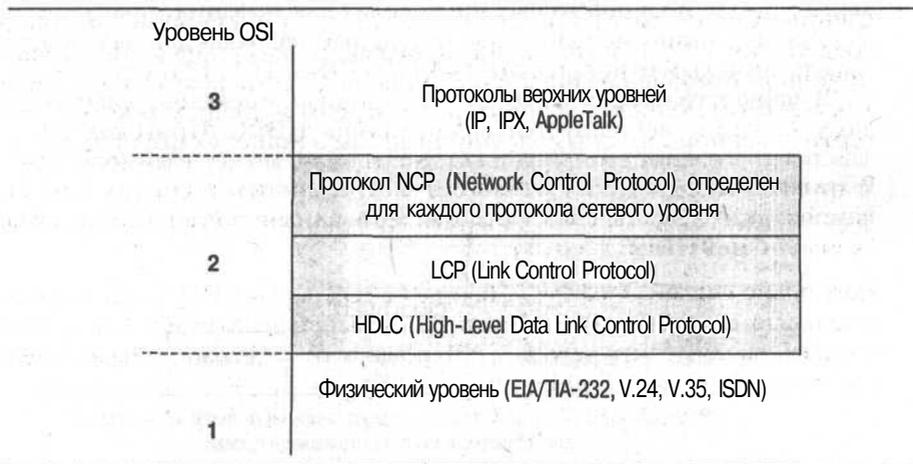


Рис. 10.3. Стек протоколов "точка-точка"

PPP состоит из четырех основных компонентов:

**EIA/TIA-232-C** Международный стандарт физического уровня для последовательных соединений.

**HDLC** Метод инкапсуляции датаграмм для передачи по последовательным линиям.

**LCP** Метод установки, настройки, обслуживания и завершения соединений "точка-точка".

**NCP** Метод установки и настройки различных протоколов сетевого уровня. PPP разработан для одновременного использования нескольких протоколов сетевого уровня, например **IPCP** (Internet Protocol Control Protocol) и **IPXCP** (Internetwork Packet Exchange Control Protocol).

Важно понять, что стек PPP специфицирован только на физическом и канальном уровнях. NCP предназначен для взаимодействия нескольких протоколов сетевого уровня за счет инкапсуляции этих протоколов с данными протокола PPP.

**Т СОВЕТУЕМ** | Знание протокола PPP обязательно!

## Параметры настройки Link Control Protocol (LCP)

Протокол Link Control Protocol обеспечивает в PPP различные возможности инкапсуляции:

**Аутентификация (Authentication)** Позволяет вызывающей стороне связи запросить информацию, идентифицирующую пользователя на другой стороне. Рассмотрим два метода аутентификации: PAP и CHAP.

**Сжатие (Compression)** Служит для увеличения пропускной способности соединения PPP. Протокол PPP производит восстановление данных на приемной стороне соединения. Компания Cisco использует методы сжатия Stackcr и Predictor, которые рассмотрены в учебном руководстве для сертификационного экзамена Advanced Cisco Router Configuration.

**Выявление ошибок (Error detection)** PPP применяет Quality and Magic Number (качественные и магические номера) для поддержки надежной и безошибочной связи данных.

**Несколько связей (Multilink)** Начиная с IOS версии 11.1 поддерживаются несколько связей по соединению PPP с маршрутизатором Cisco. Это позволяет распределить нагрузку PPP по двум и более параллельным цепям, называемым пучком (bundle).

## Процедура установки сеанса PPP

PPP может поддерживать аутентификацию, т.е. взаимодействующие маршрутизаторы обязаны предоставить информацию для идентификации линии как допустимого коммуникационного соединения. В начале соединения PPP связь проходит три фазы установления сеанса:

**Фаза установки связи (Link-establishment phase)** Каждое устройство PPP отправляет пакеты LCP для настройки и проверки связи. Пакеты LCP содержат поле Configuration Option (конфигурационные параметры), позволяющее устройствам определить размер данных, метод сжатия и способ аутентификации. Если поле Configuration Option отсутствует, используется конфигурация по умолчанию.

**Фаза аутентификации (Authentication phase)** Если это было сконфигурировано, то для аутентификации связи используется протокол CHAP или PAP. Аутентификация выполняется до начала чтения информации протокола сетевого уровня.

**Фаза протокола сетевого уровня (Network-layer protocol phase)** PPP использует протокол Network Control Protocol для инкапсуляции и пересылки по линии данных PPP нескольких протоколов сетевого уровня.

## Методы аутентификации PPP

В связях PPP могут использоваться два метода аутентификации: PAP (Password Authentication Protocol — протокол парольной аутентификации) или CHAP (Challenge Authentication Protocol — протокол аутентификации по вызову).

### Password Authentication Protocol (PAP)

Протокол Password Authentication Protocol (PAP) обеспечивает меньший уровень безопасности, чем CHAP. Пароли передаются открытым текстом, а PAP проверяет их только при первоначальном установлении связи. Во время первоначального формирования связи PPP и до подтверждения аутентификации удаленный узел возвращает запросившему маршрутизатору имя пользователя и пароль. Это и составляет проверку подлинности.

### Challenge Authentication Protocol (CHAP)

Протокол Challenge Authentication Protocol (CHAP) используется при первоначальной установке связи и периодически проверяет эту связь для гарантии взаимодействия маршрутизатора с тем же самым хостом.

По завершении начальной фазы PPP локальный маршрутизатор посылает удаленному устройству запрос вызова (challenge request). Удаленное устройство возвращает правильно вычисленное значение однонаправленной функции хеширования MD5. Локальный маршрутизатор проверяет это значение на соответствие. При несовпадении связь немедленно прерывается.

## Настройка PPP в маршрутизаторе Cisco

Настройка инкапсуляции PPP в интерфейсе маршрутизатора не является сложным процессом. Для этого следует ввести команды:

```
Router#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#ints0
```

```
Router(config-if)#encapsulation ppp
```

```
Router(config-if)#^Z
```

```
Router#
```

Разумеется, инкапсуляция PPP должна допускаться в обоих интерфейсах последовательной линии, причем о дополнительных параметрах настройки можно узнать с помощью команды help.

## Настройка аутентификации PPP

После настройки в последовательном интерфейсе инкапсуляции PPP, можно установить между маршрутизаторами режим аутентификации PPP. Сначала задается имя хоста для маршрутизатора, если оно еще не было установлено. Затем устанавливается имя пользователя и пароль для удаленного маршрутизатора, который будет подключаться к локальному маршрутизатору.

```
Router#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#hostname RouterA
```

```
RouterA(config)#username todd password Cisco
```

В команде hostname указывается имя хоста для удаленного маршрутизатора, который будет подключаться к локальному устройству. Имя зависит от регистра символов, а пароли должны быть одинаковы на обоих маршрутизаторах. Пароли хранятся в виде открытого текста и их можно вывести командой show run. Можно установить режим шифрования пароля командой service password-config, но сделать это следует до установки имени пользователя и пароля. Необходимо установить имена пользователей и пароли для каждой удаленной системы (включая маршрутизатор), к которой предполагается выполнять подключение.

После установки имени хоста, имени пользователя и пароля нужно указать тип аутентификации (CHAP или PAP).

```
RouterA#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
RouterA(config)#ints0
```

```
RouterA(config-if)#pppauthentication chap
```

```
RouterA(config-if)#pppautherntication pap
```

```
RouterA(config-if)#^Z
```

```
RouterA#
```

Если выбраны оба метода аутентификации (как в показанном примере), то во время согласования связи будет использован только первый из введенных методов. Если согласование будет неудачным, используется второй метод аутентификации.

## Проверка инкапсуляции PPP

Допустив действие инкапсуляции PPP, следует проверить ее установку и работу. Для проверки конфигурации служит команда `show interface`:

```
RouterA#show int s0
Serial0 is up, line protocol is up
 Hardware is HD64570
 Internet address is 172.16.20.1/24
 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
 Listen: IPXCP
 Open: IPCP, CDPCP, ATCP
 Last input 00:00:05, 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
 Queueing strategy: weighted fair
 Output queue: 0/1000/64/0 (size/max total/threshold/drops)
 Conversations 0/2/256 (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
 670 packets input 31845 bytes, 0 no buffer
 Received 596 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 707 packets output, 31553 bytes, 0 underruns
 0 output errors, 0 collisions, 18 interface resets
 0 output buffer failures, 0 output buffers swapped out
 21 carrier transitions
 DCD=up DSR=up DTR=up RTS=up CTS=up
RouterA#
```

В пятой строке листинга приведены сведения об инкапсуляции PPP, а в шестой строке отмечено открытие LCP. Задача протокола LCP — построение и обслуживание соединения. Восьмая строка листинга уведомляет об открытии IPCP, CDPCP и ATCP. Показана поддержка в NCP протоколов IP, CDP и AppleTalk. Седьмая строка информирует о "прослушивании" по протоколу IPXCP.

### ▼ ВНИМАНИЕ

Для проверки параметров аутентификации PPP используется команда `debug ppp authentication`.

## Frame Relay

Недавно, метод инкапсуляции для высокопроизводительных региональных сетей Frame Relay стал одной из популярных коммуникационных технологий. Этот протокол действует на физическом и канальном уровнях ссылочной модели OSI и был первоначально разработан для использования в интерфейсах Integrated Services Digital Network (ISDN). Однако сегодня Frame Relay применяется в разнообразных сетевых интерфейсах.

Frame Relay в устройствах Cisco поддерживает следующие протоколы:

- IP
- DECnet
- AppleTalk
  - Xerox Network Service (XNS)
- Novell IPX
- Connectionless Network Service (CLNS)
- Протоколы International Organization for Standards (ISO)
- Banyan Vines
- Прозрачное выполнение функций моста — прозрачное мостовое (transparent bridging)

Frame Relay предоставляет коммуникационный интерфейс между устройствами DTE (Data Terminal Equipment) и DCE (Data Circuit-Terminating Equipment, например переключатель пакетов). К категории DTE относятся терминалы, ПК, маршрутизаторы и мосты — оконечные узлы объединенной сети, которые обслуживают сами потребители. К DCE относят устройства объединенных сетей, которыми владеет оператор связи (телекоммуникационная компания).

Распространено мнение, что Frame Relay эффективнее и быстрее X.25, поскольку проверка ошибок выполняется в протоколах высокого уровня или приложениях.

Frame Relay предоставляет ориентированные на соединения связи канального уровня через виртуальные цепи, подобные цепям X.25. Эти виртуальные цепи являются логическими соединениями между двумя DTE, созданными в сети коммутации пакетов. Цепи идентифицируются DLCI (*Data Link Connection Identifier* — идентификатор соединения связи данных). Кроме того, как и X.25, Frame Relay использует PVC (Permanent Virtual Circuit — постоянные виртуальные цепи) и SVC (Switched Virtual Circuit — коммутируемые виртуальные цепи), хотя в большей части сетей Frame Relay применяются только PVC. Такая виртуальная цепь обеспечивает полный путь к сети назначения еще до отправки первого кадра.

## Термины Frame Relay

Для того чтобы понять терминологию сетей Frame Relay, нужно сначала познакомиться с основными принципами их работы. Рис. 10.4 показывает термины, определяющие отдельные части сетей Frame Relay.

Основополагающей концепцией сетей Frame Relay является разрешение пользователям взаимодействовать между двумя устройствами DTE через устройства DCE. Пользователь не должен обнаружить никаких отличий во время подключения и доступа к ресурсам, к локальному серверу и удаленному серверу в сети Frame Relay. Возможно, во втором случае скорость соединения будет меньше, чем 10 Мбит/с в локальной сети Ethernet, но физические отличия будут "прозрачны" для пользователя.

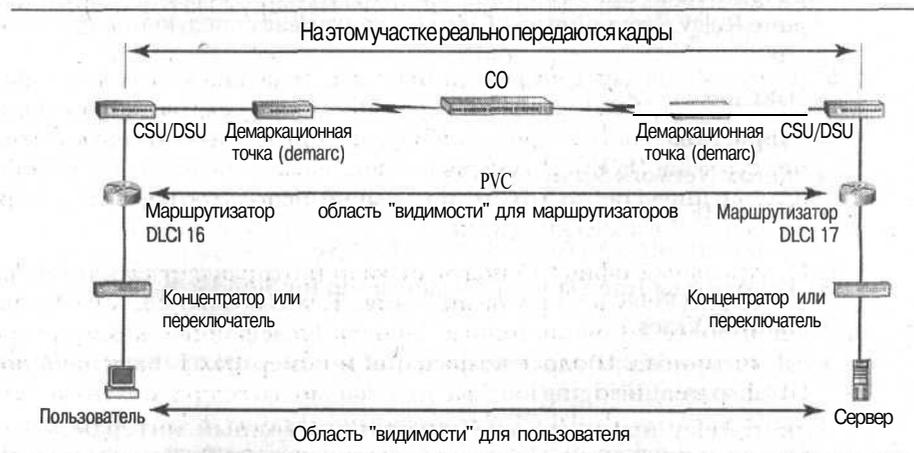


Рис. 10.4. Технологии и термины Frame Relay

На рис. 10.4 показаны операции, происходящие во время соединения двух устройств DTE. Процесс протекает так:

1. Пользовательское сетевое устройство посылает кадр из локальной сети. В заголовке кадра указан аппаратный адрес маршрутизатора (шлюза по умолчанию).
2. Маршрутизатор принимает кадр, извлекает заголовок и удаляет кадр. Затем анализируется IP-адрес назначения в извлеченном пакете для поиска сети назначения в таблице маршрутизации.
3. Маршрутизатор направляет данные в интерфейс, по которому можно достичь удаленную сеть (если сеть не отмечена в таблице маршрутизации, пакет отбрасывается). Поскольку в нужном последовательном интерфейсе используется инкапсуляция Frame Relay, маршрутизатор посылает пакет в сеть Frame Relay, вложив его в кадр Frame Relay. Добавляется номер DLCI, присвоенный последовательному интерфейсу. Идентификатор DLCI определяет виртуальную цепь (PVC или SVC) к другому маршрутизатору или переключателю провайдера в сети Frame Relay.
4. Модуль службы канала/службы данных (CSU/DSU) получает цифровой сигнал и копирует его в тот тип битового потока, который допустим для приема переключателем PSE (Packet Switch Exchange —

служба обмена коммутируемыми пакетами). Устройство PSE принимает цифровой сигнал и извлекает полученные по линии связи единицы и нули.

5. Модуль CSU/DSU подключен к демаркационной точке (demarc), обслуживаемой провайдером и находящейся на границе его зоны ответственности (последняя точка обслуживания на принимающей стороне соединения). Демаркационная точка обычно является разъемом RJ-45, находящимся вблизи маршрутизатора или модуля CSU/DSU.
6. Демаркационная точка соединяется с локальным отводом кабелем на витых парах. Локальный отвод (local loop) связывается с ближайшим центральным офисом (CO), который часто именуют точкой присутствия (POP). Локальный отвод может представлять собой разные физические носители, но обычно используются витые пары и волоконно-оптические линии.
7. Центральный офис CO получает кадр и отправляет его через "облако" Frame Relay в точку назначения. Такое облако состоит из десятков и более коммутационных офисов (телефонных коммутаторов)! Анализируется IP-адрес назначения и номер DLCI. Выяснить номер DLCI удаленного устройства или маршрутизатора можно по карте отображения IP-V-DLCI. Отображение Frame Relay статически настраивается провайдером, но может использоваться динамический протокол Inverse ARP (IARP). Перед пересылкой данных через "облако" должна быть из конца в конец создана виртуальная цепь.
8. Если кадр попадает в коммутационный офис вблизи от офиса назначения, то он направляется в локальный отвод. Затем кадр попадает в демаркационную точку и направляется в модуль CSU/DSU. Наконец, маршрутизатор извлекает из кадра пакет или датаграмму и посылает его хосту назначения внутри кадра новой локальной сети. Кадр в локальной сети имеет в своем заголовке реальный аппаратный адрес назначения. Для этого маршрутизатор просматривает собственный кэш ARP или выполняет широковещательную рассылку ARP.

Пользователь и сервер не должны знать обо всех перипетиях по пути кадра в сети Frame Relay. Доступ к удаленному серверу должен быть простым, как и к локально подключенному ресурсу.

## Инкапсуляция Frame Relay

Для настройки Frame Relay в маршрутизаторе Cisco необходимо включить инкапсуляцию в последовательном интерфейсе. Доступны два типа инкапсуляции: Cisco и IETF (*Internet Engineering Task Force* — рабочая группа инженеров Интернета). В показанном ниже листинге из маршрутизатора представлены два типа инкапсуляции для поддержки Frame Relay в маршрутизаторе Cisco:

```
RouterA(config)#ints0
RouterA(config-if)#encapsulation frame-relay ?
 ietf Use RFC1490 encapsulation
 <cr>
```

По умолчанию используется тип инкапсуляции Cisco, если только вручную не установлен тип IETF. Кроме того, тип инкапсуляции Cisco применяется при соединении двух устройств Cisco. Тип IETF потребуется для связи по Frame Relay устройства Cisco с устройством не-Cisco. Поэтому перед выбором типа инкапсуляции следует проконсультироваться у провайдера и выяснить используемый им тип инкапсуляции (если же представитель провайдера не знает типа инкапсуляции, лучше заключить договор с другим поставщиком услуг).

## Идентификатор Data Link Connection Identifier (DLCI)

Виртуальные цепи PVC сети Frame Relay идентифицируются номерами DLCI. Провайдер Frame Relay, например телефонная компания, обычно самостоятельно присваивает значение DLCI, чтобы различать отдельные виртуальные цепи в сети Frame Relay. Учитывая, что несколько виртуальных цепей могут сходиться (терминироваться) на один многоточечный интерфейс Frame Relay, с интерфейсом часто связаны несколько идентификаторов DLCI.

Для взаимодействия устройств IP на обоих концах виртуальной цепи, IP-адреса должны быть отображены на номера DLCI. Такое отображение действует подобно многоточечному устройству — оно позволяет идентифицировать в сети Frame Relay нужную виртуальную цепь назначения для каждого пакета, посланного в один физический интерфейс. Отображение может быть динамическим через IARP или формироваться вручную командой `frame relay map`.

Frame Relay использует DLCI подобно применению в X.25 адресов X.121, т.е. в сети Frame Relay любой номер DLCI может иметь как глобальное, так и локальное действие.

Иногда провайдер присваивает DLCI определенной области сети. Об этом объявляется всем удаленным областям как об одной цепи PVC. Такая постоянная виртуальная цепь (PVC) становится глобальной. Например, корпоративный офис компании может иметь номер DLCI, равный 20. Все удаленные области будут знать, что корпоративный офис идентифицируется как DLCI 20 и будут пользоваться этой цепью PVC для обращения к корпоративному офису. Однако настроенные для пользователя реализации предполагают локальное действие каждого номера DLCI. Т.е. номера DLCI не обязательно будут уникальными. Разные области могут иметь одинаковые номера DLCI для связей, поскольку Frame Relay отображает локальные номера DLCI на виртуальные цепи в каждом интерфейсе переключателя. Любой удаленный офис способен иметь собственный номер DLCI и взаимодействовать с другими корпоративными офисами на основе уникальных номеров DLCI.

Номера DLCI, используемые для идентификации PVC, обычно присваиваются провайдером начиная от значения 16. Пример присвоения интерфейсу номера DLCI:

```
RouterA(config-if)#frame-relay interface-did ?
<16-1007> Define a DLCI as part of the current subinterface
RouterA(config-if)#frame-relay interface-did 16
```

## Local Management Interface (LMI)

*Интерфейс LMI* (Local Management Interface — интерфейс локального управления) был разработан в 1990 году компаниями Cisco Systems, StrataCom, Northern Telecom и Digital Equipment Corporation, поэтому часто называется Gang-of-Four LMI (LMI от банды четырех) или просто Cisco LMI. Упомянутые четыре компании заимствовали основные концепции протокола Frame Relay из спецификации CCITT и **добавили** дополнительные возможности для упрощения коммуникации устройств по сети Frame Relay.

Интерфейс LMI — это стандарт управляющих сигналов, действующий между устройством CPE (маршрутизатор) и переключателем кадров. Интерфейс LMI отвечает за управление и обслуживание состояний взаимодействующих устройств. В сообщениях LMI распространяются сведения о следующем:

**Keeralives** (поддержка активности) Проверка потока данных

**Multicasting** (обеспечение многоадресности) Предоставление локальных номеров DLCI цепям PVC

**Multicast addressing** (многоадресная схема) Действует глобально

**Статус виртуальной цепи** Обеспечение статуса DLCI

### ▼ ВНИМАНИЕ

Начиная с IOS версии 11.2 тип LMI определяется автоматически. Это позволяет интерфейсу самостоятельно выяснить тип поддерживаемого переключателем интерфейса LMI.

Для автоопределения (auto-sense) необходимо удостовериться, что провайдер Frame Relay поддерживает необходимые типы LMI. Типом по умолчанию является Cisco, но могут использоваться ANSI или Q.933A. Все три типа LMI показаны ниже в листинге маршрутизатора.

```
RouterA(config-if)#frame-relaylmi-type ?
cisco
ansi
q933a
```

Поддерживаются три стандартных формата LMI для сигналов:

**Cisco** LMI по спецификации Gang of Four (тип по умолчанию)

ANSI Приложение D к стандарту T1.617 института ANSI

ITU-T (q933a) Приложение A к спецификации Q.933

Маршрутизаторы получают в интерфейсе информацию LMI, инкапсулированную в кадры, причем возможны обновления статуса виртуальных цепей при переходе между тремя состояниями:

**Активное состояние (Active state)** Все включено и маршрутизатор может обмениваться информацией.

**Пассивное состояние (Inactive state)** Включен и работает интерфейс маршрутизатора к коммутационному офису, но не действует удаленный маршрутизатор.

**Состояние отмены (Deleted state)** Информация LMI от переключателя не принимается интерфейсом. Возможно, проблемы связаны с отображением или отказом линии связи.

## Подинтерфейсы

В одном последовательном интерфейсе можно иметь несколько виртуальных цепей, которые считаются отдельными интерфейсами — *подинтерфейсами*. Можно считать подинтерфейс аппаратным интерфейсом, определенным в программном обеспечении IOS. Смысл введения подинтерфейсов состоит в возможности присваивания разных характеристик сетевого уровня каждому подинтерфейсу и виртуальной цепи, например, установить маршрутизацию IP в одной виртуальной цепи, а маршрутизацию IPX в другой цепи.

## Неполные сетевые структуры

Подинтерфейсы позволяют согласовать неполные сетевые структуры сетей Frame Relay и протоколы с делением горизонта. Предположим, протокол IP действует в локальной сети. Если в этой сети маршрутизатор А способен обратиться к маршрутизатору В, а В к маршрутизатору С, то предполагается, что маршрутизатор А может взаимодействовать с маршрутизатором С. Это справедливо для локальных сетей, но не всегда выполняется в сетях Frame Relay, если только маршрутизатор А не имеет цепи PVC к маршрутизатору С.

На рис. 10.5 сеть 1 сконфигурирована с пятью областями. Для полноценной работы сети необходима неполная сетевая структура, показанная для сети 2. Однако даже при работоспособности сети 2, а это слишком дорогостоящее решение, возможна конфигурация с подинтерфейсами, представленная для сети 3, которая эффективнее с точки зрения стоимости.

Введение подинтерфейсов в сети 3 позволяет реально разделить сеть Frame Relay на небольшие подсети с собственными сетевыми номерами. Поэтому области А, В и С соединены с полноценной сетью, хотя области С и D, D и E связаны между собой соединениями "точка-точка". Области С и D подключены к двум подинтерфейсам, способным перенаправлять пакеты.

Кроме того, подинтерфейсы решают проблемы протоколов маршрутизации с делением горизонта. Согласно концепции деления горизонта протокол маршрутизации не распространяет свою информацию в интерфейсе, из которого она была получена. Это приводит к возникновению в сетчатой структуре Frame Relay network. Однако с помощью подинтерфейсов протокол маршрутизации, получая обновления в одном из интерфейсов, может распространять их в других подинтерфейсах.

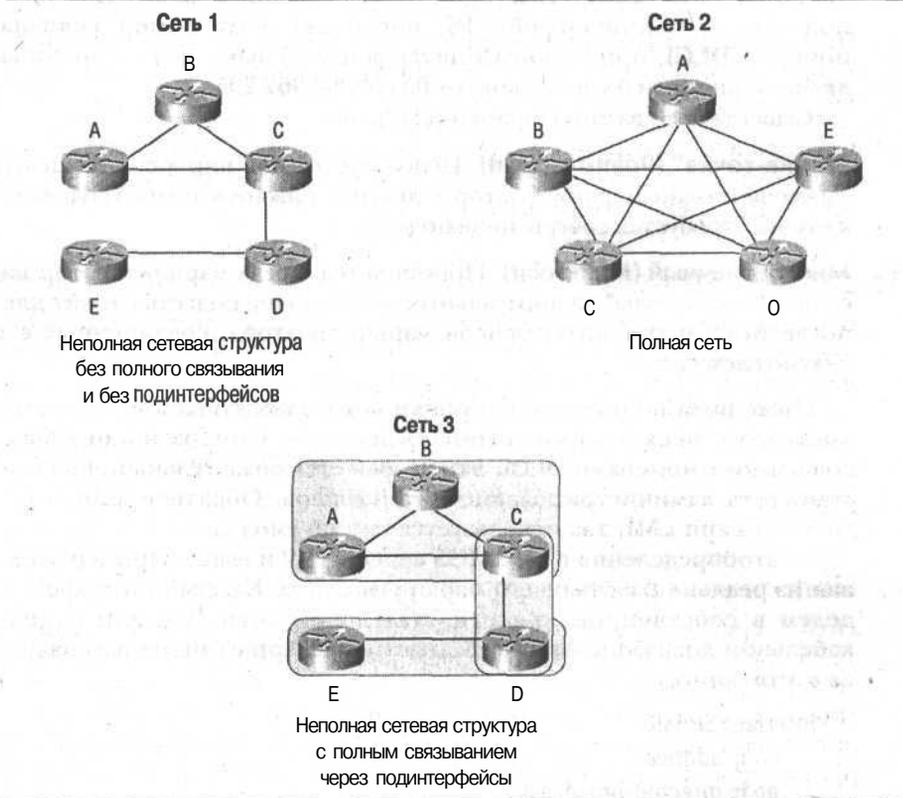


Рис. 10.5. Примеры неполных сетевых структур

### Создание подинтерфейсов

Пример создания подинтерфейсов командой `int s0.subinterface number` показан ниже. Сначала разрешается инкапсуляция в последовательном интерфейсе, затем устанавливаются подинтерфейсы.

```
RouterA(config)#ints0
RouterA(config)#encapsulationframe-relay
RouterA(config)#ints0.?
<0-4294967295> Serial interface number
```

```
RouterA(config)#int s0.16?
multipoint Treat as a multipoint link
 (трактруется как многоточечная связь)
point-to-point Treat as a point-to-point link
 (трактруется как связь "точка-точка")
```

В физическом интерфейсе можно установить практически неограниченное количество подинтерфейсов (однако следует помнить об ограниченной памяти маршрутизатора). В предложенном выше примере мы использовали подинтерфейс 16, поскольку этот номер совпадает с номером DLCI, присвоенным интерфейсу. Однако можно пользоваться любыми числами из диапазона от 0 до 4 292 967 295.

Существуют два типа подинтерфейсов:

**"Точка-точка" (Point-to-point)** Используется для виртуальной цепи, связывающей один маршрутизатор с другим. Каждому подинтерфейсу "точка-точка" требуется собственная подсеть.

**Многоточечный (Multipoint)** Применяется, когда маршрутизатор является центром "звезды" из виртуальных цепей. Одна подсеть служит для всех последовательных интерфейсов маршрутизатора, соединенных с переключателем кадров.

Ниже показан пример настройки в производственной среде маршрутизатора с несколькими подинтерфейсами. Номера подинтерфейсов совпадают с номерами DLCI. Это не является обязательным, но помогает упростить администрирование интерфейсов. Обратите внимание, что не указан тип LMI, т.е. используется тип по умолчанию Cisco или процедура автоопределения в Cisco IOS версии 11.2 и выше. Пример заимствован из реально работающего маршрутизатора. Каждый интерфейс определен в собственной подсети, отдельной сети IPX или отдельном кабельном диапазоне AppleTalk (настройка AppleTalk не рассматривается в этой книге):

```
interface Serial0
 no ip address
 no ip directed-broadcast
 encapsulation frame-relay
!
interface Serial0.102 point-to-point
 ip address 10.1.12.1 255.255.255.0
 no ip directed-broadcast
 appletalk cable-range 12-12 12.65
 appletalk zone wan2
 appletalk protocol eigrp
 no appletalk protocol rtmp
 ipx network 12
 frame-relay interface-did 102
```

```
!
interface Serial0.103 point-to-point
 ipaddress 10.1.13.1 255.255.255.0
 no ip directed-broadcast
 appletalk cable-range 13-13 13.174
 appletalk zone wan3
 appletalk protocol eigrp
 no appletalk protocol rtmp
 ipx network 13
 frame-relay interface-did 103
```

```
!
interface Serial0.104 point-to-point
 ip address 10.1.14.1 255.255.255.0
 no ip directed-broadcast
 appletalk cable-range 14-14 14.131
 appletalk zone wan4
 appletalk protocol eigrp
 no appletalk protocol rtmp
 ipx network 14
 frame-relay interface-dlci 104
```

```
!
interface Serial0.105 point-to-point
 ipaddress 10.1.15.1 255.255.255.0
 no ip directed-broadcast
 appletalk cable-range 15-15 15.184
 appletalk zone wan5
 appletalk protocol eigrp
 no appletalk protocol rtmp
 ipx network 15
 frame-relay interface-dlci 105
```

```
!
interface Serial0.106 point-to-point
 ipaddress 10.1.16.1 255.255.255.0
 no ip directed-broadcast
 appletalk cable-range 16-16 16.28
 appletalk zone wan6
 appletalk protocol eigrp
 no appletalk protocol rtmp
 ipx network 16
 frame-relay interface-dlci 106
```

```
!
interface Serial0.107 point-to-point
 ip address 10.1.17.1 255.255.255.0
```

```

no ip directed-broadcast
appletalk cable-range 17-17 17.223
appletalk zonetwan7
appletalk protocol eigrp
no appletalk protocol rtmp
ipx network 17
frame-relay interface-did 107
}
interface Serial0.108 point-to-point
ip address 10.1.18.1 255.255.255.0
no ip directed-broadcast
appletalk cable-range 18-18 18.43
appletalk zonetwan8
appletalk protocol eigrp
no appletalk protocol rtmp
ipx network 18
frame-relay interface-did 108

```

## Отображение Frame Relay

Для взаимодействия устройства IP на одном из концов виртуальной цепи, адрес этого устройства должен быть отображен на номер DLCI. Для этого применяются два способа:

- Команда `frame relay map`.
- Функция `inverse-arp`.

Пример использования команды `map` для Frame Relay:

```

RouterA(config)#ints0
RouterA(config-if)#encapframe
RouterA(config-if)#int s0.16point-to-point
RouterA(config-if)#no inverse-arp
RouterA(config-if)#ipaddress 172.16.30.1 255.255.255.0
RouterA(config-if)#frame-relaymap ip 172.16.30.17 16ietf broadcast
RouterA(config-if)#frame-relaymap ip 172.16.30.18 17 broadcast
RouterA(config-if)#frame-relay map ip 172.16.30.19 18

```

Рассмотрим этот пример. Сначала мы настроили интерфейс `serial 0` для типа инкапсуляции Cisco (по умолчанию), затем определили подинтерфейс. После этого мы отключили функцию `inverse arp` и отобразили три виртуальные цепи согласно номерам DLCI.

Обратите внимание, что для первого отображения изменен тип инкапсуляции. Команда `frame relay map` представляет собой единственно возможный способ совместного использования разных типов инкапсуляции.

Ключевое слово `broadcast` в конце команды `map` предписывает маршрутизатору пересылать широковещательные сообщения, поступающие

на этот интерфейс, по указанной виртуальной цепи. Протокол Frame Relay использует нешироковещательный многоточечный метод инкапсуляции NBMA (nonbroadcast multiaccess), не предполагающий широковещательных рассылок информации о маршрутизации. Можно использовать команду `tap` с аргументом `broadcast` или применить в процессе маршрутизации команду `neighbor`.

Вместо того чтобы писать команду `tap` для каждой отдельной виртуальной цепи, можно выполнить динамическое преобразование IP-адресов в номера DLCI с помощью функции `inverse-arp`. При ее использовании процесс настройки будет выглядеть так:

```
RouterA(config)#ints0.16 point-to-point
RouterA(config-if)#encap frame-relay ietf
RouterA(config-if)#ipaddress 172.16.30.1 255.255.255.0
```

Эта конфигурация проще, но не так стабильна, как конфигурация на основе команды `tap`. Иногда использование функции `inverse-arp` связано с ошибками в конфигурации, поскольку виртуальные цепи становятся невидными и динамически отображаются на неизвестные устройства.

## Управление нагрузкой в Frame Relay

Рассмотрим способы управления нагрузкой в переключателе Frame Relay.

**DE** (Discard Eligibility, право на отброс) Когда маршрутизатор Frame Relay выявляет перегрузку в сети Frame Relay, он включает бит DE в заголовке пакета Frame Relay. Если переключатель перегружен, то начинает отбрасывать пакеты с установленными битами DE. Если полоса пропускания настроена с параметром CIR, равным нулю, всегда включается бит DE.

**FECN** (Forward-Explicit Congestion Notification, явно отсылаемое уведомление о перегрузке) Если в облаке сети Frame Relay выявляется перегрузка, переключатель устанавливает в единицу бит FECN, который находится в заголовке пакета Frame Relay. Это указывает на перегрузку в пути, по которому данные поступают в устройство назначения DCE.

**BECN** (Backward-Explicit Congestion Notification — явно возвращаемое уведомление о перегрузке) Когда переключатель выявляет перегрузку в сети Frame Relay, это устройство устанавливает бит BECN в пакете Frame Relay и отправляет пакет маршрутизатору-источнику. Он указывает на необходимость снижения скорости передачи во время отправки пакетов.

## CIR (Committed Information Rate)

Протокол Frame Relay предназначен для одновременного предоставления коммутируемой сети нескольким разным потребителям. Таким образом можно поделить затраты на использование переключателей среди нескольких клиентов. Однако протокол Frame Relay разработан в предположении, что не всем потребителям одновременно необходима

постоянная скорость передачи данных. Frame Relay прекрасно подходит для пакетного (импульсного) трафика.

Frame Relay можно считать протоколом деления линии на части, подобно использованию одного телефона группой людей. Нужные для совместного применения частичные линии создаются в предположении, что не всем членам группы постоянно нужен телефон. Если одного телефона становится недостаточно, можно заплатить дополнительно и установить еще один аппарат. То же самое происходит в Frame Relay, но в данном случае несколько устройств могут работать одновременно. Однако если требуется подключение с постоянным потоком данных, лучше не использовать Frame Relay, а перейти на выделенную линию "точка-точка" T-1.

Frame Relay предоставляет каждому потребителю выделенную полосу пропускания, однако потребитель должен запрашивать выделение своей части общей полосы пропускания физической линии. Провайдер Frame Relay разрешает потребителям оплатить меньшую полосу пропускания. Этот уровень называется CIR (*Committed Information Rate* — согласованный уровень информации). Например, пользователь может заплатить за полосу пропускания 256к, но в пакетном кратковременном режиме затребовать скорость обмена T-1. Уровень CIR определяет, что если входные данные от устройства в сеть Frame Relay не превышают уровня CIR, то сеть продолжает передавать данные по цепи PVC. Однако если поток данных превышает уровень CIR, доставка данных не гарантируется.

Иногда допускается режим аренды Bc (Committed Burst — согласованный пакетный режим), который позволяет потребителям превысить уровень CIR в течение определенного интервала времени. В этом режиме всегда устанавливается бит DE.

Выбор уровня CIR делается на основе реалистичного прогноза трафика. Некоторые провайдеры Frame Relay позволяют аренду при нулевом значении уровня CIR. Этот режим экономит средства, когда допустима повторная пересылка информации. Однако в нем бит DE включен в любой пересылаемый потребителем кадр.

## Мониторинг Frame Relay

После установки и запуска инкапсуляции Frame Relay существует несколько способов проверки состояния интерфейса и цепи PVC:

```
RouterA>sho frame ?
ip show frame relay IP statistics
lmi show frame relay lmi statistics
map Frame-Relay map table
pvc show frame relay pvc statistics
route show frame relay route
traffic Frame-Relay protocol statistics
```

## Show Frame-Relay Lmi

Команда `show frame-relay lmi` выводит статистику о трафике LMI между локальным маршрутизатором и переключателем Frame Relay.

```
Router#sh frame lmi
```

```
LMI Statistics for interface Serial0 (Frame Relay DTE) LMI TYPE = CISCO
```

```
Invalid Unnumbered info 0 Invalid Prot Disc 0
```

```
Invalid dummy Call Ref 0 Invalid Msg Type 0
```

```
Invalid Status Message 0 Invalid Lock Shift 0
```

```
Invalid Information ID 0 Invalid Report IE Len 0
```

```
Invalid Report Request 0 Invalid Keep IE Len 0
```

```
Num Status Enq. Sent 0 Num Status msgs Rcvd 0
```

```
Num Update Status Rcvd 0 Num Status Timeouts 0
```

```
Router#
```

В листинге из маршрутизатора показаны ошибки и тип LMI.

## Show Frame-Relay Pvc

Команда `show frame-relay pvc` перечисляет все сконфигурированные цепи PVC и присвоенные номера DLCI. Можно узнать статус каждого соединения PVC и статистику трафика. Подсчитывается количество пакетов BECN и FECN, полученных маршрутизатором.

```
RouterA#sho frame pvc
```

```
PVC Statistics for interface Serial0 (Frame Relay DTE)
```

```
DLCI = 16,DLCI USAGE = LOCAL,PVC STATUS =ACTIVE,INTERFACE = Serial0.1
```

```
input pkts 50977876 output pkts 41822892 in bytes
```

```
3137403144
```

```
out bytes 3408047602 dropped pkts 5 in FECN pkts 0
```

```
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
```

```
in DE pkts 9393 out DE pkts 0
```

```
pvc create time 7w3d, last time pvc status changed 7w3d
```

```
DLCI = 18,DLCI USAGE =LOCAL,PVC STATUS =ACTIVE,INTERFACE = Serial0.3
```

```
input pkts 30572401 output pkts 31139837 in bytes 1797291100
```

```
out bytes 3227181474 dropped pkts 5 in FECN pkts 0
```

```
in BECN pkts 0 out FECN pkts 0 out BECN pkts 0
```

```
in DE pkts 28 out DE pkts 0
```

```
pvc create time 7w3d, last time pvc status changed 7w3d
```

Для вывода сведений только о цепи PVC 16 используйте команду `show frame-relay pvc 16`.

## Show Interface

Командой `show interface` можно проверить трафик LMI. Появятся сведения об инкапсуляции и информация об уровнях 2 и 3.

В листинге выделены сведения о LMI DLCI, позволяющие узнать тип используемого интерфейса LMI. Если указано значение 1023, то это тип LMI по умолчанию Cisco. Если LMI DLCI равно нулю, значит это ANSI LMI.

```
RouterA#sho int s0
Serial0 is up, line protocol is up
 Hardware is HD64570
 MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 2/255
 Encapsulation FRAME-RELAY, loopback not set, keepalive
set (10 sec)
 LMI enq sent 451751, LMI stat recvd 451750, LMI upd recvd
164, DTE LMI up
 LMI enq recvd 0, 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 0/0, interface broadcasts 839294
```

Команда `show interface` показывает сведения о линии, протоколе, DLCI и LMI.

## Show Frame Map

Команда `show frame map` выводит сведения об отображении сетевого уровня на DLCI.

```
RouterB#show frame map
 Serial0 (up): ipx 20.0007.7842.3575 dlc1 16(0x10,0x400),
dynamic, broadcast, status defined, active
 Serial0 (up): ip 172.16.20.1 dlc1 16(0x10,0x400),
dynamic, broadcast, status defined, active
 Serial1 (up): ipx 40.0007.7842.153a dlc1 17(0x11,0x410),
dynamic, broadcast/ status defined, active
 Serial1 (up): ip 172.16.40.2 dlc1 17(0x11,0x410),
dynamic, broadcast, status defined, active
```

В данном случае последовательный интерфейс имеет два отображения: одно для IP и одно для IPX. Адреса сетевого уровня разрешаются с помощью динамического протокола Inverse ARP (IARP). Если администратор отобразит некоторый адрес вручную, то он будет отмечен в листинге "static" — статический.

После номеров DLCI в листинге в скобках указаны числа. Первое число — 0x10 — является ширококвещательным эквивалентом для номера 16 идентификатора DLCI, используемого в интерфейсе serial 0, число 0x11 — это ширококвещательное DLCI 17 для serial 1. Вторые числа 0x400

и 0x410 показывают номера DLCI для кадров Frame Relay. Они отличаются, поскольку использованы разные методы распределения битов в кадре.

**▼ ВНИМАНИЕ** [ Для отмены динамического отображения служит команда `clear frame-relay-inarp`.

### Debug Frame Lmi

Команда `debug frame lmi` по умолчанию выводит листинг на консоль маршрутизатора. Она помогает проверять и диагностировать подключения Frame Relay. Можно определить, правильно ли маршрутизатор и переключатель обмениваются информацией LMI.

```
Router#debug frame-relay lmi
Serial3/1(in): Status, myseq 214
RT IE 1, length 1, type 0
KA IE 3, length 2, yourseq 214, myseq 214
PVC IE 0x7, length 0x6, dlcI 130, status 0x2, bw 0
Serial3/1(out): StEnq, myseq 215, yourseen 214, DTE up
datagramstart= 0x1959DF4, datagramsize= 13
FR encap= 0xFCF10309
00 75 01 01 01 03 02 D7 D6
Serial3/1(in): Status, myseq 215
RT IE 1, length 1, type 1
KA IE 3, length 2, yourseq 215, myseq 215
Serial3/1(out): StEnq, myseq 216, yourseen 215, DTE up
datagramstart= 0x1959DF4, datagramsize = 13
FR encap= 0xFCF10309
00 75 01 01 01 03 02 D8 D7
```

## Integrated Services Digital Network (ISDN)

*Цифровые сети с интегрированными службами* (ISDN — Integrated Services Digital Network) разработаны для обычных телефонных сетей. ISDN поддерживают как передачу голоса, так и данных. Но для использования ISDN требуется полоса пропускания. Типичные приложения и реализации ISDN — это программы высокоскоростной обработки изображений (например, факсимильная связь Group IV), скоростного обмена файлами, видеоконференции и несколько каналов из жилого помещения к телекоммуникационному провайдеру.

ISDN — это набор коммуникационных протоколов, предлагаемых телекоммуникационной компанией (оператором связи) для поддержки группы цифровых служб. Они способны передавать конечным пользователям данные, текст, звук, музыку, графику и видео, причем все это предназначено для уже существующих телефонных систем. ISDN

определяется в наборе стандартов ITU-T и соответствует физическому, каналному и сетевому уровням модели OSI. Стандарты ISDN специфицируют требования к оборудованию и схеме вызова для формирования сквозного цифрового подключения.

Протокол PPP используется в ISDN для инкапсуляции данных, проверки целостности линий и аутентификации. Преимущества ISDN:

- Одновременная передача голоса, видео и данных
- Быстрое по сравнению с модемом обслуживание вызова
- Быстрая по сравнению с модемом скорость передачи данных

## Компоненты ISDN

Компоненты ISDN называются функциями (function) и опорными точками (reference point). Рис. 10.6 показывает типы терминалов и опорных точек в сетях ISDN.

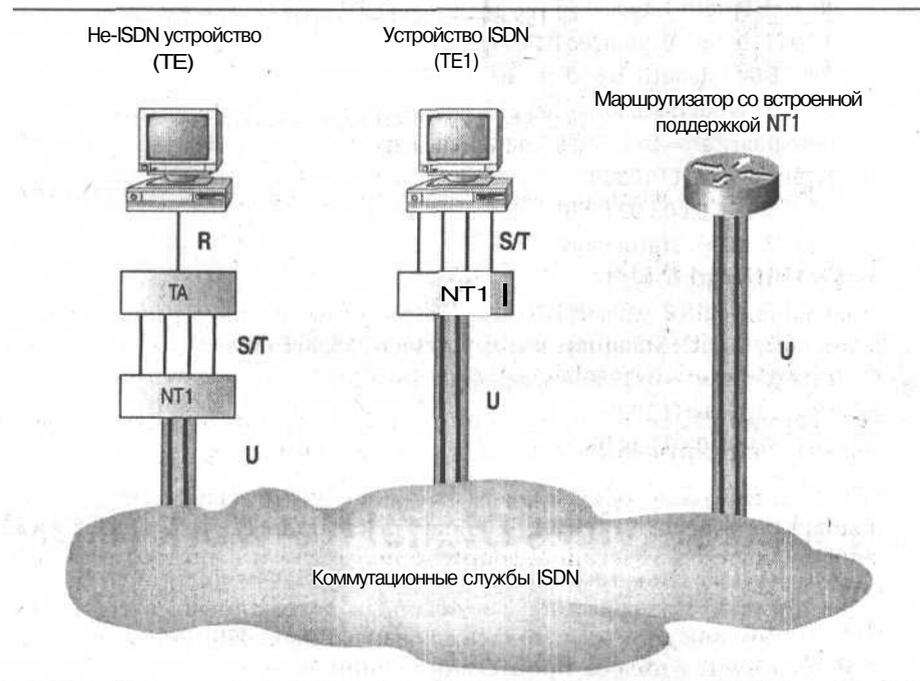
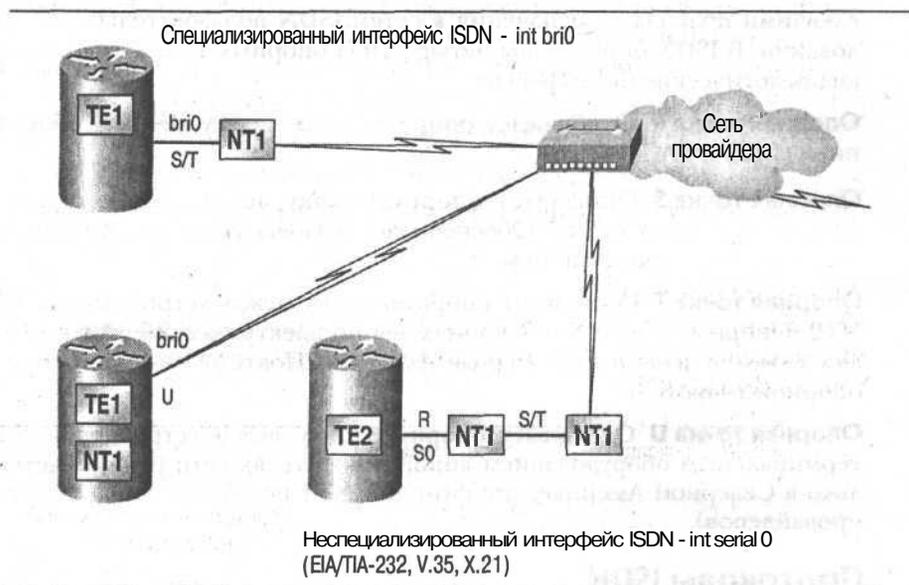


Рис. 10.6. Функции и опорные точки ISDN

В Северной Америке ISDN использует двухпроводное подключение к квартире или к офисному помещению. Это называется опорной точкой "U". Устройство NT1 служит для преобразования двухпроводного подключения в четырехпроводное, которое необходимо для телефонов и терминальных адаптеров (TA, terminal adapter) сетей ISDN. Многие маршрутизаторы имеют встроенные интерфейсы NT1 (U).

На рис. 10.7 показаны разные опорные точки и терминальное оборудование, используемое с интерфейсом Cisco ISDN BRI.



**Рис. 10.7.** Опорные точки и терминальное оборудование ISDN BRI

### Терминалы ISDN

Подключенные к сети ISDN устройства называются терминальным оборудованием TE (terminal equipment) и терминальным оборудованием сети NT (network termination). Доступные типы оборудования:

**TE1** Терминальное оборудование типа 1 — терминалы, способные поддержать стандарты ISDN и подключаться к сетям ISDN.

**TE2** Терминальное оборудование типа 2 — терминалы, выпущенные до появления стандартов ISDN. Для использования TE2 необходим терминальный адаптер TA (terminal adapter), позволяющий подключить устройство TE2 к сети ISDN.

**NT1** Терминальная сеть типа 1 реализует спецификацию ISDN для физического уровня и обеспечивает подключение пользовательских устройств к сети ISDN.

**NT2** Терминальная сеть типа 2 обычно является оборудованием провайдера, например переключателем или коммутатором (PBX). Действует на канальном и сетевом уровнях. Редко располагается в помещениях потребителя.

**ТА** Терминальный адаптер преобразует кабельное подключение TE2 в TE1 для дальнейшего соединения с устройством NT1 и преобразования в двухпроводную сеть ISDN.

## Опорные точки ISDN

Опорные точки определяются несколькими спецификациями, устанавливающими правила подключения к сетям ISDN пользовательского оборудования. В ISDN определены четыре типа опорных точек, специфицирующих логические интерфейсы:

**Опорная точка R** Отображает опорную точку между не-ISDN оборудованием (TE2) и ТА.

**Опорная точка S** Описывает опорную точку между пользовательским маршрутизатором и NT2. Обеспечивает вызовы между различным пользовательским оборудованием.

**Опорная точка T** Описывает опорную точку между устройствами NT1 и NT2. Опорные точки S и T одинаковы по электрическим характеристикам и могут выполнять сходные функции. Поэтому иногда говорят об опорной точке S/T.

**Опорная точка U** Описывает опорную точку между устройством NT1 и терминальным оборудованием линий в носителях сети (применяется только в Северной Америке, где функции NT1 не обеспечиваются в сетях провайдеров).

## Протоколы ISDN

Протоколы ISDN определены ITU и специфицируют несколько различных аспектов:

- Протоколы, название которых начинается на букву *E*, специфицируют использование ISDN в существующих телефонных сетях.
- Протоколы, название которых начинается на букву *I*, определяют концепции, технические свойства и службы.
- Протоколы, название которых начинается на букву *Q*, специфицируют коммутацию и сигналы.

## Типы переключателей ISDN

Большая часть современных переключателей ISDN — это устройства компаний AT&T и Nortel, но существуют и другие производители. В таблице 10.1 столбец "Ключевое слово" перечисляет параметры команды `isdn switch-type` для настройки маршрутизатора на соединение с разными переключателями. Если не известен используемый в центральном офисе провайдера переключатель, необходимо точно выяснить его тип у представителя провайдера.

**Таблица 10.1.**

### Типы переключателей ISDN

Тип переключателя	Ключевое слово
Переключатель AT&T для режима Basic Rate	Basic-5ess
Переключатель Nortel DMS-100 для режима Basic Rate	Basic-dms100

Таблица 10.1.  
(продолжение)

Тип переключателя	Ключевое слово
Переключатель National ISDN-1	Basic-nil
AT&T 4ESS (только ISDN PRI)	Primary-4ess
AT&T 5ESS (только ISDN PRI)	Primary-5ess
Nortel DMS-100 (только ISDN PRI)	Primary-dms100

## Basic Rate Interface (BRI)

В ISDN интерфейс базового уровня *BRI* (Basic Rate Interface, иногда называется 2B+1D) предоставляет два канала В и один канал D. Канал В интерфейса *BRI* работает на скорости 64 Кбит/с и служит для передачи данных, а канал D функционирует на скорости 16 Кбит/с и используется для управления и передачи сигнальной информации.

Протокол канала D охватывает физический, каналный и сетевой уровни. Канал D переносит сигналы для установки и управления вызовами, а также используется для других функций, например системы аварийной сигнализации в заданиях или любых функций, где необходима полоса пропускания. Однако все функции ограничиваются в совокупности скоростью 16 Кбит/с. Канал D действует на канальном уровне по протоколу LAPD.

Для настройки ISDN *BRI* необходимо получить идентификатор SPID (Service Profile Identifier — идентификатор профиля службы), причем необходимы идентификаторы SPID для каждого канала В. Идентификатором SPID может быть телефонный номер отдельного канала В. Устройство ISDN предоставляет SPID переключателю ISDN, что позволяет устройству обращаться к сетевым службам *BRI* или *PRI*. Без указания SPID многие переключатели ISDN не допускают устройство до вызова службы в сети.

Для установки вызова *BRI* должны быть выполнены четыре условия:

1. Установлен канал D между маршрутизатором и локальным переключателем ISDN.
2. Переключатель ISDN должен использовать сигналы SS7 для установки пути к удаленному переключателю.
3. Удаленный переключатель обязан установить связь по каналу D с удаленным маршрутизатором.
4. Должен быть сформирован канал В из конца в конец линии связи.

## Primary Rate Interface (PRI)

В Северной Америке и Японии интерфейс основного уровня *Primary Rate Interface* (*PRI* или 23B+D1) предоставляет в ISDN-сети 23 службы доставки

по каналу В со скоростью 64 Кбит/с и один канал D со скоростью 64 Кбит/с, что в сумме позволяет получить скорость обмена до 1.544 Мбит/с.

В Европе, Австралии и некоторых других странах сеть ISDN предоставляет 30 служб канала В со скоростью 64 Кбит/с и один канал D со скоростью 64 Кбит/с. В сумме это составляет скорость обмена до 2.048 Мбит/с.

## ISDN в маршрутизаторах Cisco

Доступ к ISDN в маршрутизаторе Cisco означает, что необходимо устройство со встроенной поддержкой NT1 (опорная точка U) или с модемом ISDN (называемым TA). Если маршрутизатор имеет интерфейс BRI, то дополнительного оборудования не требуется. Иначе придется использовать один из последовательных интерфейсов маршрутизатора для подключения TA. Маршрутизатор с интерфейсом BRI называется устройством TE1 (оконечная точка терминала типа 1), а устройство, которому необходим адаптер TA, называется TE2 (оконечная точка терминала типа 2, terminal equipment 2).

ISDN поддерживает почти все высокоуровневые сетевые протоколы (IP, IPX, AppleTalk и т.д.), а в качестве протокола инкапсуляции можно выбрать PPP, HDLC или LAPD.

### Т ВНИМАНИЕ

Во время конфигурации ISDN необходимо знать тип переключателя, используемого провайдером. Для этого используйте команду `isdnswitch-type ?` в режиме глобального конфигурирования или конфигурации интерфейса. Это обязательно, поскольку каждый производитель имеет лицензированные протоколы для обмена сигналами.

В каждом интерфейсе ISDN BRI нужно указать идентификатор SPID подкомандой интерфейса `isdn spid1` и `isdn spid2`. Эти идентификаторы предоставляются провайдером ISDN и определяют пользователя в переключателе (можно считать SPID похожими на телефонные номера). Однако некоторые провайдеры уже не требуют использование идентификаторов SPID во время настройки маршрутизатора. Все вопросы относительно SPID следует выяснить у конкретного провайдера.

Второй частью конфигурации SPID является локальный номер вызова для этого идентификатора. Номер вызова необязателен. Однако некоторым переключателям он необходим для одновременного использования в маршрутизаторе обоих каналов В.

Пример настройки:

```
RouterA#config t
Enter configuration commands, one per line. End with CNTL/Z.
RouterA(config)#isdn switch-type basic-nil
RouterA(config)#int bri0
RouterA(config-if)#encapppp (optional)
```

```
RouterA(config-if)#isdn spid1 086506610100 8650661
```

```
RouterA(config-if)#isdn spid2 086506620100 8650662
```

**Т СОВЕТУЕМ** | Команда `isdn switch-type` может исполняться в глобальном режиме или режиме настройки интерфейса. Настройка в глобальном режиме устанавливает тип переключателя для всех интерфейсов BRI в маршрутизаторе. Если присутствует только один интерфейс, можно пользоваться любой командой.

## Dial-on-Demand Routing (DDR)

*Маршрутизация DDR (Dial-on-demand)*, вызов по запросу) позволяет нескольким маршрутизаторам Cisco вызывать коммутируемые соединения ISDN по мере надобности. Маршрутизация DDR пригодна только для непродолжительных сетевых подключений в обычных телефонных сетях PSTN (Public Switched Telephone Network, общественные коммутируемые телефонные сети) или сетях ISDN. DDR разработана для снижения стоимости при поминутном или по пакетному тарифе на услуги.

DDR начинает действовать после получения интерфейсом пакета, отвечающего требованиям списка доступа, который установлен администратором. Список доступа определяет так называемый "интересный" трафик (interesting traffic). Ниже перечислены пять основных концепций работы DDR при обслуживании полученного интерфейсом маршрутизатора "интересного" пакета:

1. Определение пути к сети назначения.
2. Интересный пакет предполагает вызов DDR.
3. Извлекается информация о наборе номера.
4. Пересылка трафика.
5. Вызов завершения операции, когда по связи передан весь трафик или истек период тайм-аута.

## Настройка DDR

Для настройки унаследованной маршрутизации DDR необходимо выполнить три задачи:

1. Определить статический путь, специфицирующий метод доступа к удаленной сети и используемый для этого интерфейс.
2. Определить в маршрутизаторе критерии для "интересного" трафика.
3. Настроить информацию вызова для набора номера, используемого интерфейсом для доступа к удаленной сети.

## Настройка статических путей

Для направления трафика в связь ISDN необходимо настроить статические пути во всех маршрутизаторах. Можно сконфигурировать протокол динамической маршрутизации для связи ISDN, но такое подключение никогда не будет прерываться. Поэтому рекомендуется метод маршрутизации со статическими путями. Для таких путей характерно следующее:

- Все участвующие маршрутизаторы обязаны иметь статические пути ко всем известным им сетям.
- Маршрутизация по умолчанию может применяться только в тупиковых областях сети.

Пример статической маршрутизации в сети ISDN:

```
RouterA(config)#iproute 172.16.50.0 255.255.255.0 172.16.60.2
RouterA(config)#iproute 172.16.60.2 255.255.255.255 bri0
```

Здесь маршрутизатору указано, что сеть 172.16.50.0 доступна через 172.16.60.2. Во второй строке маршрутизатору задан путь к сети 172.16.60.2.

## Указание "интересного" трафика

После создания таблиц путей в каждом маршрутизаторе необходимо настроить маршрутизатор на состав информации, передаваемой в линию ISDN. Для определения "интересных" пакетов администратор должен использовать команду глобального конфигурирования dialer-list.

Пример команды, включающей весь трафик IP:

```
804A(config)#dialer-list 1 protocol ip permit
804A(config)#int bri0
804A(config-if)#dialer-group 1
```

Команда dialer-group устанавливает список доступа для интерфейса BRI. В dialer-list можно использовать улучшенный список доступа для описания "интересного" трафика на основе приложений.

## Настройка информации о набираемом номере

Настройка информации о набираемом номере состоит из пяти операций.

1. Выбор интерфейса.
2. Установка IP-адреса.
3. Настройка типа инкапсуляции.
4. Связывание "интересного" трафика с интерфейсом.
5. Настройка набираемого номера(ов).

Пример всех пяти операций:

```
804A#config t
```

```
804A(config)#int bri0
804A(config-if)#ip address 172.16.60.1 255.255.255.0
804A(config-if)#no shut
804A(config-if)#encapsulation ppp
804A(config-if)#dialer-group 1
804A(config-if)#dialer-string 8350661
```

Вместо команды `dialer-string` можно пользоваться `dialer map`, обеспечивающей больший уровень безопасности.

```
804A(config-if)#dialer map ip 172.16.60.2 name 804B 8350661
```

Команда `dialer map` может использоваться совместно с `dialer-group`, причем соответствующий список доступа применяется для инициализации вызова. Команда `dialer map` пользуется IP-адресом маршрутизатора следующего участка, именем хоста удаленного маршрутизатора для аутентификации и номером, который будет набран для доступа к удаленному маршрутизатору.

Пример настройки в маршрутизаторе 804:

```
804B#sh run
Building configuration...
Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 804B
!
ip subnet-zero
!
isdn switch-type basic-ni
!
interface Ethernet0
ip address 172.16.50.10 255.255.255.0
no ip directed-broadcast
!
interface BRIO
ip address 172.16.60.2 255.255.255.0
no ip directed-broadcast
encapsulation ppp
dialer idle-timeout 300
dialer string 8358661
```

```

dialer load-threshold 2 either
dialer-group 1
isdn switch-type basic-ni
isdn spid1 0835866201 8358662
isdn spid2 0835866401 8358664
hold-queue 75 in
!
ip classless
ip route 172.16.30.0 255.255.255.0 172.16.60.1
ip route 172.16.60.1 255.255.255.255 BRI0
!
dialer-list 1 protocol ip permit
!
```

Интерфейс **BRI** использует инкапсуляцию **PPP** и тайм-аут длиной в 300 с. Команда `load-threshold` гарантирует немедленное включение интерфейсов **BRI** (если оплачены оба, то и использоваться они должны **оба**). Единственное, что следует отметить особо, — это команда `dialer-group 1`. Используемый номер должен совпадать с номером в списке вызовов. Параметр `hold-queue 75` в команде указывает маршрутизатору, что после получения "интересного" пакета следует сохранить его в очереди длиной до 75 пакетов для ожидания доступа к **BRI**. Если в очереди появится более 75 пакетов до создания связи, то лишние пакеты отбрасываются.

## Необязательные команды

Существуют еще две команды для настройки интерфейса **BRI**: `dialer load-threshold` и `dialer idle-timeout`

Команда `dialer load-threshold` указывает интерфейсу **BRI**, когда следует создавать второй канал **B**. Первый параметр команды имеет значение из диапазона 1 — 255, причем 255 устанавливает, что второй канал **B** создается только после 100% загрузки первого канала. Второй параметр имеет значения `in`, `out` или `either`, который определяет подсчет нагрузки интерфейса для выходного, входного или любого из этих трафиков. По умолчанию используется `out` (**outbound**).

Команда `dialer idle-timeout` устанавливает интервал в секундах перед разрывом соединения, когда послан последний "интересный" трафик. Значение по умолчанию равно 120 с.

```

RouterA(config-if)#dialer load-threshold 125 either
RouterA(config-if)#dialer idle-timeout 180
```

Команда `dialer load-threshold 125` устанавливает в интерфейсе **BRI** то, что второй канал **B** создается при 50% нагрузке по входному или выходному трафику. Команда `dialer idle-timeout 180` изменит установленное по умолчанию время разрыва соединения со 120 на 180 с.

## DDR со списками доступа

Списки доступа позволяют более точно указать "интересный" трафик. В предыдущем примере мы установили список вызова, разрешающий передавать в линию любой трафик IP. Этот режим полезен во время тестирования, но не пригоден для реального применения линии DDR. Воспользуемся улучшенным списком доступа для ограничения трафика только службами электронной почты и Telnet.

Пример установки списка вызова на основе списка доступа:

```
804A(config)#dialer-list 1 list 110
804A(config)#access-list 110 permit tcp any any eq smtp
804A(config)#access-list 110 permit tcp any any eq telnet
804A(config)#int bri0
804A(config-if)#dialer-group 1
```

В примере использована команда dialer-list для просмотра списка доступа. Так можно поступить не только с протоколом IP, но и с любым другим. Сначала создается список, а затем он применяется к интерфейсу BRI командой dialer-group.

## Проверка работы ISDN

Ниже перечислены команды для проверки унаследованной маршрутизации DDR и ISDN:

**Ping и Telnet** Прекрасно подходят для проверки IP в любой сети. Однако "интересный" трафик должен быть построен так, чтобы в нем допускались Ping и Telnet для создания связи. После создания связи можно проверить по ping или telnet удаленный маршрутизатор вне зависимости от списка "интересного" трафика.

**Show dialer** Выводит подробную информацию о номеронабирателе, причем будет показано количество времени для достижения строки набора номера, длина вызова, а также имя маршрутизатора, к которому подключен интерфейс.

**Show isdn active** Показывает вызванный номер и процедуру выполнения этого вызова.

**Show isdn status** Хорошая проверка перед реальным вызовом. Показывает, корректен ли идентификатор SPID, а также можно ли соединиться и взаимодействовать с информацией уровней от 1 до 3 в переключателе провайдера.

**Sho ip route** Показывает все известные маршрутизатору пути.

**Debug isdn q921** Показывает только информацию уровня 2.

**Debug isdn q931** Показывает информацию уровня 3, включая сведения об установке вызова и его разделении.

**Debug dialer** Задает установку вызова и действия по его разделению.

**Isdn disconnect int bri0** Очищает интерфейс и обрывает соединение. Выполнение в интерфейсе команды shutdown дает те же самые результаты.

## Упражнение

---

1. Напишите команду вывода метода инкапсуляции в интерфейсе serial 0 маршрутизатора Cisco.
2. Напишите команду настройки s0 на инкапсуляцию PPP.
3. Напишите команду настройки на имя пользователя todd и пароль cisco для маршрутизатора Cisco.
4. Напишите команду разрешения аутентификации CHAP в интерфейсе Cisco BRI.
5. Напишите команду настройки номеров DLCI для двух последовательных интерфейсов 0 и 1. Значение 16 для s0 и 17 для s1.
6. Напишите команду настройки удаленного офиса на подинтерфейс "точка-точка". Значение dlc1 16 и IP-адрес 172.16.60.1/24. Сеть IPX с номером 16.
7. Напишите команду установки типа переключателя в значение basic-ni для интерфейса BRI маршрутизатора Cisco.
8. Установите тип переключателя в маршрутизаторе Cisco на уровне интерфейса.
9. Напишите команду описания "интересного" трафика для установки связи ISDN так, чтобы она действовала на весь трафик IP.
10. Напишите команды применения в маршрутизаторе Cisco из п. 9.
11. Напишите команды настройки информации о наборе номера в маршрутизаторе Cisco.
12. Напишите команды установки при наборе номера порогового уровня и времени холостого хода.
13. Напишите команды установки очереди пакетов длиной 75 пакетов для "интересного" трафика так, чтобы реализовать ожидание создания *линии* ISDN.
14. Напишите пять операций настройки информации о наборе номера.
15. Напишите пять операций по базовому описанию работы DDR при обслуживании "интересного" трафика в интерфейсе маршрутизатора.

## Лабораторные работы

Настроим маршрутизатор Cisco на четыре разные региональные сети.

### О Лабораторная работа 10.1.

#### Настройка инкапсуляции PPP и аутентификации

По умолчанию маршрутизатор Cisco использует протокол High-Level Data Link Control (HDLC) в качестве метода инкапсуляции для связей "точка-точка" в последовательных линиях. При подключении к оборудованию не-Cisco необходимо использовать инкапсуляцию PPP.

Лабораторная работа проводится согласно рис. 10.8.

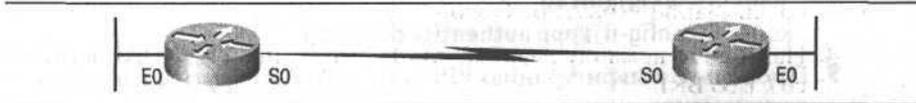


Рис. 10.8. Настройка PPP

1. Введите `sh int s0` в маршрутизаторах А и В, чтобы просмотреть методы инкапсуляции.
2. Проверьте, что каждый маршрутизатор имеет присвоенное им имя хоста:

```
RouterA#config t
RouterA(config)#hostname RouterA

RouterB#config t
RouterB(config)#hostname RouterB
```

3. Для изменения метода инкапсуляции по умолчанию (HDLC) на PPP в обоих маршрутизаторах примените команду `encapsulation` в режиме конфигурации интерфейса. На обоих концах соединения должен быть установлен один и тот же метод инкапсуляции.

```
RouterA#Config t
RouterA(config)#Ints0
RouterA(config)#Encap ppp
```

4. В маршрутизаторе В установите в `serial 0` инкапсуляцию PPP.

```
RouterB#config t
RouterB(config)#int s0
RouterB(config)#encap ppp
```

5. Проверьте конфигурацию обоих маршрутизаторов командой `sh int s0`.
6. Обратите внимание на IPSP, IPXSP и CDPSP. Эта информация служит для передачи данных протоколов верхнего уровня ( сетевого уровня) по ISO HDLC на подуровень MAC.

- Установите имя пользователя и пароль на каждом маршрутизаторе. Именем пользователя должно быть имя удаленного маршрутизатора. Кроме того, пароли обязаны быть **ОДИНАКОВЫМИ**.

```
RouterA#config t
```

```
RouterA(config)#username RouterB password todd
```

```
RouterB#config t
```

```
RouterB(config)#username RouterA password todd
```

- Разрешите аутентификацию CHAP или PAP в каждом интерфейсе.

```
RouterA(config)#ints0
```

```
RouterA(config-if)#ppp authentication chap
```

```
RouterB(config)#ints0
```

```
RouterB(config-if)#ppp authentication chap
```

- Проверьте конфигурацию PPP в каждом маршрутизаторе с помощью двух команд:

```
sh int s0
```

```
debug PPP authentication
```

## О Лабораторная работа 10.2.

### *Настройка и мониторинг HDLC*

Пока не настроен протокол HDLC. Однако после завершения лабораторной работы 10.1 в обоих маршрутизаторах должна быть установлена инкапсуляция PPP. Именно поэтому настройка PPP сделана в первой лабораторной работе — теперь можно конфигурировать инкапсуляцию HDLC в маршрутизаторе.

**▼ ВНИМАНИЕ** | Вторая лабораторная работа проводится согласно рис. 10.8 из лабораторной работы 10.1.

- Командой `encapsulation hdlc` установите инкапсуляцию в каждом последовательном интерфейсе.

```
RouterA#config t
```

```
RouterA(config)#ints0
```

```
RouterA(config-if)#encapsulation hdlc
```

```
RouterB#config t
```

```
RouterB(config)#ints0
```

```
RouterB(config-if)#encapsulation hdlc
```

- Проверьте инкапсуляцию HDLC командой `show interface s0` в каждом маршрутизаторе.

### О Лабораторная работа 10.3. Настройка Frame Relay и подинтерфейсов

Лабораторная работа 10.3 проводится согласно рис. 10.9, где указаны параметры настройки Frame Relay.

На учебных курсах в качестве переключателя кадров обычно используют маршрутизатор серии 2522, который имеет 10 последовательных портов. Однако вполне допустимо использование трех маршрутизаторов 2501.

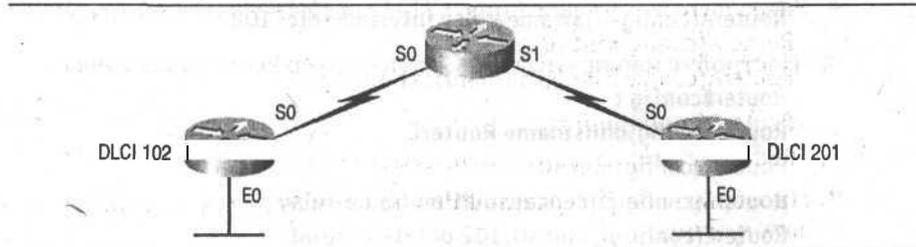


Рис. 10.9. Настройка Frame Relay

1. Командой `frame-relay switching` установите имя хоста и тип инкапсуляции во всех последовательных интерфейсах переключателя Frame Relay.

```
Router#config t
Router(config)#hostname RouterB
RouterB(config)#frame-relay switching
RouterB(config)#ints 0
RouterB(config-if)#encapsulation frame-relay
RouterB(config-if)#ints 1
RouterB(config-if)#encapsulation frame-relay
```

2. В каждом интерфейсе настройте отображение Frame Relay. Не обязательно устанавливать IP-адреса в этих интерфейсах, поскольку предполагается только коммутация кадров Frame Relay из одного интерфейса в другой.

```
RouterB(config-if)#ints 0
RouterB(config-if)#frame-relay route 102 interface Serial1 201
RouterB(config-if)#frame intf-type dce
RouterB(config-if)#ints 1
RouterB(config-if)#frame-relay route 201 interface Serial0 102
RouterB(config-if)#frame intf-type dce
```

Команда `route` показывает, что полученные в PVC 102 кадры передаются в интерфейс `int s1` с цепью PVC 201. Противоположное действие выполняет второе отображение в `serial 1`. Все, что поступает в `int s1`, маршрутизируется в `serial 0` с цепью PVC 102.

3. Настройте маршрутизатор А на подинтерфейс "точка-точка".

```
Router#config t
Router(config)#hostname RouterA
RouterA(config)#ints0
RouterA(config-if)#encapsulation frame-relay
RouterA(config-if)#int s0.102 point-to-point
RouterA(config-if)#ipaddress 172.16.10.1 255.255.255.0
RouterC(config-if)#ipx network 10
RouterA(config-if)#frame-relayinterface-did 102
```

4. Настройте маршрутизатор С на подинтерфейс "точка-точка".

```
Router#config t
Router(config)#hostname RouterC
RouterC(config)#int s0
RouterC(config-if)#encapsulationframe-relay
RouterC(config-if)#int s0.102 point-to-point
RouterC(config-if)#ip address 172.16.10.2 255.255.255.0
RouterC(config-if)#ipx network 10
RouterC(config-if)#frame-relay interface-dlci 201
```

5. Проверьте конфигурацию командами:

```
RouterA>sho frame ?
ip show frame relay IP statistics
lmi show frame relay lmi statistics
map Frame-Relay map table
pvc show frame relay pvc statistics
routes how frame relay route
traffic Frame-Relay protocol statistics
```

6. Кроме того, проверьте соединения с помощью Ping и Telnet.

## О Лабораторная работа 10.4.

### *Настройка ISDN и интерфейсов BRI*

Данная лабораторная работа выполняется согласно рис. 10.10, который показывает конфигурацию и мониторинг ISDN в маршрутизаторе Cisco. Мы настроим маршрутизаторы 804А и 804В для коммутируемых вызовов ISDN между сетями 172.16.30.0 и 172.16.50.0 с помощью сети 172.16.60.0 в интерфейсе ISDN BRI.

1. В устройстве 804В установите имя хоста и тип переключателя ISDN.

```
Router#Config t
Router(config)#hostname 804B
804B(config)#isdn switch-type basic-ni
```



Рис. 10.10. Настройка ISDN

2. На уровне интерфейса установите имя хоста и тип переключателя в 804A. Обратите внимание на строки 1 и 2, где показана возможность настройки типа переключателя в режимах глобального конфигурирования и на уровне интерфейса.

```
Router#Config t
Router(config)#hostname 804A
804A(config)#int bri0
804B(config-if)#isdnswitch-type basic-ni
```

3. В устройстве 804A установите номер SPID в BRI 0 и IP-адрес 171.16.60.1/24. Если есть реальное подключение к сети ISDN или имитатору ISDN, введите номера SPID.

```
804a#config t
804A(config)#int bri0
804A(config-if)#isdnspid 1 0835866101 ldn8358661
804A(config-if)#isdnspid 2 0835866301 ldn8358663
804A(config-if)#ipaddress 172.16.60.1 255.255.255.0
804A(config-if)#no shut
```

4. Установите номер SPID в 804B и укажите для интерфейса IP-адрес 172.16.60.2/24.

```
804A#config t
804A(config)#int bri0
804A(config-if)#isdnspid 1 0835866201 ldn8358662
804A(config-if)#isdnspid 2 0835866401 ldn8358664
804A(config-if)#ipaddress 172.16.60.2 255.255.255.0
804A(config-if)#no shut
```

5. Создайте в маршрутизаторе статические пути для удаленных интерфейсов ISDN. Динамическая маршрутизация приведет к двум проблемам: (1) линия ISDN всегда будет включена и (2) возникнет сетевая петля, поскольку между областями появятся несколько связей. На экзамене CCNA достаточно знать о протоколах маршрутизации по вектору расстояния (RIP и IGRP). Для ISDN рекомендуется статическая маршрутизация.

```
804A(config)#iproute 172.16.50.0255.255.255.0 172.16.60.2
```

```
804A(config)#iproute 172.16.60.2 255.255.255.255 bri0
```

```
804B(config)#iproute 172.16.30.0 255.255.255.0 172.16.60.1
```

```
804B(config)#iproute 172.16.60.1 255.255.255.255 bri0
```

6. Укажите "интересный" трафик для линии ISDN. Выберите для этого весь трафик IP. Команду следует вводить в режиме глобального конфигурирования.

```
804A(config)#dialer-list 1 protocol ip permit
```

```
804B(config)#dialer-list 1 protocol ip permit
```

7. В интерфейсах BRI обоих маршрутизаторов добавьте команду dialer-group 1, которая должна быть согласована с номером списка вызовов.

```
804B(config)#config t
```

```
804B(config)#int bri0
```

```
804B(config)#dialer-group 1
```

8. Настройте в обоих маршрутизаторах информацию о наборе номеров.

```
804A#Config t
```

```
804A(config)#Int bri0
```

```
804A(config-if)#Dialerstring 8358662
```

```
804B#Config t
```

```
804B(config)#Int bri0
```

```
804B(config-if)#Dialerstring 8358661
```

9. Установите границу нагрузки командой dialer load-threshold и выполните команду multilink, а также укажите процентное соотношение холостого времени (idle-time) в обоих маршрутизаторах 804.

```
804A#Config t
```

```
804A(config)#int bri0
```

```
804B(config-if)#Dialerload-threshold 125 either
```

```
804B(config-if)#Dialer idle-timeout 180
```

```
804B#Config t
```

```
804B(config)#int bri0
```

```
804B(config-if)#Dialer load-threshold 125 either
```

```
804B(config-if)#Dialer idle-timeout 180
```

10. Установите очередь хранения пакетов так, чтобы при обнаружении "интересного" трафика выполнялась задержка перед установлением связи ISDN.

```
804A#Config t
```

```
804A(config)#int bri0
```

```
804B(config-if)#hold-queue 75 in
```

```
804B#Config t
```

```
804B(config)#int bri0
```

```
804B(config-if)#hold-queue 75 in
```

**11.** Проверьте соединение ISDN.

Ping

Telnet

Show dialer

**Show isdn status**

Sh iproute

## Проверочные вопросы

- Какие протоколы поддерживают PPP?
  - HDLC
  - LCP**
  - SDLC
  - NCP
  - LAPB
- Когда следует использовать ISDN?
  - Для соединения с большими ЭВМ компании IBM
  - Для соединения локальных сетей (LAN) с помощью цифровых служб с неодинаковыми носителями
  - Для поддержки приложений, которым необходимы высокоскоростные передачи голоса, видео и данных
  - Когда требуется согласованность и высокая скорость передачи данных
- Сколько типов инкапсуляции Frame Relay доступны в маршрутизаторе Cisco?
  - Два
  - Три
  - Четыре**
  - Пять
- Сколько доступно типов LMI?
  - Два
  - Три
  - Четыре**
  - Пять
- Что справедливо для Frame Relay?
  - Необходимо использовать инкапсуляцию Cisco для подключения к оборудованию не-Cisco.

- B.** Необходимо использовать инкапсуляцию ANSI для подключения к оборудованию не-Cisco.
  - C.** Необходимо использовать инкапсуляцию IETF для подключения к оборудованию не-Cisco.
  - D.** Необходимо использовать инкапсуляцию Q.933A для подключения к оборудованию не-Cisco.
6. Каков тип LMI по умолчанию?
- A.** Q.933A
  - B.** ANSI
  - C.** IETF
  - D.** Cisco
7. Что из перечисленного использует цепи PVC на уровне 2?
- A.** X.25
  - B.** ISDN
  - C.** Frame Relay
  - D.** HDLC
8. Какой префикс протоколов ISDN определяет коммутацию?
- A.** I
  - B.** E
  - C.** S
  - D.** Q
9. Какая команда покажет номера DLCI, сконфигурированные в сети Frame Relay? (Укажите все правильные ответы.)
- A.** sh frame-relay
  - B.** show running
  - C.** sh intsO
  - D.** sh frame-relay dlci
  - E.** sh frame-relay pvc
10. Для чего используется IARP?
- A.** Отображение адресов X.121 на адреса X.25
  - B.** Отображение DLCI на адреса сетевого протокола
  - C.** Для адресации SMDS
  - D.** Отображение адресов ATM на виртуальные адреса
11. Что в ISDN обеспечивает интерфейс Basic Rate Interface (BRI)?
- A.** 23 канала B и один канал D на скорости 64 Кбит/с
  - B.** Общую битовую скорость до 1544 Мбит/с
  - C.** Два канала B на скорости 56 Кбит/с и один канал D на скорости 64 Кбит/с
  - D.** Два канала B на скорости 64 Кбит/с и один канал D на скорости 16 Кбит/с

12. Что справедливо для номеров DLCI в Frame Relay?
  - A. DLCI необязательны в сетях Frame Relay.
  - B. DLCI представляют отдельные физические цепи.**
  - C. DLCI идентифицируют логические соединения между устройствами DTE.
  - D. DLCI используются для маркировки начала кадров, когда кадр коммутируется в локальной сети.
13. Какая команда выводит все сконфигурированные PVC и DLCI?
  - A. sh frame pvc
  - B. sh frame**
  - C. sh frame lmi
  - D. sh pvc
14. Какова инкапсуляция по умолчанию для связи "точка-точка" между двумя маршрутизаторами Cisco?
  - A. SDLC
  - B. HDLC**
  - C. Cisco
  - D. ANSI
15. Какая информация предоставляется интерфейсом Local Management Interface? (Укажите все правильные ответы)
  - A. Статус виртуальной цепи**
  - B. Текущее значение DLCI**
  - C. Глобальное или локальное действие значения DLCI**
  - D. Тип инкапсуляции LMI**
16. Какой протокол, используемый в PPP, позволяет применить во время соединения несколько протоколов сетевого уровня?
  - A. LCP
  - B. NCP**
  - C. HDLC
  - D. X.25
17. Какой протокол используется в PPP для установки, настройки и аутентификации подключения по связи данных?
  - A. LCP
  - B. NCP**
  - C. HDLC
  - D. X.25
18. Что в Frame Relay идентифицирует PVC?
  - A. NCP
  - B. LMI**

- C. IARP
  - D. DLCI
19. Что справедливо для LMI?
- A. LMI отображает номера DLCI на виртуальные цепи.
  - B. LMI отображает адреса X.121 на виртуальные цепи.
  - C. LMI выводит статус виртуальной цепи.
  - D. Сообщения LMI предоставляют информацию о текущем значении DLCI.
20. Что содержит управляющую информацию Frame Relay?
- A. DLCI
  - B. IARP
  - C. LMI
  - D. BECN

## Ответы к упражнению

---

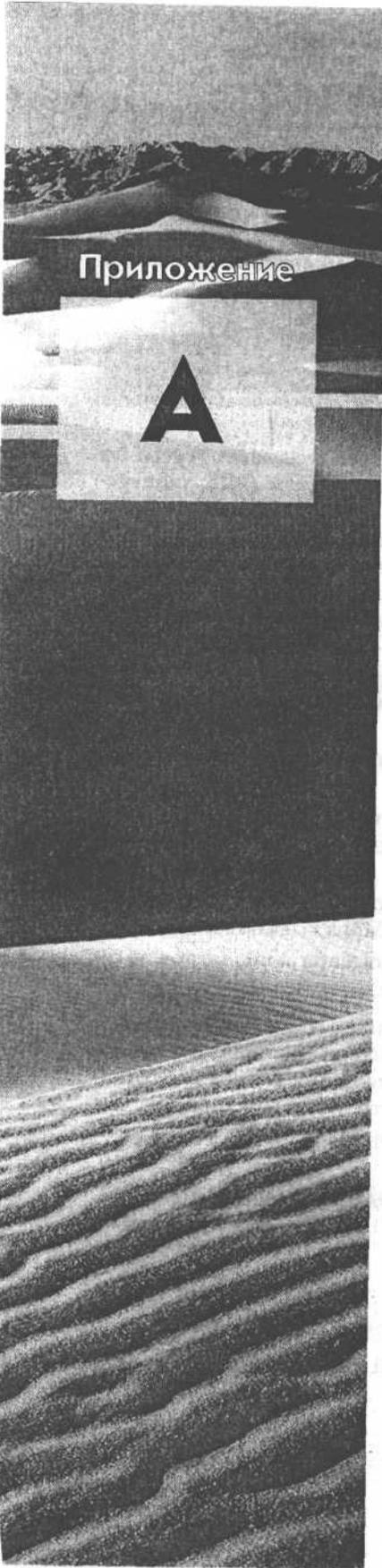
1. sh int s0
2. Config t  
Int s0  
Encap ppp
3. Config t  
username todd password Cisco
4. Config t  
int bri0  
ppp authentication chap
5. Config t  
Ints0  
Frame interface-dlci 16  
Ints1  
Frame interface-dlci 17
6. config t  
int s0  
encap frame  
int s0.16 point-to-point  
ip address 172.16.60.1255.255.255.0  
ipx netw 16  
frame interface-dlci 16
7. Config t  
Isdn switch-type basic-ni
8. Config t Interface bri 0 Isdn switch-type basic-ni

- 9. Router(config)#dialer-list 1 protocol ip permit**
- 10.** config t  
int bri0  
dialer-group 1
- 11. Config t Int bri0 Dialer string 8358662**
- 12. Config t**  
Int bri0  
Dialer load-threshold 125 either  
Dialer idle-timeout 180
- 13. Config t**  
Int bri0  
Hold-queue 75 in
- 14.** 1. Выбор интерфейса  
2. Установка IP-адреса  
3. Настройка типа инкапсуляции  
4. Связывание "интересного" трафика с интерфейсом  
5. Настройка номера(ов) для вызова
- 15.** 1. Определение пути к сети назначения.  
2. "Интересный" пакет инициирует (предписывает) вызов DDR.  
3. Извлекается информация о набираемых номерах.  
4. Передается трафик.  
5. Вызов завершается, когда по связи передан весь трафик или закончился период тайм-аута.

## Ответы на проверочные вопросы

- |             |             |
|-------------|-------------|
| 1. A, B и D | 11. D       |
| 2. C        | 12. C       |
| 3. A        | 13. A       |
| 4. B        | 14. B       |
| 5. C        | 15. A, B, C |
| 6. D        | 16. B       |
| 7. C        | 17. A       |
| 8. D        | 18. D       |
| 9. B, E     | 19. C, D    |
| 10. B       | 20. D       |





Приложение

**A**

## Пример сертификационного экзамена

Вопросы для экзамена

1. Как называется процесс, при котором...

2. Какие факторы влияют на...

3. Каким образом можно...

4. Какие методы используются...

5. Какими способами можно...

6. Какие задачи решаются...

7. Какими инструментами...

8. Какими методами...

9. Какими способами...

10. Какими методами...

## Вопросы сертификационного экзамена

1. Какой протокол используется в PPP для идентификации протокола сетевого уровня?
  - A. NCP
  - B. ISDN**
  - C. HDLC
  - D. LCP
2. Крупная компания по разработке приложений оказывает услуги по созданию управленческих информационных систем (MIS, management information system). Компания имеет четыре совместно используемых концентратора по 10 Мбит/с для сетевого доступа к серверу NT. Для обеспечения **бизнес-требований** необходима поддержка разных типов хостов, чтобы тестировать разрабатываемые приложения. Хосты должны обмениваться данными между собой и корпоративным сервером. Хосты работают на скорости 10 Мбит/с, а сервер — на 100 Мбит/с. Приложениям не требуется полоса пропускания выше 3 Мбит/с. Что можно рекомендовать компании, если она имеет ограниченный бюджет?
  - A. Заменить концентраторы 10 Мбит/с на концентраторы 100 Мбит/с.**
  - B. Установить маршрутизатор и подключить все концентраторы в отдельные домены конфликтов, но в один общий ширококвещательный домен.
  - C. Установить переключатель уровня 2, сформировав соединения 10 Мбит/с с хостами и соединения 100 Мбит/с с сервером.
  - D. Использовать мосты для разделения доменов конфликтов и создания одного большого ширококвещательного домена.
3. Напишите команду настройки маршрутизации IPX в маршрутизаторе Cisco с двумя **интерфейсами**. Первый интерфейс подключен к локальной сети Ethernet и должен поддерживать 802.3 и 802.2. Второй интерфейс подключен к региональной сети WAN и использует инкапсуляцию HDLC. Применяйте любой произвольный номер сети IPX.
4. Что позволяет предпринять команда `routerA(config)#line cons 0`?
  - A. Установить пароль Telnet.**
  - B. Выключить маршрутизатор.
  - C. Установить пароль консоли.
  - D. Отменить консольное соединение.
5. Какая команда ISDN устанавливает второй интерфейс BRI при 50% нагрузке?
  - A. `load balance 50`
  - B. `load share 50`**

- C. dialer load-threshold 125
  - D. dialer idle-timeout 125
6. Какой протокол из набора PPP обеспечивает динамическую адресацию, аутентификацию и режим нескольких связей?
- A. NCP
  - B. HDLC**
  - C. LCP
  - D. X.25
7. Какая команда выводит сведения о линии, протоколе, DLCI и информации LMI для интерфейса?
- A. sh pvc
  - B. show interface**
  - C. show frame-relay pvc
  - D. sho runn
8. Списки доступа какого типа используют номера 1 — 99?
- A. Стандартный IP**
  - B. Стандартный IPX**
  - C. Улучшенный IP
  - D. Улучшенный IPX
  - E. Фильтр IPX SAP**
9. Что устанавливает команда passive в динамическом протоколе маршрутизации?
- A. Отменяет в интерфейсе отправку или получение периодических динамических обновлений**
  - B. Отменяет в интерфейсе отправку периодических динамических обновлений, но сохраняет получение обновлений**
  - C. Отменяет в маршрутизаторе получение любых динамических обновлений
  - D. Отменяет в маршрутизаторе отправку любых динамических обновлений
10. Каким протоколом пользуется Ping?
- A. TCP
  - B. ARP**
  - C. ICMP
  - D. BootP
11. Напишите команду для вывода информации IPX RIP и SAP, получаемой и отправляемой маршрутизатором.
12. Какая команда устанавливает пароль Telnet в маршрутизаторе Cisco?
- A. Line telnet 0 4
  - B. Line aux 0 4**

- C. Line vty 0 4
  - D. Line con 0
13. Какая команда создает в переключателе серии 1900 виртуальную локальную сеть VLAN 5 с идентификатором Marketing?
- A. 1900A#vlan 5 name Marketing
  - B. 1900A(config)#vlan name Marketing 5
  - C. 1900A(config)#vlan 5 name Marketing
  - D. 1900A(config)# Marketing vlan 5
14. Какой порт моста является корневым?
- A. Порт с наименьшей стоимостью к корневому мосту
  - B. Порт с наибольшей стоимостью к корневому мосту
  - C. Любой активный порт
  - D. Любой порт 100 Мбит/с
15. Что нужно ввести для стирания конфигурации в NVRAM?
- A. Erase startup
  - B. Erase nvram
  - C. Delete nvram
  - D. Erase running
16. Напишите команду создания второй сети IPX с типом кадров SNAP в интерфейсе Ethernet 0.
17. Какой класс IP-адресов по умолчанию имеет наибольшее количество хостов?
- A. А
  - B. В
  - C. С
  - D. А и В
18. Как часто элементы BPDU отсылаются из устройства уровня 2?
- A. Никогда
  - B. Каждые две секунды
  - C. Каждые 10 минут
  - D. Каждые 30 с
19. Что справедливо для виртуальных локальных сетей VLAN? (Выберите все подходящие ответы.)
- A. Во всех переключателях Cisco по умолчанию конфигурируются две сети VLAN.
  - B. Сеть VLAN действует только в полных коммутируемых объединенных сетях Cisco. Не допускаются переключатели, работающие вне основной полосы пропускания.

- C. Нельзя получить более 10 переключателей в одном домене VTP.  
D. VTP используется для передачи информации VLAN в переключатели сконфигурированного домена VTP.
20. Какой режим коммутации локальных сетей минимизирует количество ошибок CRC, но сохраняет фиксированный уровень запаздывания?
- A. STP
  - B. Store and forward (сохранить и передать)
  - C. Cut-through (сквозной)
  - D. FragmentFree
21. Сколько широковещательных доменов создается в сети с 12-портовым переключателем?
- A. Один
  - B. Два
  - C. Пять
  - D. 12
22. Какой элемент PDU соответствует транспортному уровню?
- A. Пользовательских данных
  - B. Сеанса
  - C. Сегмента
  - D. Кадра
23. Какой протокол служит для настройки магистральных сетей в переключателе? (Укажите все правильные ответы.)
- A. Virtual Trunk Protocol
  - B. VLAN
  - C. Trunk
  - D. ISL
24. Что такое тупиковая сеть (stub network)?
- A. Сеть с несколькими точками выхода
  - B. Сеть с несколькими точками входа и выхода
  - C. Сеть только с одной точкой входа, не имеющая точки выхода
  - D. Сеть только с одной точкой входа и выхода
25. Где в модели OSI определен концентратор?
- A. Сеансовый уровень
  - B. Физический уровень
  - C. Канальный уровень
  - D. Уровень приложений
26. Когда необходимо настроить порты в переключателе Cisco, то какие доступны способы для настройки членства в сети VLAN? (Выберите все правильные ответы.)

- A.** С помощью сервера DHCP
  - B.** Статические
  - C.** Динамические
  - D.** С помощью базы данных VTP
27. Что показывает команда `show controllers s 0`?
- A.** Тип подключения в последовательном порту (т.е. Ethernet или Token Ring)
  - B.** Тип подключения (т.е. DTE или DCE)
  - C.** Конфигурацию интерфейса, включая IP-адрес и тактовую частоту
  - D.** Управляющий процессор интерфейса
28. Какая команда из IOS версии ниже 10.3 копирует содержимое NVRAM в DRAM?
- A.** `config t`
  - B.** `config net`
  - C.** `config mem`
  - D.** `wr mem`
29. Какова главная причина для создания модели OSI?
- A.** Создать модель с уровнями, которая больше модели DoD
  - B.** Чтобы разработчики приложений могли изменять на каждом уровне только один протокол
  - C.** Чтобы могло взаимодействовать оборудование разных компаний-производителей
  - D.** Чтобы эту модель могла использовать компания Cisco
30. На каком уровне модели OSI перед передачей данных создаются виртуальные цепи между хостами?
- A.** Приложений
  - B.** Сеансов
  - C.** Транспортном
  - D.** Сетевом
  - E.** Канальном
31. Какой протокол транспортного уровня используется DHCP?
- A.** IP
  - B.** TCP
  - C.** UDP
  - D.** ARP
32. Как скопировать IOS из маршрутизатора на хост TFTP?
- A.** `copy run starting`
  - B.** `copy start running`
  - C.** `copy running tftp`
  - D.** `copy flash tftp`

33. Если маршрутизатор выступает как устройство CSU/DSU, то какая команда необходима для формирования в маршрутизаторе последовательной связи со скоростью 64000 бит?
- A. RouterA(config)#bandwidth 64
  - B. RouterA(config-if)#bandwidth 64000**
  - C. RouterA(config)#clockrate 64000
  - D. RouterA(config-if)clockrate 64
  - E. RouterA(config-if)clock rate 64000
34. Что из перечисленного обеспечивается на уровне распределения? (Выберите все правильные ответы.)
- A. Разделение доменов конфликтов**
  - B. Маршрутизация**
  - C. Списки доступа**
  - D. Сети VLAN
35. Какая команда устанавливает пароль Telnet в маршрутизаторе Cisco?
- A. Line telnet 0 4
  - B. Line aux 0 4**
  - C. Line vty 0 4**
  - D. Line con 0
36. Какая команда устанавливает пароль разрешенного секрета в маршрутизаторе Cisco?
- A. RouterA(config)#enable password todd
  - B. RouterA(config)#enable secret todd**
  - C. RouterA(config)#enablesecret password todd**
  - D. RouterA(config-if)#enable secret todd
37. Какой протокол позволяет найти адрес Ethernet по известному IP-адресу?
- A. IP
  - B. ARP**
  - C. RARP**
  - D. BootP
38. Какая команда обновляет IOS в маршрутизаторе Cisco?
- A. copy tftp run
  - B. copy tftp start**
  - C. config net**
  - D. copy tftp flash
39. Какая команда копирует конфигурацию из памяти DRAM маршрутизатора в NVRAM?
- A. copy run start
  - B. copy start run**

- C. config net
  - D. config mem
  - E. copy flash nvram
40. Если интерфейс отключен административно, то в чем проблема?
- A. Интерфейс неисправен.
  - B. Интерфейс не подключен к другому устройству.
  - C. Проблемы не существует.
  - D. Интерфейс заиклен.
41. Если в анализаторе Ethernet обнаружен кадр ISL с размером больше обычного кадра Ethernet, то какой размер покажет анализатор?
- A. 1518
  - B. 1522
  - C. 4202
  - D. 8190
42. Сколько доменов конфликтов создается при сегментировании сети с помощью 12-портового переключателя?
- A. Один
  - B. Два
  - C. Пять
  - D. 12
43. Каково по умолчанию административное расстояние статического пути?
- A. 0
  - B. 1
  - C. 10
  - D. 100
44. Каково первое из возможных решений проблемы счета до бесконечности?
- A. Удержание
  - B. Тригерное обновление
  - C. Установка максимального значения счетчика участков
  - D. Опасный реверс
45. Какой протокол возвращает хосту сообщение Destination Network Unknown (сеть назначения неизвестна)?
- A. TCP
  - B. ARP
  - C. ICMP
  - D. BootP

46. Каково расстояние линии для устройства 1000BaseSX MMF с 62.5- и 50-микронным ядром и лазером 780-нм?
- A. 100 метров
  - B. 260 метров
  - C. 400 метров
  - D. 1000 футов
47. На каком уровне возникают пакеты?
- A. Сеансовом
  - B. Транспортном
  - C. Сетевом
  - D. Канальном
48. Каково одно из преимуществ статических путей в сравнении с динамическими?
- A. Быстрая конвергенция
  - B. Не используется центральный процессор
  - C. Не используется полоса пропускания
  - D. Безопасность
49. Как скопировать в DRAM конфигурацию, хранящуюся на хосте TFTP?
- A. copy run start
  - B. copy start run
  - C. copy tftp flash
  - D. copy tftp running
50. Как создать динамическую сеть VLAN?
- A. Использовать статическое членство
  - B. Нанять младшего администратора
  - C. С помощью сервера DHCP
  - D. С помощью сервера Management Policy Server сети VLAN
51. Какой тип списков доступа использует номера 100— 199?
- A. Стандартный IP
  - B. Стандартный IPX
  - C. Улучшенный IP
  - D. Улучшенный IPX
  - E. Фильтр IPXSAP
52. Напишите команду для добавления подинтерфейса в Ethernet 0 с типом кадров 802.3.
53. Какой протокол маршрутизации используется при выборе пути оценки полосы пропускания и задержки?
- A. RIP

- B.** Static
  - C.** IGRP
  - D.** OSPF
54. Какой тип списков доступа использует номера 1000 — 1099?
- A.** Стандартный IP
  - B.** Стандартный IPX
  - C.** Улучшенный IP
  - D.** Улучшенный IPX
  - E.** Фильтр IPX SAP
55. Какая команда IOS версии ниже 10.3 копирует конфигурацию из хоста TFTP в DRAM?
- A.** config t
  - B.** config net
  - C.** config mem
  - D.** wr mem
56. Какой командой настраивается маршрутизация по протоколу RIP?
- A.** RouterA#**routing** rip
  - B.** Router(config)#**routing** rip
  - C.** RouterA#**router** rip
  - D.** Router(config)#**router** rip
  - E.** router(config-router)#**router** rip
57. Какой тип списков доступа использует номера 800 — 899?
- A.** Стандартный IP
  - B.** Стандартный IPX
  - C.** Улучшенный IP
  - D.** Улучшенный IPX
  - E.** Фильтр IPX SAP
58. Какие две команды покажут все настроенные цепи PVC?
- A.** sh pvc
  - B.** show interface
  - C.** show frame-relay pvc
  - D.** sho runh
59. Если соединить маршрутизатор Cisco и маршрутизатор 3Com по линии T-1, то почему они не будут взаимодействовать при параметрах по умолчанию?
- A.** Устройства Cisco и 3Com несовместимы.
  - B.** 3Com была куплена Cisco.
  - C.** Инкапсуляции в последовательных линиях по умолчанию несовместимы.

- D. Типы кадров Ethernet по умолчанию несовместимы.
60. Что справедливо для крупной офисной сети Ethernet?
- A. Полнодуплексные соединения FastEthernet можно использовать на основе 10Base2.
  - B. Полнодуплексные соединения можно использовать в подключениях "точка-точка" между узлами.
  - C. Для полнодуплексных соединений допускается режим "сохранение и пересылка".
  - D. Можно использовать сквозной режим в полудуплексных соединениях.
61. Необходимо переслать большой файл из дома в офис компании. Делать это нужно быстро и периодически. Какую лучше выбрать технологию?
- A. Frame Relay
  - B. Ethernet
  - C. ISDN
  - D. Token Ring
  - E. ATM
62. Напишите команду показа действующих в сети серверов NetWare.
63. Какой протокол позволяет исключить петли на уровне 2?
- A. BPDU
  - B. STP
  - C. VLAN
  - D. Переключатели
64. Напишите команду для создания подинтерфейса в Ethernet 0 с типом кадров Ethernet\_II.
65. Какая команда в переключателе серии 1900 позволяет проверить настройку сети VLAN?
- A. Show config
  - B. Show vlan
  - C. Show vlan info
  - D. Sh startup-config
66. Для чего используется BECN?
- A. Аутентификация PPP
  - B. Балансировка нагрузки в интерфейсе BRI сети ISDN
  - C. Управление перегрузками в сети Frame Relay
  - D. Идентификация на сетевом уровне по протоколу HDLC
67. Напишите команду для вывода таблицы маршрутизации IPX.

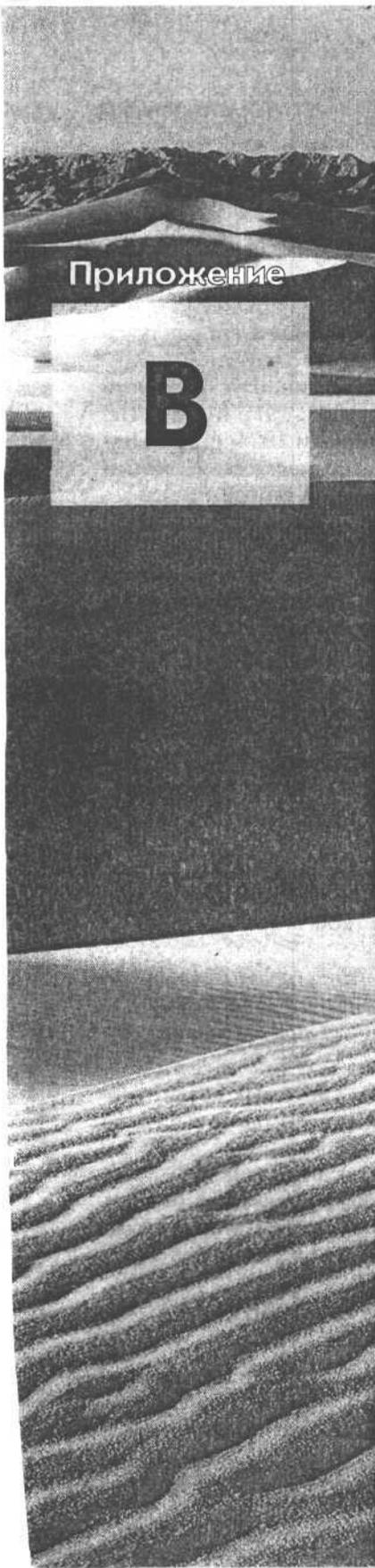
68. Каков корректный диапазон хостов для IP-адреса 192.168.168.188  
255.255.255.192?
- A.** 192.168.168.129 – 190
  - B.** 192.168.168.129 – 191
  - C.** 192.168.168.128 – 190
  - D.** 192.168.168.128 – 192
69. Какой тип списков доступа использует номера 900 – 999?
- A.** Стандартный IP
  - B.** Стандартный IPX
  - C.** Улучшенный IP
  - D.** Улучшенный IPX
  - E.** Фильтр IPX SAP
70. Сколько корневых мостов в сети с десятком переключателей?
- A.** Один
  - B.** Два
  - C.** Пять
  - D.** 12

## Ответы на вопросы сертификационного экзамена

---

1. A (см. главу 10)
2. C
3. **Config t**  
Ipx routing  
Int e0  
Ipx network 10  
Int e0.10  
Ipx network 10a encap sap  
Int s0  
Ipx network 20  
(см. главу 8)
4. C (см. главу 4)
5. C (см. главу 10)
6. C (см. главу 10)
7. B (см. главу 10)
8. A (см. главу 9)
9. B (см. главу 5)
10. C (см. главу 3)
11. **show ipx traffic**  
(см. главу 8)
12. C (см. главу 4)
13. C (см. приложение B)
14. A (см. главу 2)
15. A (см. главу 4)
16. **Config t**  
Ipx network 10c encap snap  
secondary  
(см. главу 8)
17. A (см. главу 3)
18. B (см. главу 2)
19. D (см. главу 6)
20. **D**(см. главу 2)
21. A (см. главу 2)
22. C (см. главу 1)
23. C, D (см. главу 6)
24. D (см. главу 5)
25. B (см. главу 1)
26. B, C (см. главу 6)
27. B (см. главу 4)
28. C (см. главу 7)
29. C (см. главу 1)
30. C (см. главу 1)
31. C (см. главу 3)
32. D (см. главу 7)
33. E (см. главу 4)
34. B, C, D (см. главу 1)
35. C (см. главу 4)
36. B (см. главу 4)
37. B (см. главу 3)
38. D (см. главу 7)
39. A (см. главу 7)
40. C (см. главу 4)
41. B (см. главу 6)
42. D (см. главу 2)
43. B (см. главу 5)
44. C (см. главу 5)
45. C (см. главу 3)
46. B (см. главу 1)
47. C (см. главу 1)
48. A (см. главу 5)
49. D (см. главу 7)
50. D (см. главу 6)
51. C (см. главу 9)
52. **Config t**  
Int e0.100  
Ipx network 10a encap  
novell-ether  
(см. главу 8)
53. C (см. главу 5)
54. E (см. главу 9)
55. B (см. главу 7)
56. D (см. главу 5)
57. B (см. главу 9)
58. C, D (см. главу 10)
59. C (см. главу 10)

- |                                              |                                     |
|----------------------------------------------|-------------------------------------|
| 60. В                                        | 65. В (см. приложение В).           |
| «1. С                                        | 66. С (см. главу 10)                |
| 62. show ipx servers<br>(см. главу 8)        | 67. show ipx route<br>(см. главу 8) |
| 63. В (см. главу 2)                          | 68. А (см. главу 3)                 |
| 64. Config t                                 | 69. D (см. главу 9)                 |
| Int e0.10                                    | 70. А (см. главу 2)                 |
| Ipx network 10b encaps agra<br>(см. главу 8) |                                     |



Приложение

**В**

# Настройка переключателя Catalyst 1900

**В** учебный курс CCNA по новому экзамену CCNA попал переключатель Cisco Catalyst 1900, поэтому нужно хорошо знать его работу.

Переключатели серии 1900 находятся в начале линейки устройств Cisco Catalyst. Поставляются две модели Catalyst 1900: 1912 и 1924. Переключатель 1912 имеет 12 портов ЮBaseT, а в модели 1924 присутствует 24 порта ЮBaseT. Каждая модель имеет две каскадные линии 100 Мбит/с на витых парах или волоконно-оптическом кабеле.

Переключатели 1900 теперь исполняют Cisco IOS, поэтому такие устройства помогут изучить все модели переключателей компании Cisco. Не все переключатели Cisco исполняют IOS, но это временное явление.

В данном приложении мы рассмотрим запуск и настройку переключателя Cisco Catalyst 1900 через интерфейс командной строки CLI (Command-Line Interface). Сначала опишем процесс подключения консольного кабеля, затем обсудим процесс включения устройства 1900, после этого перейдем к основным конфигурационным командам переключателя 1900.

Познакомившись с командами настройки, мы изучим процедуры конфигурирования виртуальных локальных сетей VLAN (Virtual LAN), а также маршрутизацию ISL и протокол VTP (Virtual Trunk Protocol, протокол виртуальной магистральной сети).

В конце этого приложения приведены упражнения, лабораторные работы и проверочные вопросы, которые позволят самостоятельно проверить знания по настройке переключателей серии 1900.

## Возможности переключателей 1900

Переключатель Catalyst 1900 теперь поддерживает интерфейс CLI для настройки в устройстве операционной системы Cisco IOS (Internetworking Operating System — операционная система для объединенных сетей). До появления интерфейса CLI переключатели 1900 можно было настраивать только через меню.

Интерфейс CLI делает настройку переключателя, похожей на конфигурацию маршрутизатора. В серии Cisco Catalyst 5000 (одна из самых дорогих линеек устройств Cisco) для настройки все еще применяется команда `set`. Однако мы обсудим только команды конфигурирования переключателя Catalyst 1900.

В переключателе Cisco могут выполняться операционные системы двух типов:

**IOS** В этой системе можно настраивать переключатель через интерфейс CLI подобно маршрутизаторам Cisco. В переключателях Catalyst 1900, 2820 и 2900 используется интерфейс CLI системы IOS, хотя можно пользоваться и меню.

**На основе команды Set** Эти системы используют устаревшие конфигурационные команды CLI на основе set. К таким устройствам относятся серии Cisco 2926, 1948G, 4000, 5000 и 6000.

Познакомимся с переключателями Catalyst серии 1900. На этой серии основаны учебный курс и сертификационный экзамен CCNA. Кроме того, в командных интерфейсах CLI этих устройств можно выполнять команды IOS, хотя сами устройства гораздо дешевле устройств серии 5000. Переключатели 1900 прекрасно подходят для домашних и небольших офисов, где достаточно коммутируемых портов 10 Мбит/с и каскадных подключений 100 Мбит/с.

### Три варианта настройки

В переключателях Catalyst используется интерфейс CLI, который во многом похож на пользовательский интерфейс маршрутизатора (см. главу 4). Однако переключатель можно конфигурировать через Web с помощью визуального менеджера переключателя VSM (Visual Switch Manager). Для этого введите IP-адрес переключателя в Web-браузере. Установка IP-адреса переключателя будет рассмотрена ниже.

Переключатели 1900 имеют исходную систему меню, позволяющую настраивать устройство посредством выбора пунктов в меню. Для настройки переключателя с помощью Telnet или VSM сконфигурируйте IP-адрес.

### Подключение к консольному порту

Переключатели 1900 имеют консольный порт на задней стенке корпуса, как и маршрутизаторы серии 2500 (см. главу 4). Порт оснащён разъемом RJ-45 и предполагает подключение к терминалу шлейфовым кабелем.

**Т ВНИМАНИЕ** Переключатели 1924 имеют консольный порт для нуль-модемного кабеля.

После соединения порта с кабелем нужно запустить программу эмуляции терминала, например NupurTerm в системе Windows. Параметры настройки программы:

- 9600 Бит/с
- 8 бит данных
- Без проверки четности
- 1 стоповый бит
- Управление потоком отключено

**▼ ОСТОРОЖНО** Не подключайте к консольному порту кабель Ethernet, ISDN или работающую телефонную линию. Это может повредить электронные компоненты переключателя.

## Запуск переключателя 1900

Перед первым включением питания проверьте следующее:

- Надежно подключены все сетевые кабели.
- Терминал соединен с консольным портом.
- Правильно настроено программное обеспечение терминала.

Если выполнены все перечисленные условия, включите сетевой кабель в розетку и проверьте последовательность срабатывания индикаторных лампочек. Проверьте листинг в консоли. Рис. В.1 показывает размещение светоизлучающих диодов (LED, Light Emitting Diode) на корпусе переключателя 1900.

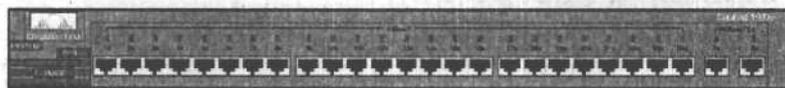


Рис. В.1. Переключатель Catalyst 1900

Зеленая системная лампочка (светодиод) свидетельствует о рабочем режиме устройства. Лампочка горит желтым цветом, когда обнаружена неисправность системы. Лампочка RPS показывает состояние резервного источника питания (redundant power supply). Лампочка горит, когда с помощью переключателя можно обнаружить этот источник питания.

Единственная кнопка переключателя 1900 называется кнопкой режимов (mode button). Нажатие этой кнопки позволяет увидеть разные лампочки состояния устройства:

**Stat (статус)** Эта лампочка показывает статус порта. Зеленый цвет говорит о соединении устройства с переключателем. Мигание этой лампочки указывает на состояние активности порта (когда лампочка включена, в порту выполняются операции). Если лампочка порта горит желтым цветом, значит выявлена ошибка линии.

**UTL (утилизация)** Эта лампочка показывает полосу пропускания переключателя. Если на 1912 нажать кнопку режима, загорятся лампочки для портов от первого до четвертого, что означает утилизацию полосы пропускания переключателем на уровне между 0.1 и 1.5 Мбит/с. Если включены лампочки от пятой до восьмой, утилизация полосы пропускания равна от 1.5 до 20 Мбит/с, а для лампочек от 9 до 12 — от 20 до 120 Мбит/с.

**FDUP** Эта лампочка показывает порты, настроенные на полнодуплексный режим.

Во время включения переключателя 1900 запускается тест POST (power-on self test — самотестирование по включению питания). В начале теста все лампочки горят зеленым цветом. Лампочки выключаются после завершения POST. Если в порту тест POST обнаружит неисправность, желтыми станут лампочки System и соответствующего порта. Если же все тестирование будет удачным, все лампочки сначала мигнут, а затем выключатся.

После выполнения POST и при подключенном консольном кабеле выводится меню. Нажав K, мы перейдем в интерфейс Command-Line Interface, а щелкнув на M сможем настроить переключатель через систему меню. Пункт I допускает в переключателе настройку конфигурации IP, однако это же можно сделать в любой момент времени с помощью меню или CLI. После установки конфигурации IP, пункт I удаляется из меню.

Показанный ниже листинг демонстрирует консольный экран после включения переключателя.

```
1 user(s) now active on Management Console.
(в консоли управления один активный пользователь)
```

```
 User Interface Menu
(меню пользовательского интерфейса)
```

```
[M] Menus
(меню)
```

```
[K] Command Line
(командная строка)
```

```
[I] IP Configuration
(конфигурация IP)
```

```
Enter Selection: K
(выберите пункт меню)
```

```
CLI session with the switch is open.
```

```
To end the CLI session, enter [Exit].
```

```
(открыт сеанс CLI с переключателем. Для завершения сеанса CLI
нажмите Enter)
```

```
>
```

## Подключение к порту Ethernet

Переключатели Catalyst 1900 имеют порты фиксированного типа в сравнении с модульными портами в переключателях серии 5000. Переключатели 1900 могут предоставить для рабочих станций **только** порты 10BaseT и порты 100BaseT или FX для каскадного соединения (uplink). Каждый переключатель имеет 12 (модель 1912) или 24 (модель 1924) 10BaseT коммутируемых портов, а также один или два каскадных порта FastEthernet. Порты 100BaseX маркируются буквами A и B. Для подключения порта к другому переключателю в виде каскадного соединения необходим перекрестный кабель. Было бы неплохо иметь кнопку переключения типа кабеля.

### Т ВНИМАНИЕ

**Для соединения переключателя с рабочими станциями, серверами, принтерами и маршрутизаторами используется прямой кабель. Между собой переключатели соединяются перекрестным кабелем.**

Во время подключения устройства к порту включается и постоянно горит лампочка состояния этого порта. Если лампочка сначала

включается, а затем выключается, то возможна неполадка в кабеле, либо проблемы с автоопределением скорости или дуплексного режима (см. ниже). Если до подачи сетевого питания с переключателем не соединено устройство, то лампочка порта включается при запуске, а затем выключается.

## Команды настройки IOS в переключателе Cisco 1900

Рассмотрим основные команды настройки переключателя Catalyst 1900.

Эти команды необходимо знать для сдачи сертификационного экзамена CCNA, а также для создания сложных конфигураций устройства.

### Установка паролей

Сначала установите пароли переключателя, поскольку следует как можно быстрее запретить к нему неавторизованный доступ. Введите как пароль пользовательского режима, так и пароль привилегированного режима (подобно маршрутизатору). Однако для этого используются иные команды, чем в маршрутизаторе.

Пароль входа (регистрации или пользовательского режима) служит для выполнения авторизации в переключателе и защищает доступ по любой линии или через консоль. Разрешенный пароль открывает доступ к просмотру и изменению конфигурации переключателя. Он похож на аналогичный пароль во всех маршрутизаторах Cisco.

**▼ ВНИМАНИЕ** | Пароль не должен быть короче четырех символов и длиннее восьми символов. Он не зависит от регистра ввода символов.

Хотя переключатель 1900 использует для доступа к IOS интерфейс CLI, команды установки паролей пользовательского и привилегированного режима отличаются от аналогичных команд в маршрутизаторе. Следует ввести команду `enable password`, которая используется и в маршрутизаторах. Однако вам надо указать уровни доступа, которые являются необязательными в маршрутизаторах Cisco, но обязательными в переключателях 1900.

### Установка паролей пользовательского и привилегированного режимов

В переключателях 1900 одна и та же команда устанавливает пароли пользовательского и привилегированного режимов. Однако для управления типом доступа используются разные уровни команды.

Для настройки пользовательского режима и разрешения пароля нажмите К на экране консоли переключателя. Для перехода в режим разрешения служит команда `enable`, а для перехода в режим глобального конфигурирования — команда `config t`. Ниже показан листинг, демонстрирующий переход в режим разрешения, а затем — в режим глобального конфигурирования.

1 user(s) now active on Management Console.

User Interface Menu

[M] Menus  
[K] Command Line  
[I] IP Configuration

Enter Selection: K

CLI session with the switch is open.

To end the CLI session, enter [Exit].

>enable

flconfig

Enter configuration commands, one per line. End with CNTL/Z

(config)#

В режиме глобального конфигурирования можно установить пароли пользовательского и привилегированного режимов. Воспользуйтесь командой `enable password`. Пример настройки паролей для обоих режимов:

```
(config)#enablepassword?
```

```
level Set exec level password
```

```
(config)#enablepasswordlevel?
```

```
<1-15> Level number
```

Для ввода пароля пользовательского режима используется уровень номер 1, а для ввода пароля разрешенного режима — уровень 15. Пароль не должен быть короче четырех символов и не длиннее восьми символов. Пример неудачного ввода пароля длиной более восьми символов:

```
(config)#enablepasswordlevel1toddlammle
```

```
Error: Invalid password length.
```

```
Password must be between 4 and 8 characters
```

Пример ввода пароля пользовательского режима и пароля разрешенного режима в переключателе 1900:

```
(config)#enablepasswordlevel1todd
```

```
(config)#enablepasswordlevel15todd1
```

```
(config)#exit
```

```
#exit
```

```
CLI session with the switch is now closed.
```

```
(сеанс CLI с переключателем закрыт)
```

```
Press any key to continue.
```

```
(для продолжения нажмите любую клавишу)
```

Теперь можно нажать `Enter` и проверить действие паролей. После нажатия `K` выводится приглашение для ввода пароля пользовательского режима, а после ввода `enable` можно ввести пароль разрешенного режима.

После выхода из режима настройки и перехода в привилегированный режим получится показанный ниже консольный экран (после нажатия К переключатель выводит приглашение для пароля пользовательского режима).

```
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc. 1993-1998
All rights reserved.
Enterprise Edition Software
Ethernet Address: 00-30-80-CC-7D-00
PCANumber: 73-3122-04
PCA Serial Number: FAB033725XG
Model Number: WS-C1912-A
System Serial Number: FAB0339T01M
Power Supply S/N: PHI031801CF
PCB Serial Number: FAB033725XG,73-3122-04
```

```

1 user(s) now active on Management Console.
```

```
 User Interface Menu
```

```
 [M] Menus
```

```
 [K] Command Line
```

```
Enter Selection: K
```

```
Enter password: ****
```

```
 CLI session with the switch is open.
```

```
 To end the CLI session, enter [Exit].
```

```
>en
```

```
Enter password: ****
```

```
#
```

После входа в пользовательский режим введите en (краткая форма команды enable) и получится приглашение для ввода разрешенного пароля.

**▼ ОСТОРОЖНО** | Следует хорошо запомнить установленные пароли, поскольку в переключателях 1900 **невозможно** восстановить потерянные пароли. Для восстановления пароля обращайтесь в компанию Cisco.

Были установлены пароли пользовательского режима и разрешенного режима. Однако в переключателе 1900 есть еще пароль разрешенного секрета.

### Установка пароля разрешенного секрета

Пароль разрешенного секрета имеет больший уровень защиты, поэтому при установке заменяет разрешенный пароль. Пароль разрешенного секрета устанавливается подобно аналогичному паролю в маршрутизаторе.

Если установлен пароль разрешенного секрета, то можно не вводить пароль разрешенного режима.

```
(config)#enablesecret todd2
```

В переключателе 1900 команды `enable password` и `enable secret` действуют одинаково, но это недопустимо в маршрутизаторе. Для просмотра текущей конфигурации переключателя служит команда `show running-config` (краткая форма `show run`).

```
#sh run
Building configuration...
Current configuration:

enable secret 5 1FMFQ$wFVYVLYn2aXscfB3J95.w.
enable password level 1 "TODD"
enable password level 15 "TODD1"
```

Пароли разрешенного режима по умолчанию не шифруются, хотя шифруется пароль разрешенного секрета. Точно так же выполняется шифрование в маршрутизаторах.

Заметим, что даже при вводе пароля в нижнем регистре клавиатуры команда `running-config` показывает его в верхнем регистре. Безразличен как режим ввода пароля, так и способ его показа, поскольку пароли не зависят от регистра.

## Установка имени хоста

Имя хоста в переключателе (а также в маршрутизаторе) действует только локально. Т.е. это имя не используется в сети или службе разрешения имен. Однако имя хоста идентифицирует переключатель в удаленных соединениях. Рекомендуется присваивать имена хостов согласно местоположению устройств.

В переключателе 1900 для установки имени хоста используется команда `hostname` (как и в маршрутизаторах). Имя должно состоять из одного слова. Ниже показан листинг консольного экрана. Нажав `K`, мы перешли в пользовательский режим, ввели пароль командой `enable` и установили пароль разрешенного секрета. В режиме глобального конфигурирования команда `hostname` использовалась для ввода имени хоста.

```
1 user(s) now active on Management Console.
```

```
User Interface Menu
```

```
[M] Menus
```

```
[K] Command Line
```

```
[I] IP Configuration
```

```
Enter Selection: K
```

```
Enter password: ****
```

```
CLI session with the switch is open.
```

```
To end the CLI session, enter [Exit].
```

```
>en
Enter password: ****
#config t
Enter configuration commands, one per line. End with CNTL/Z
(config)#hostname Todd 1900EN
Todd1900EN(config)#
```

После нажатия Enter на экране появилось имя хоста. Запомните, что в режиме глобального конфигурирования (куда мы вошли с помощью команды `config t`) изменяется команда `running-config`. Любые изменения конфигурации будут применяться немедленно.

## Установка информации IP

Для работы переключателя не обязательно вводить информацию о протоколе IP. Достаточно подключить к устройству кабели и включить питание (как это делается в концентраторах). Для установки в переключателе информации о IP-адресе существуют две причины: управление по Telnet или ином программном обеспечении сетевого управления устройствами, либо необходимость настройки переключателя на разные виртуальные сети VLAN или другие сетевые функции (сети VLAN рассмотрены в главе 6).

Переключатель Catalyst 1900 имеет готовые значения параметров по умолчанию, установленные во время производства устройства:

- IP-адрес и шлюз по умолчанию: 0.0.0.0
- CDP: Допускается
- Режим коммутации: FragmentFree
- Порт 100BaseT: автосогласование дуплексного режима
- Порты 10BaseT: полудуплексный режим
- Покрывающее дерево (Spanning Tree): Допускается
- Пароль консоли: Не установлен

По умолчанию не установлен IP-адрес или шлюз по умолчанию. Для переключателей уровня 2 необходимо обязательно ввести эти сведения (как и для любого хоста). Команда `show ip` (или `sh ip`) покажет конфигурацию IP по умолчанию, существующую в переключателе.

```
Todd1900EN#sh ip
IP Address: 0.0.0.0
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0
Management VLAN: 1
Domain name:
Nameserver 1: 0.0.0.0
Name server 2: 0.0.0.0
HTTP server : Enabled
```

```
HTTPport :80
```

```
RIP : Enabled
```

В листинге отсутствуют сведения о IP-адресе, шлюзе по умолчанию и других параметрах IP. Для установки конфигурации IP в переключателях 1900 служит команда `ip address`. Шлюз по умолчанию указывается командой `ip default-gateway`.

Пример настройки IP-адреса и шлюза по умолчанию в переключателе 1900:

```
Todd1900EN#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z
```

```
Todd1900EN(config)#ip address 172.16.10.16 255.255.255.0
```

```
Todd1900EN(config)#ip default-gateway 172.16.10.1
```

```
Todd1900EN(config)#
```

Настроив информацию IP, проверим изменение параметров командой `show ip`.

```
Todd1900EN#sh ip
```

```
IP Address: 172.16.10.16
```

```
Subnet Mask: 255.255.255.0
```

```
Default Gateway: 172.16.10.1
```

```
Management VLAN: 1
```

```
Domain name:
```

```
Name server 1: 0.0.0.0
```

```
Nameserver2: 0.0.0.0
```

```
HTTPserver : Enabled
```

```
HTTP port : 80
```

```
RIP : Enabled
```

```
Todd1900EN#
```

Для изменения IP-адреса или шлюза по умолчанию в переключателе следует ввести новый адрес или удалить информацию IP командами `no ip address` и `no ip default-gateway`.

## Настройка интерфейсов переключателя

Важно понять правила доступа к портам коммутации. Переключатель 1900 использует для настройки портов команду `type slot/port`. Например, Ethernet 0/3 — это порт ЮBaseT номер 3. Другой пример — FastEthernet 0/26. Это первый из портов FastEthernet переключателя серии 1900.

Команда `type slot/port` в переключателе 1900 может использоваться совместно с командой `interface` или `show`. Команда `interface` служит для настройки конфигурации на уровне интерфейса. В переключателе 1900 только один слот: zero (0).

Экран справки о конфигурации интерфейсов не очень полезен. Этот экран показывает только порты 1 — 25 для Ethernet и порты 26/27 для

FastEthernet. В модели 1912 мы имеет только порты 1 — 12. Однако есть еще порт 25 на задней стенке корпуса переключателя. Это порт адаптера AUI (Attachment Unit Interface — интерфейс модуля подключения) для соединения переключателей друг с другом, либо соединения переключателя 1900 с сетью Ethernet на коаксиальном кабеле.

## Настройка интерфейсов 10BaseT

Для настройки интерфейсов переключателя 1900 перейдите в режим глобального конфигурирования и примените команду `interface`. Ниже показан экран справки с описанием методов настройки в команде `type slot/port` В режиме глобального конфигурирования у команды `interface` доступны два варианта (типа интерфейса): Ethernet или FastEthernet. Сначала рассмотрим настройку интерфейса на тип Ethernet.

```
Todd1900EN#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z
```

```
Todd1900EN(config)#int ethernet ?
```

```
<0-0> IEEE 802.3
```

В листинге запрашивался слот. Переключатель 1900 не является модульным устройством, поэтому имеет только один слот. Следующий листинг показывает использование символа слеш (/) для разделения конфигурации слота/порта.

```
Todd1900EN(config)#int ethernet 0?
```

```
/
```

```
Todd1900EN(config)#int ethernet 0/?
```

```
<1-25> IEEE 802.3
```

После конфигурационной команды `0/` показано количество настраиваемых портов. Однако в модели 1912 мы имеем только порты с номерами 1 — 12 и порт 25 на задней стенке устройства, а порты 26 и 27 служат для каскадного соединения со скоростью 100 Мбит/с. В листинге не представлены порты FastEthernet, поскольку для типа интерфейса выбрано значение Ethernet. Каскадные порты имеют тип FastEthernet.

Пример полной команды:

```
Todd1900EN(config)#int ethernet 0/1
```

Во время настройки интерфейсов приглашение изменится на `(config-if)`. Это интерфейсное приглашение, позволяющее получить справку о доступных командах.

```
Todd1900EN(config-if)#?
```

```
Interface configuration commands:
```

```
(команды конфигурирования интерфейса)
```

```
cdp
```

```
Cdp interface subcommands
(подкоманда интерфейса CDP)
```

```
description
```

```
Interface specific description
(описание интерфейса)
```

duplex	Configure duplex operation (настройка дуплексного режима)
exit	Exit from interface configuration mode (выход из режима настройки интерфейса)
help	Description of the interactive help system (интерактивная справочная система)
no	Negate a command or set its defaults (отмена команды или установка по умолчанию)
port	Perform switch port configuration (настройка коммутируемого порта)
shutdown	Shutdown the selected interface (выключение указанного порта)
spantree	Spanning tree subsystem (подсистема покрывающего дерева)
vlan-membership	VLAN membership configuration (настройка членства в виртуальной локальной сети)

Для переключения между настройкой интерфейсов и режимом глобального конфигурирования служит команда `int e 0/#`, которую можно вводить в любое время.

### Настройка интерфейса FastEthernet

Для настройки двух портов FastEthernet тоже используется команда `type slot/port`, но с типом FastEthernet вместо Ethernet, например `interface fastEthernet 0/#`.

Ниже показан пример настройки в переключателе 1900 порта Fast Ethernet. Использована команда `interface fastEthernet`, но слот номер 0. Доступны только порты 26 и 27.

```
Todd1900EN(config)#int fastEthernet ?
<0-0> FastEthernet IEEE 802.3
Todd1900EN(config)#int fastEthernet 0/?
<26-27> FastEthernet IEEE 802.3
Todd1900EN(config)#int fastEthernet 0/26
Todd1900EN(config-if)#int fast 0/27
Todd1900EN(config-if)# [control+Z]
```

После изменения параметров интерфейса можно вывести характеристики других интерфейсов командой `show interface`.

В показанном ниже листинге представлены команды вывода сведений об интерфейсах IOBaseT и FastEthernet.

```
Todd1900EN#sh int e0/1
Ethernet 0/1 is Suspended-no-linkbeat
Hardware is Built-in 10Base-T
Address is 0030.80CC.7D01
MTU 1500 bytes, BW 10000Kbits
802.1dSTPState: Forwarding Forward Transitions: 1
```

```
[листинг сокращен]
Todd1900EN#sh int f0/26
FastEthernet 0/26 is Suspended-no-linkbeat
Hardware is Built-in 100Base-TX
Address is 0030.80CC.7D1A
MTU 1500 bytes, BW 100000 Kbits
802.1dSTP State: Blocking Forward Transitions: 0
[листинг сокращен]
```

## Настройка описания интерфейса

Администратор может установить имя для каждого интерфейса в переключателе 1900. Как и имя хоста, описание интерфейса действует только локально.

В переключателях серии 1900 описание вводится командой `description`. В самом описании нельзя использовать пробелы, но допустимы символы подчеркивания.

### Установка описания

Для установки описания необходимо перейти в режим конфигурации интерфейса, а затем ввести описание каждого интерфейса командой `description`. Описание может состоять из нескольких слов. Однако запрещены пробелы, которые рекомендуется заменить символами подчеркивания:

```
Todd1900EN#config t
Enter configuration commands, one per line. End with CNTL/Z
Todd1900EN(config)#int e0/1
Todd1900EN(config-if)#description Finance_VLAN
Todd1900EN(config-if)#int f0/26
Todd1900EN(config-if)#description trunk_to_Building_4
Todd1900EN(config-if)#
```

В примере установлены описания портов 10 Мбит/с и 100 Мбит/с.

### Просмотр описаний

После установки описаний каждого интерфейса, их можно вывести командой `show interface` или `show running-config`.

```
Todd1900EN#sh int e0/1
Ethernet 0/1 is Suspended-no-linkbeat
Hardware is Built-in 10Base-T
Address is 0030.80CC.7D01
MTU 1500 bytes, BW 10000 Kbits
802.1dSTP State: Forwarding Forward Transitions: 1
Port monitoring: Disabled
Unknown unicast flooding: Enabled
```

Unregistered multicast flooding: Enabled

**Description:** Finance\_VLAN

Duplex setting: Half duplex

Back pressure: Disabled

Todd1900EN#sh run

Building configuration...

Current configuration:

hostname "Todd1900EN"

!

ip address 172.16.10.16 255.255.255.0

ip default-gateway 172.16.10.1

!

interface Ethernet 0/1

**description "Finance\_VLAN"**

!

[листинг сокращен]

В представленном листинге команды sh int e0/1 и show run показывают одинаковое описание интерфейса.

## Настройка дуплексного режима порта

В переключателях 1900 доступны 12 или 24 порта ЮBaseT вместе с одним или двумя портами FastEthernet. Команда duplex в переключателях 1900 разрешается только для портов с фиксированной скоростью, причем команда duplex вводится в режиме конфигурации интерфейса.

Листинг показывает параметры настройки порта FastEthernet:

Todd1900EN(config)#int f0/26

Todd1900EN(config-if)#duplex ?

    auto            Enable auto duplex configuration  
(разрешение автоопределения дуплексного режима)

    full            Force full duplex operation  
(работа в полнодуплексном режиме)

    full-flow-control Force full duplex with flow control  
(работа в полнодуплексном режиме с управлением потоком)

    half            Force half duplex operation  
(работа в полудуплексном режиме)

Todd1900EN(config-if)#duplex full

В таблице В.1 перечислены описания доступных параметров настройки дуплексного режима для переключателей 1900. Порты FastEthernet по умолчанию установлены в режим *auto duplex*, т.е. предпринимается попытка автоматического определения дуплексного режима на другой стороне соединения. Автоопределение не всегда бывает успешным, поэтому рекомендуется в портах FastEthernet устанавливать полудуплексный режим.

**Таблица В.1.****Параметры дуплексного режима**

Параметр	Описание
Auto	Режим автоматического согласования. Установлен по умолчанию для всех портов 100BaseTX.
Full	Полнодуплексный режим для портов 10 и 100 Мбит/с.
Full-flow-control	Только для портов 100BaseTX. Использование управления потоком для устранения переполнения буфера.
Half	Установлен по умолчанию для портов 10BaseT. Предписывает работу только в полудуплексном режиме.

После установки параметров дуплексного режима, эти значения выводятся командой `show interface`.

```
Todd1900EN#sh int f0/26
FastEthernet0/26 is Suspended-no-linkbeat
Hardware is Built-in 100Base-TX
Address is 0030.80CC.7D1A
MTU 1500 bytes, BW 100000 Kbits
802.1dSTP State: Blocking Forward Transitions: 0
Port monitoring: Disabled
Unknown unicast flooding: Enabled
Unregistered multicast flooding: Enabled
Description: trunk_to_Building_4
Duplex setting: Full duplex
Back pressure: Disabled
```

В данном случае установлен полнодуплексный режим.

## Проверка соединений по протоколу IP

Необходимо проверить конфигурацию IP в переключателе. Для этого к устройству серии 1900 можно обратиться по Ping или Telnet. Однако нельзя использовать на самом переключателе 1900 команды `telnet` и `traceroute`.

Рассмотрим пример проверки одного из хостов сети по Ping из интерфейса CLI переключателя. Листинг показывает успешную проверку, о чем свидетельствует восклицательный знак (!). Если будет выведена точка (.), значит произошел тайм-аут.

```
Todd1900EN#ping 172.16.10.10
Sending 5, 100-byte ICMP Echos to 172.16.10.10, time out
is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
```

```
O/2/10/ ms
Todd1900EN#telnet 172.16.10.10
л
```

```
% Invalid input detected at '^' marker.
```

В показанном листинге проверка по Telnet оказалась неудачной, поскольку команда telnet не поддерживается в переключателе 1900. Однако можно в любой момент обратиться по Telnet к самому переключателю, если конечно правильно настроено соединение по протоколу IP.

## Стирание конфигурации переключателя

Конфигурация переключателя хранится в NVRAM, как и в любом маршрутизаторе. Нельзя просмотреть файл `startup-config` или содержимое NVRAM. Доступна только конфигурация `running-config`. Когда в переключателе изменяется конфигурация `running-config`, устройство автоматически копирует конфигурацию переключателя в NVRAM. Это коренным образом отличается от поведения маршрутизаторов, где копирование выполняется командой `copy running-config startup-config`. В переключателях 1900 копирование вручную запрещено.

Для удаления конфигурации в памяти NVRAM переключателя 1900 (когда необходимо заново начать процесс настройки) служит команда `delete nvram`.

В показанном ниже листинге видно, что есть два варианта стирания: `nvram` и `vtp`. В данном случае стирание содержимого NVRAM сопровождается восстановлением заводских значений по умолчанию.

```
Todd1900EN#delete ?
nvram NVRAM configuration
vtp Reset VTP configuration to defaults
Todd1900EN#delete nvram
```

```
This command resets the switch with factory defaults. All system parameters will
revert to their default factory settings. All static and dynamic addresses will be
removed.
```

```
Reset system with factory defaults, [Y]es or [N]o?Yes
```

Обратите внимание на сообщение после ввода команды `delete nvram`. Если выбрать `yes`, то будут восстановлены заводские параметры устройства.

## Обслуживание таблиц МЛС-адресов

Мосты и переключатели фильтруют сетевой трафик. Они используют MAC-адреса (аппаратные адреса), прошитые в сетевых адаптерах (NIC) хостов, чтобы решить дальнейшую судьбу пересылаемых данных. Переключатели создают таблицы MAC, содержащие динамические, постоянные и статические адреса. Такая фильтрующая таблица формируется на основе полученных от хостов кадров, по которым переключатель изучает MAC-адреса источников и соответствующие им сегменты и порты.

Переключатель вставляет в фильтрующую таблицу MAC новые MAC-адреса, по которым в сеть отправляется информация. При добавлении или удалении хостов в сети переключатель динамически обновляет фильтрующую таблицу MAC-адресов. Если устройство удалено или переключатель долго не может получить к нему доступ, то из таблицы удаляется соответствующая устройству запись.

Увидеть фильтрующую таблицу переключателя позволяет команда `show mac-address-table`. Ниже показан листинг, полученный такой командой.

```
ToddI900EN#sh mac-address-table
```

```
Number of permanent addresses : 0
```

```
Number of restricted static addresses : 0
```

```
Number of dynamic addresses : 4
```

Address	Dest Interface	Type	Source
Interface List			
00A0.246E.0FA8	Ethernet 0/2	Dynamic	All
0000.8147.4E11	Ethernet 0/5	Dynamic	All
0000.8610.C16F	Ethernet 0/1	Dynamic	All
00A0.2448.60A5	Ethernet 0/4	Dynamic	All

В таблице собраны адреса четырех хостов, соединенных с переключателем 1900. Все записи в таблице *динамические*, т.е. переключатель анализирует адрес источника, поступившего в интерфейс кадра, и сохраняет его в фильтрующей таблице. В показанном примере хосты подключены к интерфейсам 1, 2, 4 и 5.

Переключатель Catalyst 1900 способен сохранить в фильтрующей таблице до 1024 MAC-адресов. Если таблица переполняется, переключатель отбрасывает все новые записи до тех пор, пока не освободится одна из записей таблицы.

Можно очистить фильтрующую таблицу MAC-адресов командой `clear mac-address-table`, причем очищаются динамические, постоянные и ограниченные статические адреса.

Ниже показан листинг из переключателя с доступными параметрами команды `clear mac-address-table`.

```
#clear mac-address-table ?
```

```
dynamic Clear 802.1d dynamic address
 (очистка динамических адресов 802.1d)
```

```
permanent Clear 802.1d permanent addresses
 (очистка постоянных адресов 802.1d)
```

```
restricted Clear 802.1d restricted static address
 (очистка ограниченных статических адресов 802.1d)
```

```
<cr>
```

## Установка постоянных и статических МЛС-адресов

Администратор может специально присваивать постоянный адрес (permanent address) порту переключателя. Срок действия этого адреса неограничен. Постоянные адреса присваиваются для защиты порта, т.е. порт переключателя не действует, пока в нем не сконфигурирован определенный аппаратный адрес. Администратор может создать статическую запись в переключателе, которая реально специфицирует путь к аппаратному адресу источника. Им нужно пользоваться осторожно (лучше просто снять питание с переключателя, если есть подозрения в неправильной конфигурации).

### Установка записей о постоянных MAC-адресах

Настройка постоянного MAC-адреса для порта переключателя выполняется командой глобального конфигурирования mac-address-table permanent [MAC\_адрес] [интерфейс].

В показанном ниже листинге выведены параметры этой команды:

**Срок действия (Aging-time)** Используется для изменения срока действия MAC-адреса (времени нахождения в фильтрующей таблице перед очисткой соответствующей записи).

**Постоянный (Permanent)** Определяет постоянный адрес для интерфейса. Если пользователь заменит на хосте сетевой адаптер, то хост не сможет работать до изменения записи о постоянном адресе в переключателе.

**Ограниченно (Restricted)** Используется в команде static для указания пути к аппаратному адресу источника. Вводится ограничение на место отправки кадров из хоста.

Для настройки в интерфейсе постоянного аппаратного адреса служит команда mac-address-table permanent в режиме глобального конфигурирования:

```
Todd1900EN#config t
Enter configuration commands, one per line. End with CNTL/Z
Todd1900EN(config)#mac-address-table ?
 aging-time Aging time of dynamic addresses
 permanent Configure a permanent address
 restricted Configure a restricted static address
```

После ввода команды mac-address-table permanent добавь аппаратный адрес источника и связанный с ним интерфейс. Это разрешит интерфейсу прием только кадров из указанного аппаратного адреса источника.

```
Todd1900EN(config)#mac-address-table permanent ?
 H.H.H 48 bit hardware address
Todd1900EN(config)#mac-address-table permanent
OOA0.2448.60A5 eO/4
```

После настройки записи в таблице следует проверить ее. Используйте команду `show mac-address-table`.

```
Todd1900EN#shmac-address-table
```

```
Number of permanent addresses : 1
```

```
Number of restricted static addresses : 0
```

```
Number of dynamic addresses : 3
```

Address	Dest Interface	Type	Source
Interface List			
00A0.2448.60A5	Ethernet0/4	Permanent	All
00A0.246E.OFA8	Ethernet 0/2	Dynamic	All
0000.8147.4E11	Ethernet 0/5	Dynamic	All
0000.8610.C16F	Ethernet 0/1	Dynamic	All

```
Todd1900EN#
```

В показанном листинге из переключателя интерфейсу 4 присвоена постоянная запись с аппаратным адресом `00A0.2448.60A5`. Ни одно другое устройство не сможет подключиться к интерфейсу 4, пока не будет изменена запись о постоянном адресе в фильтрующей таблице MAC-адресов.

### Установка записи о статическом МЛС-адресе

Можно еще больше усилить защиту порта. Для этого командой `restricted static` следует указать интерфейс источника, который может пересылать кадры.

Команда `mac-address-table restricted static` имеет два параметра: для установки аппаратного адреса интерфейса назначения и для установки единственного интерфейса источника, который может взаимодействовать с интерфейсом назначения.

В режиме глобального конфигурирования ввод команды `mac-address-table restricted static` сопровождается указанием аппаратного адреса устройства назначения:

```
Todd1900EN(config)#mac-address-table restricted static ?
```

```
 H.H.H 48 bit hardware address
```

```
Todd1900EN(config)#mac-address-table restricted static
```

```
00A0.246E.OFA8 ?
```

```
Ethernet IEEE 802.3
```

```
FastEthernet FastEthernet IEEE 802.3
```

Добавив аппаратный адрес целевого устройства, следует указать адрес интерфейса, с которым будет связан этот аппаратный адрес назначения.

```
Todd1900EN(config)#mac-address-table restricted static
```

```
00A0.246E.OFA8 e0/2 ?
```

```
Ethernet IEEE 802.3
```

```
FastEthernet FastEthernet IEEE 802.3
<cr>
```

Введем сведения об интерфейсе источника, который может взаимодействовать с указанным ранее адресом назначения.

```
Todd1900EN(config)#table restricted static
OOA0.246E.OFA8 eO/2 eO/5
```

Завершив ввод команды, мы получим в фильтрующей таблице MAC-адресов три разных типа записей. Их увидеть позволяет команда `show mac-address-table` (краткая форма: `sh mac`).

```
Todd1900EN#sh mac
Number of permanent addresses : 1
Number of restricted static addresses : 1
Number of dynamic addresses : 2
```

Address	Dest Interface	Type	Source Interface List
OOA0.2448.60A5	Ethernet 0/4	Permanent	All
OOA0.246E.OFA8	Ethernet 0/2	Static	EtO/5
0000.8147.4E11	Ethernet 0/5	Dynamic	All
0000.8610.C16F	Ethernet 0/1	Dynamic	All

```
Todd1900EN#
```

В листинге интерфейс 0/5 ограничен только передачей кадров в интерфейс 0/2 при аппаратном адресе назначения OOA0.246E.OFA8.

Очистить записи можно командой `mac-address-table [dynamic/permanent/restricted] [интерфейс_назначения] [интерфейс_источника]`.

## Настройка безопасности порта

*Безопасность порта* — это способ запрещения пользователям подключения концентраторов к разъемам устройства в своих рабочих помещениях, а также самостоятельного добавления хостов. По умолчанию в одном интерфейсе переключателя допускается до 132 аппаратных адресов. Но изменить это значение позволяет команда `port secure max-mac-count`.

В показанном ниже листинге из переключателя команда `port secure max-mac-count` установила для интерфейса 0/2 разрешение только на одну запись.

```
Todd1900EN#config t
Enter configuration commands, one per line. End with CNTL/Z
Todd1900EN(config)#inteO/2
Todd1900EN(config-if)#port secure ?
max-mac-count Maximum number of addresses allowed on the port
<cr>
Todd1900EN(config-if)#port secure max-mac-count ?
```

<1-132> Maximum mac address count for this secure port

```
Todd1900EN(config-if)#port secure max-mac-count 1
```

Созданные защищенные порты могут пользоваться статическими или "хитро изученными" вручную (sticky-learned) аппаратными адресами. Если защищенному порту аппаратный адрес не присвоен статически, то порт исследует адреса источников из поступивших кадров и автоматически присваивает их в виде постоянных адресов. Термин *Sticky-learn* введен компанией Cisco для процедуры динамического поиска портом аппаратных адресов источников и создания на их основе постоянных записей в фильтрующей таблице MAC-адресов.

## Команда Show Version

Команда `show version` выводит основную информацию о переключателе: время его работы, версию IOS и базовый MAC-адрес.

Этот MAC-адрес очень важен, поскольку при утере пароля в переключателях серии 1900 не обеспечивается его восстановление. Вам придется отправить MAC-адрес в компанию Cisco и получить пароль, который позволит войти в систему переключателя.

Листинг из переключателя показывает аппаратную конфигурацию, версию программного обеспечения, а также имена и источники конфигурационных и загрузочных файлов:

```
Todd1900EN#sh ver
Cisco Catalyst 1900/2820 Enterprise Edition Software
Version V9.00.00
Copyright (c) Cisco Systems, Inc. 1993-1999
Todd1900EN uptime is Oday(s) 03hour(s) 37minute(s)
15second(s)
Cisco Catalyst 1900 (486sxl) processor with 2048K/1024K
bytes of memory
Hardware board revision is 5
Upgrade Status: No upgrade currently in progress.
Config File Status: No configuration upload/download is in
progress
15 Fixed Ethernet/IEEE 802.3 interface(s)
Base Ethernet Address: 00-B0-64-75-6A-C0
Todd1900EN#
```

В листинге представлены 15 фиксированных интерфейсов Ethernet 802.3, что указывает на модель 1912 переключателя. Модель 1912 имеет 12 портов 10BaseT, 1 порт AUI и 2 порта FastEthernet, т.е. всего 15 портов. Модель 1924 включает 24 порта 10BaseT, 1 порт AUI и 2 порта FastEthernet, т.е. всего 27 портов.

## Изменение типа коммутации локальной сети

Увидеть тип локальной сети в переключателе 1900 можно с помощью команды `show port system`. Изменение типа коммутации выполняется командой `switching-mode` в режиме глобального конфигурирования. Допустимые типы коммутации: `store-and-forward` и `FragmentFree`.

Команда `show port system` показывает, что типом коммутации локальной сети по умолчанию является `FragmentFree`. Команда `switching-mode` в режиме глобального конфигурирования позволит перейти на тип коммутации `store-and-forward` (сохранить и передать).

```
1900EN#sh port system
```

```
Switching mode: FragmentFree
```

```
Use of store and forward for multicast: Disabled
```

```
Network port: None
```

```
Half duplex backpressure (10 Mbps ports): Disabled
```

```
Enhanced Congestion Control (10 Mbps ports): Disabled
```

```
Default port LED display mode: Port Status
```

```
1900EN(config)#switching-mode?
```

```
fragment-free Fragment Free mode
```

```
store-and-forward Store-and-Forward mode
```

Изменение типа коммутации должно быть выполнено во всех портах переключателя.

## Настройка сетей VLAN

Не сложно провести настройку виртуальной локальной сети (VLAN). Сначала следует выявить состав пользователей в каждой сети VLAN (на это может уйти много времени). Выбрав количество сетей VLAN и состав их членов, можно переходить к настройке сетей VLAN. Переключатель 1900 способен поддерживать до 64 сетей VLAN, причем для каждой из них можно сконфигурировать собственный экземпляр алгоритма покрывающего дерева (`spanning-tree`).

Для настройки VLAN в переключателе серии 1900 выберите пункт К в меню начального пользовательского интерфейса, чтобы перейти в режим настройки IOS. Хотя можно создавать сети VLAN с помощью системы меню переключателя 1900, рекомендуется использовать интерфейс CLI. Это интерфейс операционной системы Cisco IOS. Кроме того, на экзамене CCNA достаточно знать о настройке переключателей 1900 только через интерфейс CLI.

Ниже показан консольный экран переключателя 1900. Нажмите К для перехода в режим CLI и введите `enable` и `config t` для перехода в режим глобального конфигурирования.

```
1 user(s) now active on Management Console.
```

```
User Interface Menu
```

```
[M] Menus
[K] Command Line
[I] IP Configuration
```

Enter Selection: K

CLI session with the switch is open.  
To end the CLI session, enter [Exit].

Для настройки VLAN в переключателе с системой IOS служит команда `vlan [номер_сети] name [имя_сети]`. Рассмотрим пример для настройки трех разных сетей VLAN для трех отделов компании.

```
>en
#config t
Enter configuration commands, one per line. End with CNTL/Z
(config)#hostname 1900EN
1900EN(config)#vlan2 name sales
1900EN(config)#vlan3 name marketing
1900EN(config)#vlan4 name mis
1900EN(config)#exit
```

После создания сетей VLAN, их конфигурация выводится командой `show vlan`. Однако по умолчанию все порты переключателя присваиваются VLAN 1. Для изменения связанной с портом сети VLAN нужно перейти в режим настройки соответствующего интерфейса и указать, частью какой виртуальной сети станет этот интерфейс.

**ВНИМАНИЕ** | Помните, что созданные сети VLAN не используются до отображения на коммутируемый порт. Предварительно все порты принадлежат сети VLAN 1.

После создания сетей VLAN следует проверить их конфигурацию командой `show vlan` (краткая форма: `sh vlan`).

```
1900EN#sh vlan
```

VLAN Name	Status	Ports
1 default	Enabled	1-12, AUI, A, B
2 sales	Enabled	
3 marketing	Enabled	
4 mis	Enabled	
1002 fddi-default	Suspended	
1003 token-ring-defau	Suspended	
1004 fddinet-default	Suspended	
1005 trnet-default	Suspended	

[листинг сокращен]

Мы видим три сети VLAN, а также присвоенные им порты переключателя. Любой порт может быть частью только одной сети VLAN. Однако, ко есть метод, при котором одновременно нескольким сетям VLAN присваивается порт (см. ниже).

## Присваивание коммутируемых портов сети VLAN

Настройка порта на определенную сеть VLAN выполняется командой `vlan-membership`. Включать порты в сеть VLAN разрешается только по одному порту за один раз. В переключателе 1900 не существует команды одновременного присваивания VLAN нескольких портов.

Для порта членство в виртуальной локальной сети может быть статическим или динамическим. Экзамен CCNA и наша книга рассматривают только статическое членство в сети VLAN.

Рассмотрим пример присваивания интерфейса 2 сети VLAN 2, интерфейса 4 — VLAN 3 и интерфейса 5 — VLAN 4.

```
1900EN#config t
Enter configuration commands, one per line. End with CNTL/Z
1900EN(config)#inteO/2
1900EN(config-if)#vlan-membership ?
 dynamic Set VLAN membership type as dynamic
 static Set VLAN membership type as static
1900EN(config-if)#vlan-membershipstatic ?
 <1-1005> ISLVLAN index
1900EN(config-if)#vlan-membershipstatic 2
1900EN(config-if)#inteO/4
1900EN(config-if)#vlan-membershipstatic 3
1900EN(config-if)#inteO/5
1900EN(config-if)#vlan-membershipstatic 4
1900EN(config-if)#exit
1900EN(config)#exit
```

Теперь можно снова ввести `show vlan`, чтобы проверить присваивание портов каждой сети VLAN.

```
1900EN#sh vlan
```

VLAN Name	Status	Ports
1 default	Enabled	1,3,6-12,AUI,A,B
2 sales	Enabled	2
3 marketing	Enabled	4
4 mis	Enabled	5
1002 fddi-default	Suspended	
1003 token-ring-defau	Suspended	
1004 fddinet-default	Suspended	

```
1005 trnet-default Suspended
```

```
[листинг сокращен]
```

Для получения сведений только об одной сети VLAN служит команда **show vlan** [номер].

```
1900EN#sh vlan 2
```

VLAN	Name	Status	Ports
2	sales	Enabled	2

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	Transl	Trans2
2	Ethernet	100002	1500	0	1	1	Unkn	O	O

```
1900EN#
```

Еще одна команда для знакомства с присвоенными VLAN портами — это **show vlan-membership**. В ее листинге показаны все порты переключателя, их принадлежность сетям VLAN и тип членства (статический или динамический).

```
1900A#sh vlan-membership
```

Port	VLAN	Membership
1	1	Static
2	2	Static
3	1	Static
4	3	Static
5	4	Static
6	1	Static
7	1	Static
8	1	Static
9	1	Static
10	1	Static
11	.1	Static
12	1	Static
AUI	1	Static
A	1	Static
B	1	Static

```
1900A#
```

## Настройка транковых портов

В переключателях 1900 поддерживается только метод инкапсуляции DISL (Dynamic Inter-Switch Link — динамические межпереключательные

связи). Для настройки магистрального канала в порту FastEthernet служит команда `trunk` [параметр].

Ниже показан листинг конфигурации канала связи в интерфейсе 26 переключателя.

```
1900EN#config t
Enter configuration commands, one per line. End with CNTL/Z
1900EN(config)#int f0/26
1900EN(config-if)#trunk?
 auto Set DISL state to AUTO
 desirable Set DISL state to DESIRABLE
 nonegotiate Set DISL state to NONEGOTIATE
 off Set DISL state to OFF
 on Set DISL state to ON
1900EN(config-if)#trunkon
```

При установке магистрального интерфейса доступны следующие параметры.

**Auto** (автоопределение) Интерфейс становится магистральным только при подключении к устройству, которое включено в магистральном режиме или собирается там работать.

**Desirable** (предлагаемый) Согласование магистрального режима. Для устройств, работающих в этом режиме, предполагается его установка или установка режима автоопределения.

**Nonegotiate** (без согласования) Интерфейс становится постоянным магистральным портом ISL и не согласовывает этот режим с подключаемыми к порту устройствами.

**Off** (выключено) В интерфейсе запрещен магистральный режим и попытки его установки со стороны подключаемых устройств.

**On** (включено) Интерфейс становится постоянным магистральным портом ISL и может согласовывать с подключаемыми устройствами переход в магистральный режим.

Какие порты сети VLAN становятся магистральными? По умолчанию — все. По умолчанию не допускается сконфигурировать порты определенной сети VLAN (ниже мы покажем процедуру отмены магистрального режима в портах сети VLAN).

## Очистка магистральных связей в сети VLAN

Итак, все VLAN настраиваются на магистральные линии, если иное не указано администратором. Для очистки переноса информации VLAN по магистральным связям существуют две причины: отмена широковещательных рассылок определенной сети VLAN по магистральным связям и запрет пересылки информации об изменениях топологии по связям, не включенным в состав сетей VLAN.

В переключателе 1900 для удаления в порту VLAN магистрального режима используется интерфейсная команда `no trunk-vlan`. Пример очистки VLAN 5 от обмена информацией по магистральным связям:

```
1900EN(config-if)#no trunk-vlan?
 <1-1005> ISLVLAN index
1900EN(config-if)#no trunk-vlan5
1900EN(config-if)#
```

К сожалению, в устройствах серии 1900 не существует команды одновременной очистки нескольких VLAN. На практике не возникает задач очистки большого числа сетей VLAN, поскольку с функциональной точки зрения включение магистрального режима не влияет на работу сети VLAN. Однако отмена магистрального режима иногда полезна для решения вопросов с безопасностью, ширококвещательными рассылками и обновлениями маршрутизации.

## Проверка магистральных связей

Для проверки магистральных портов используется команда `show trunk`. Если магистральными являются несколько портов, но нужна статистика только по одному из них, то применяется команда `show trunk [номер_порта]`.

Пусть в переключателе 1900 порт FastEthernet номер 0/26 является магистральным портом А, а порт 0/27 — магистральным портом В. Ниже показан листинг проверки магистрального порта в интерфейсе 26:

```
1900EN#sh trunk?
 A Trunk A
 B Trunk B
1900EN#sh trunk a
DISLstate: Auto, Trunking: On, Encapsulation type: ISL
```

Значение DISL равно auto, магистральный режим включен, и для магистральной связи установлен тип инкапсуляции VLAN, равный ISL.

Для просмотра разрешенных в магистральной связи сетей VLAN служит команда `show trunk [A или B] allowed-vlans`. Пример вывода допускаемых VLAN в магистральном интерфейсе 26:

```
1900EN#shtrunk ?
 A Trunk A
 B Trunk B
1900EN#sh trunk a ?
 allowed-vlans Display allowed vlans
 joined-vlans Display joined vlans
 joining-vlans Display joining vlans
 prune-eligible Display pruning eligible vlans
 <cr>
```

```
1900EN#sh trunk a allowed-vlans
1-4, 6-1004
1900EN#
```

В предыдущем разделе мы показали очистку VLAN 5, поэтому в листинге сеть VLAN 5 не включена в состав магистральных связей.

## Настройка маршрутизации ISL

Для поддержки маршрутизации ISL в отдельном интерфейсе FastEthernet этот интерфейс делится на несколько логических интерфейсов — по одному на каждую сеть VLAN. Получаем *подинтерфейсы*. В примерах мы работаем с четырьмя сетями VLAN, поэтому необходимы четыре подинтерфейса. Каждая сеть VLAN находится в собственной подсети, причем адресация такова:

VLAN 1 по умолчанию	172.16.10.0/24
VLAN 2 отдел продаж	172.16.20.0/24
VLAN 3 отдел маркетинга	172.16.30.0/24
VLAN 4 сеть mis	172.16.40.0/24

Все хосты одной сети VLAN должны иметь одинаковый адрес подсети. Для настройки каскада маршрутизаторов на маршрутизацию между сетями VLAN необходимо решить три задачи:

1. Разрешить магистральный режим ISL в порту переключателя, к которому подключен маршрутизатор.
2. Допустить инкапсуляцию ISL в подинтерфейсе маршрутизатора.
3. Присвоить IP-адрес подинтерфейсу и выполнить другую логическую адресацию, если это необходимо (например, присвоить адреса IPX).

Для создания подинтерфейса в режиме глобального конфигурирования укажите интерфейс FastEthernet, затем введите точку и далее номер. Появится приглашение (*config-subif*) нужного интерфейса.

Для настройки маршрутизации ISL в подинтерфейсе служит команда *encapsulation isl [номер\_VLAN]*. Затем можно присвоить подинтерфейсу IP-адрес, а также адреса IPX, AppleTalk и т.д. Это отдельная подсеть и все хосты сети VLAN должны принадлежать этой подсети. Данное правило не является обязательным, но настоятельно рекомендуется для выполнения на практике.

Вернемся к настройке маршрутизатора 2621 на поддержку маршрутизации ISL с четырьмя VLAN. Сначала настроим подинтерфейсы на номера, которые запланированы для VLAN. Номера являются логическими, т.е. их значения не влияют на номера подинтерфейсов в сети. Далее следует установить инкапсуляцию. В противном случае при попытке установки IP-адреса для подинтерфейса появится сообщение об ошибке. VLAN 1 находится в сети 172.16.10.0. Необходимо присвоить подинтерфейсу корректный адрес хоста из этой подсети.

```

2621#config t
2621(config) int f0/0.1
2621(config-subif)# encapsulation isl 1
2621(config-subif)# ip address 172.16.10.1 255.255.255.0
2621(config-subif)# int f0/0.2
2621(config-subif)# encapsulation isl 2
2621(config-subif)# ip address 172.16.20.1 255.255.255.0
2621(config-subif)# int f0/0.3
2621(config-subif)# encapsulation isl 3
2621(config-subif)# ip address 172.16.30.1 255.255.255.0
2621(config-subif)# int f0/0.4
2621(config-subif)# encapsulation isl 4
2621(config-subif)# ip address 172.16.40.1 255.255.255.0
2621(config-subif)# exit
2621(config)#int f0/0
2621(config-if) no shutdown

```

После настройки инкапсуляции и IP-адреса в сети VLAN 1, аналогичные операции следует провести для сетей VLAN 2, 3 и 4. Однако каждый подинтерфейс должен находиться в отдельной подсети.

## Настройка VTP

По умолчанию переключатель Catalyst 1900 настроен на режим сервера VTP, как впрочем и все остальные модели переключателей. Для настройки протокола VTP сначала нужно указать имя домена (см. ниже), а затем проверить конфигурацию с помощью параметра VTP.

### Настройка домена

В процессе настройки домена VTP можно указать его имя, пароль операционного режима и возможности по сокращению действия (pruning). Эти данные вводятся командой vtp в режиме глобального конфигурирования. Ниже показан пример установки переключателя в режим сервера VTP с доменом lammlle и паролем todd.

```

Todd1900EN(config)#vtp ?
 client VTP client
 domain Set VTP domain name
 password Set VTP password
 pruning VTP pruning
 server VTP server
 transparent VTP transparent
 trap VTP trap
Todd1900EN(config)#vtpserver

```

```
Todd1900EN(config)#vtp domain lammle
Todd1900EN(config)#vtp password todd
```

После ввода информации VTP нужно проверить конфигурацию командой `show vtp`.

```
Todd1900EN#sh vtp
VTP version: 1
Configuration revision: 0
Maximum VLANs supported locally: 1005
Number of existing VLANs: 5
VTP domain name : lammle
VTP password : todd
VTP operating mode : Server
VTP pruning mode : Disabled
VTP traps generation : Enabled
Configuration last modified by: 0.0.0.0 at 00-00-0000 00:00:00
Todd1900EN#
```

В листинге из переключателя показан домен VTP, пароль VTP и режим переключателя.

## Добавление в домен VTP

Добавлять новый переключатель в существующий домен нужно очень осторожно. Если добавляемый переключатель имеет некорректную информацию VLAN, то она из базы данных VTP может распространиться по всей объединенной сети. Компания Cisco рекомендует удалять базу данных VTP перед включением в домен VTP нового переключателя.

Мы уже обсуждали стирание NVRAM в переключателе 1900. Однако это не приводит к удалению конфигурации VTP в переключателе, поскольку информация VTP имеет собственную память NVRAM. Для удаления в переключателе 1900 информации VTP необходимо применить команду `delete vtp`. Пример удаления базы данных VTP из NVRAM:

```
Todd1900EN#delete ?
 nvram NVRAM configuration
 vtp Reset VTP configuration to defaults
```

```
Todd1900EN#delete vtp
```

This command resets the переключатель with VTP parameters set to factory defaults.

All other parameters will be unchanged.

Reset system with VTP parameters set to factory defaults,

[Y]es or [N]o? **Yes**

После ввода команды появится приглашение для установки информации VTP в значения фабричной конфигурации по умолчанию.

## Сокращение действия УТР

Рассмотрим пример установки режима ограничения действия в переключателе 1900. Помните, что включение режима ограничения действия протокола VTP на сервере VTP приводит к распространению его на весь домен.

```
Todd1900EN(config)#vtp ?
 client VTP client
 domain Set VTP domain name
 password Set VTP password
 pruning VTP pruning
 server VTP server
 transparent VTP transparent
 trap VTP trap
Todd1900EN(config)#vtp pruning ?
 disable Disable VTP pruning
 enable Enable VTP pruning
Todd1900EN(config)#vtp pruning enable
Todd1900EN(config)#
```

Ограничение действия VTP установлено для всего переключателя. Широковещательные рассылки VTP не будут направлять в магистральную сеть, если в переключателе для этой связи не сконфигурирована сеть VLAN.

## Восстановление и обновление IOS в переключателе Catalyst 1900

Допускается восстановление и обновление операционной системы IOS в переключателе Cisco Catalyst 1900, хотя не существует специальной команды для копирования образа IOS из переключателя Catalyst 1900 на хост TFTP.

Команда для восстановления и обновления IOS в переключателе 1900:

```
copy tftp://адрес_хоста_TFTP/имя_файла_IOSорcode
```

Здесь:

`copy tftp` указывает на копирование IOS из хоста TFTP.

`//адрес_хоста_TFTP` указывает адрес хоста TFTP.

`имя_файла_IOS` определяет файл в каталоге по умолчанию на хосте TFTP (например, `cat1900EN_9_00.bin` для корпоративной версии).

`орcode` — это команда для загрузки файла во флэш-память.

Пример команды:

```
1900B#copy tftp://192.168.0.120/cat1900EN_9_00.bin nvram
TFTP operation succeeded
1900B#
```

## Резервное копирование и восстановление конфигурации Catalyst 1900

Файл конфигурации переключателей Cisco Catalyst 1900 называется **nvram** для переключателей серии 1900. Команда копирования файла на хост TFTP:

```
copy nvram tftp://адрес_хоста_TFTP/имя_файла_конфигурации
```

Перед резервным копированием рекомендуется с консоли проверить хост TFTP утилитой Ping, чтобы гарантировать успешное подключение по локальной сети:

```
1900B#ping 192.168.0.120
Sending 5, 100-byte ICMP Echos to 192.168.0.120, time out
is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
0/2/10/ ms
```

Проверьте соединение, введите команду `copy nvram tftp:` для создания резервной копии конфигурации:

```
1900B#copy nvram tftp://192.168.0.120/1900en
Configuration upload is successfully completed
```

Вот пример вывода на консоль TFTP-хоста. -

```
Wed Jun 01 14:16:10 2000: Receiving '1900en' file from
192.168.0.120 in ASCII mode
##
Wed Mar 01 14:16:11 2000: Successful.
```

В нашем примере на хост TFTP скопированы два пакета UDP, которые отмечены в листинге символом "номер" (#) кода ASCII.

Для восстановления сохраненной на хосте TFTP конфигурации используется команда:

```
copy tftp://адрес_хоста_TFTP/имя_файла_конфигурации nvram
```

Для копирования из хоста TFTP необходимо знать имя файла и IP-адрес, например:

```
1900B#copy tftp://192.168.0.120/1900en nvram
TFTP successfully downloaded configuration file
```

Команда в конце строки указывает хосту TFTP на место копирования файла (в нашем случае — nvram).

Для удаления файла конфигурации **startup-config** (он же файл nvram) в переключателе 1900 служит команда `delete nvram`, например:

#### 1900B#delete nvram

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

(эта команда сбрасывает переключатель в фабричные значения по умолчанию. Все системные параметры будут возвращены в исходные значения по умолчанию. Будут удалены все статические и динамические адреса)

Reset system with factory defaults, [Y]es or [N]o? **Yes**

Данная команда почти не действует на переключатель, если не установлены сети VLAN. Переключатель прекрасно работает и без конфигурации, однако рекомендуется указать IP-адрес для управления устройством.

## Протокол CDP в переключателях 1900

Протокол CDP реализован во всех устройствах Cisco, в том числе в переключателе Catalyst 1900. Это подтверждается листингом из переключателя 1900:

```
switch#sh cdp
```

```
Global CDP information :
```

```
CDP version: 2
```

```
Sending CDP packets every 60 seconds
```

```
Sending a holdtime value of 180 seconds
```

```
#
```

Как маршрутизатор, так и переключатель имеет для таймера CDP значение 60 с и время удержания, равное 180 с (см. главу 7). Информация CDP, полученная из соседнего маршрутизатора, будет сохраняться 180 с. Если маршрутизатор или переключатель не получают от соседа следующего сообщения за время хранения, то информация удаляется.

### ▼ ВНИМАНИЕ

Переключатель 1900 способен объявить протокол CDP версии 2 — новый вариант CDP для некоторых современных устройств Cisco. Переключатель 1900 способен отправлять сообщения по протоколам CDP версий 1 и 2, но получать сообщения — только по протоколу CDP версии 1. В нашей книге не рассматривается CDP версии 2.

Допускается изменение значений таймеров в обоих устройствах командами `cdp timer` и `cdp holdtime` режима глобального конфигурирования:

```
switch#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z
```

```
switch(config)#cdp ?
```

```
advertise-v2 CDP sends version-2 advertisements
```

```
(отправка уведомлений по протоколу CDP версии 2)
```

```
holdtime Specify the holdtime (in sec) to be sent in packets
```

```
(время хранения в секундах, которое будет указано в пакетах)
```

```
timer Specify the rate at which CDP packets are sent (in sec)
```

```
(определяет частоту отправки пакетов CDP в секундах)
```

После этого перейдем к изменению таймера и времени хранения, например в переключателе 1900:

```
switch(config)#cdp timer 90
```

```
switch(config)#cdp holdtime 240
```

## Упражнение

---

Напишите команды для выполнения следующих операций:

1. Показ конфигурации переключателя
2. Показ конфигурации IP переключателя
3. Вывод фильтрующей таблицы MAC-адресов
4. Установка порта e0/2 для защищенной таблицы размером в одну запись
5. Присвоение MAC-адреса 1234.4567.8912 порту e0/1 в виде постоянного адреса
6. Удаление постоянного адреса, добавленного в порт e0/1
7. Просмотр статистики для порта e0/5
8. Создание трех сетей VLAN с именами: Purchasing, Sales и MIS
9. Присвоение портов 2 и 3 сети Sales, 4 и 5 — сети Purchasing, 6 и 7 — сети MIS (использовать только статическое присваивание)
10. Установка в переключателе режима клиента VTP
11. Установка в переключателе режима прозрачного переключателя
12. Вывод статуса VTP переключателя
13. Установка интерфейса B в режим автоопределения магистральной связи
14. Показ информации обо всех сетях VLAN переключателя
15. Присвоение интерфейса 5 сети VLAN 2

## Лабораторные работы

Нам предстоит выполнить семь лабораторных работ, в которых необходим доступ к переключателю 1900. Однако в двух работах можно использовать программный эмулятор CCNA e-trainer издательства Sybex, либо RouterSim версии 2.0 (см. [www.routersim.com](http://www.routersim.com)).

### О Лабораторная работа В. 1.

#### Обслуживание переключателя серии 1900

В этой лабораторной работе мы подключимся к устройству Cisco Catalyst 1900 и исследуем его возможности.

1. В переключателе 1900 введите К для перехода в режим CLI.
2. В интерфейсе CLI переключателя 1900 нажмите Enter, а затем в приглашении пользовательского режима (>) введите **enable**.
3. Введите **show running-config** для вывода текущей конфигурации. Обратите внимание на значения параметров по умолчанию.
4. Введите **show version** для вывода версии IOS, исполняемой переключателем.
5. Установите имя устройства командой hostname:  

```
config t
hostname 1900A
```
- i. Введите show ip для показа установленных по умолчанию IP-адреса, маски подсети и шлюза по умолчанию.
7. Установите для переключателя IP-адрес, маску подсети и шлюз по умолчанию командами:  

```
config t
ip address 172.16.10.3 255.255.255.0
ip default-gateway 172.16.10.1
```
8. Введите show ip для просмотра новой конфигурации.
9. В CLI проверьте доступ к маршрутизатору А по Ping командой ping [IP\_адрес].
10. Введите show mac-address-table для показа фильтрующей таблицы переключателя, используемой при перенаправлении.
11. Введите show interfaces для вывода статистики по всем интерфейсам.
12. Введите show int ? для вывода доступных команд Ethernet и Fast-Ethernet.
13. Введите sho int **Ethernet** ? для выбора карты 0. <0-0> означает одну карту с 12 или 24 портами.
14. Введите sh int e 0/? для вывода всех доступных интерфейсов.

15. Введите `sh int e 0/2` для показа статистики по интерфейсу Ethernet 2.
16. Введите `delete nvram` для удаления конфигурации запуска `startup-config`.

**ВНИМАНИЕ** | Нельзя увидеть содержимое файла `startup-config`, поскольку доступен только файл исполняемой конфигурации `running-config`. Кроме того, файл `running-config` автоматически сохраняется в памяти NVRAM.

## О Лабораторная работа В.2.

### Операции переключателя 1900

Во второй лабораторной работе мы установим пароли, IP-адрес и режим безопасности в переключателе 1900.

1. Нажмите К в консоли переключателя 1900А или 1900В для перехода в режим CLI.
2. Введите `en` или `enable` для перехода в привилегированный режим.
3. Установите три пароля командами:  
`config t`  
`enable password level 1 todd`  
`enable password level 15 todd1`  
`enable secret todd2`
4. Введите `sh run` для просмотра паролей. Разрешенные пароли не шифруются.
5. Перейдите в интерфейс Ethernet 0/5 и установите полнодуплексный режим.  
`config t`  
`int e0/5`  
`duplex full`
6. Перейдите в интерфейс Ethernet 0/6 и установите полудуплексный режим.  
`config t`  
`int e0/6`  
`duplex half`
7. Проверьте изменение режимов командой `sh interface`, `sh int e0/5` или `sh int e0/6`.
8. Удалите из переключателя все сведения о конфигурации IP:  
`Config t`  
`no ipaddress`
9. Проверьте отсутствие информации о IP командой `show ip`.

10. Установите IP-адрес, маску подсети и шлюз по умолчанию.

```
config t
ip address 172.16.10.100 255.255.255.0
ip default-gateway 172.16.10.1
```

11. Проверьте конфигурацию командой **show ip**.
12. Введите **show mac-address-table** для просмотра таблицы разных направлений. Все MAC-адреса будут найдены динамически.
13. Добавьте в фильтрующую таблицу статическую запись, воспользовавшись командой **permanent**:

```
config t
mac-address-table permanent 083c.0000.0001 e0/9
```

14. Введите **show mac-address-table** и обратите внимание на постоянную запись для интерфейса e0/9.
15. Глобальной командой **mac-address-table restricted static** свяжите с коммутируемым портом переключателя ограниченный статический адрес:

```
Config t
Mac-address-table restricted static 083c.0000.0002 e0/3 e0/4
```

Введенная команда разрешает только трафик к ограниченному статическому адресу 083c.0000.0002 интерфейса e0/3 из интерфейса e0/4.

16. Перейдите в интерфейс e0/1 и командой **port secure max-mac-count 1** установите безопасную адресацию, разрешающую для одного порта в фильтрующей таблице только один MAC-адрес. По умолчанию с одним портом может быть связано до 132 MAC-адресов. С помощью команды вам будет доступен порт только одной рабочей станции.

```
Config t
Int e0/1
Port secure max-mac-count 1
```

17. Проверьте установку безопасности в портах командой **show mac-address-table security**. Безопасность будет разрешена только в порту e0/1.

## О Лабораторная работа В.3.

### Создание сетей VLAN

В этой лабораторной работе мы сформируем в одном переключателе несколько виртуальных локальных сетей. В лабораторной работе В.4 мы зададим конфигурации сетей VTP, разрешающие распространение сведений о сети VLAN во второй переключатель.

1. Соединитесь по Telnet или подключитесь к первому устройству 1900. Установите для этого переключателя имя хоста 1900A.

```

ttconfig
(config)#hostname 1900A
1900A#

```

- Создайте четыре сети VLAN (2-5) и присвойте им имена согласно списку:

```

VLAN2=Sales
VLAN3=Management
VLAN4=Engineering
VLAN5=Marketing

```

```

1900A#config t
Enter configuration commands, one per line. End with CNTL/Z
1900A(config)#vlan 2 name Sales
1900A(config)#vlan 3 name Management
1900A(config)#vlan 4 name Engineering
1900A(config)#vlan 5 name Marketing
1900A(config)#exit

```

Проверьте конфигурацию сетей VLAN командой `show vlan`.

```

1900A#sh vlan
VLAN Name Status Ports

 1 default Enabled 1-12,AUI, A, B
 2 Sales Enabled
 3 Management Enabled
 4 Engineering Enabled
 5 Marketing Enabled
1002 fddi-default Suspended
1003 token-ring-defau Suspended
1004 fddinet-default Suspended
1005 trnet-default Suspended

```

# [листинг сокращен]

## О Лабораторная работа В.4.

### *Присваивание коммутируемых портов сетям VLAN*

В этой лабораторной работе мы настроим два порта переключателя для участия в каждой сети VLAN.

- Настройте порты 1 и 2 на сеть VLAN 2. Все порты принадлежат VLAN 1, пока не указано иное.

```

1900A#config t
Enter configuration commands, one per line. End with CNTL/Z
1900A(config)#int e0/1

```

```

1900A(config-if)#vlan-membershipstatic 2
1900A(config-if)#inteO/2
1900A(config-if)#vlan-membershipstatic 2

```

2. Присвойте порты 3 и 4 сети VLAN 3.

```

1900A(config-if)#inteO/3
1900A(config-if)#vlan-membershipstatic 3
1900A(config-if)#inteO/4
1900A(config-if)#vlan-membershipstatic 3

```

- Присвойте порты 5 и 6 сети VLAN 4.

```

1900A(config-if)#inteO/5
1900A(config-if)#vlan-membershipstatic 4
1900A(config-if)#inteO/6
1900A(config-if)#vlan-membershipstatic 4

```

- Присвойте порты 7 и 8 сети VLAN 5.

```

1900A(config-if)#inteO/7
1900A(config-if)#vlan-membershipstatic 5
1900A(config-if)#inteO/8
1900A(config-if)#vlan-membershipstatic 5
1900A(config-if)#exit
1900A(config)#exit

```

3. Проверьте конфигурацию командой `show vlan`.

```
1900A#sh vlan
```

VLAN	Name	Status	Ports
1	default	Enabled	8-12, AUI, A, B
2	Sales	Enabled	1-2
3	Management	Enabled	3-4
4	Engineering	Enabled	5-6
5	Marketing	Enabled	7-8
1002	fddi-default	Suspended	
1003	token-ring-defau	Suspended	
1004	fddinet-default	Suspended	
1005	trnet-default	Suspended	

4. Проверьте участие в сетях VLAN командой `show vlan-membership`.

```
1900A#sh vlan-membership
```

Port	VLAN	Membership
1	2	Static

```

2 2 Static
3 3 Static
4 3 Static
5 4 Static
6 4 Static
7 5 Static
8 5 Static
9 1 Static
10 1 Static
11 1 Static
12 1 Static
AUI 1 Static
A 1 Static
B 1 Static

```

```
1900A#
```

## О Лабораторная работа В. 5.

### Настройка магистральных связей

Перед разрешением совместного использования информации со вторым переключателем необходимо настроить связи между устройствами. Не обязательно конфигурировать магистральную связь, но тогда через переключатель будет пересылаться только информация о сети VLAN 1. Мы же хотим настроить устройство так, чтобы информация всех сетей VLAN пересылалась между переключателями.

1. В устройстве 1900A настройте порт 26 на режим автоопределения магистральной связи. Вы сможете включить магистральный режим, как только он будет установлен в магистральном порту второго переключателя.

```
1900A#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z
```

```
1900A(config)#intf 0/26
```

```
1900A(config-if)#trunk?
```

```
auto Set DISL state to AUTO
```

```
desirable Set DISL state to DESIRABLE
```

```
nonegotiate Set DISL state to NONEGOTIATE
```

```
off Set DISL state to OFF
```

```
on Set DISL state to ON
```

```
1900EN(config-if)#trunk auto
```

2. Подключите второе устройство 1900 и присвойте ему имя 1900B. Укажите для порта 26 режим постоянной транковой связи.

```
#config t
```

```
Enter configuration commands, one per line. End with CNTL/Z
```

```

(config)#hostname 1900B
1900B(config)#int f0/26
1900B(config-if)#trunk?
 auto Set DISL state to AUTO
 desirable Set DISL state to DESIRABLE
 nonegotiate Set DISL state to NONEGOTIATE
 off Set DISL state to OFF
 on Set DISL state to ON
1900B(config-if)#trunk on

```

## О Лабораторная работа В.6. Настройка VTP

В этой лабораторной работе мы настроим в переключателе 1900А имя домена VTP, сделаем клиентским второй переключатель и проверим обновление информации VTP от сервера к клиенту.

1. Соединитесь по Telnet или подключитесь к консоли устройства 1900А. Установите этот переключатель в режим сервера VTP (это уже сделано по умолчанию, но мы хотим показать пример ввода команд).

```

1900A#config t
1900A(config)#vtpserver

```

2. Установите имя домена VTP — Classroom1.

```

1900A#config t
1900A(config)#vtpdomain Classroom1

```

3. Проверьте правильность настройки информации VTP.

```

1900A#showvtp

```

4. Соединитесь по Telnet или подключитесь к консоли устройства 1900В, установите имя домена VTP и укажите режим клиента VTP.

```

1900B#config t
1900B(config)#vtpdomain Classroom1
1900B(config)#vtp client

```

5. Проверьте конфигурацию VTP в обоих переключателях командой `show vtp`, а также распространение информации VLAN от серверного переключателя к клиентскому. Воспользуйтесь командой `show vlan`.

6. В устройстве 1900В введите `show vlan` для проверки распространения информации VLAN от переключателя 1900А.

```

1900B#sh vlan

```

VLAN	Name	Status	Ports
1	default	Enabled	1-12, AUI, A, B
2	Sales	Enabled	

3	Management	Enabled
4	Engineering	Enabled
5	Marketing	Enabled
1002	fddi-default	Suspended
1003	token-ring-defau	Suspended
1004	fddinet-default	Suspended
1005	trnet-default	Suspended

Были обнаружены сети VLAN, но все порты переключателя 1900B принадлежат VLAN 1. Если не указано иное, то все порты присваиваются сети VLAN. Однако рекомендуется устанавливать порты в каждом переключателе (протокол VTP передает информацию о сетях VLAN, но не сведения о портах).

## О Лабораторная работа В.7. Настройка маршрутизации между сетями VLAN с помощью ISL

После настройки сетей VLAN и включения режима обмена между переключателями информацией о домене VTP (что приводит к согласованию конфигураций VLAN в обоих устройствах), нужно настроить маршрутизатор 2600 на поддержку маршрутизации между сетями VLAN.

1. Подключите маршрутизатор 2600 к одному из портов FastEthernet любого переключателя. Место подключения маршрутизатора к коммутационной фабрике безразлично.

2. Настройте порт переключателя на режим магистральной связи.

```
1900A#config t
1900A(config)#int f0/027
1900A(config-if)#trunk on
```

3. Настройте порт FastEthernet маршрутизатора 2600 для перенаправления трафика между всеми сетями VLAN.

```
2621#config t
2621(config)#int f0/0.1
2621(config-if)#no shutdown
2621(config-subif)#encapsulation isl 1
2621(config-subif)# ip address 172.16.10.1 255.255.255.0
2621(config-subif)# int f0/0.2
2621(config-subif)# encapsulation isl 2
2621(config-subif)# ip address 172.16.20.1 255.255.255.0
2621(config-subif)# int f0/0.3
2621(config-subif)# encapsulation isl 3
2621(config-subif)# ip address 172.16.30.1 255.255.255.0
2621(config-subif)# intf0/0.4
```

```
2621(config-subif)# encapsulation isl 4
2621(config-subif)# ip address 172.16.40.1 255.255.255.0
2621(config-subif)# encapsulation isl 5
2621(config-subif)# ip address 172.16.50.1 255.255.255.0
2621(config-subif)# exit
2621(config)#int f0/0
```

Помните, что каждый хост в настроенной сети VLAN должен принадлежать одной подсети.

## Проверочные вопросы

---

1. Что не характерно для переключателя 1900?
  - A. Поддерживается Ping из переключателя 1900, если такой режим установлен.
  - B. Поддерживается Ping к переключателю 1900, если такой режим установлен.
  - C. Поддерживается Telnet к переключателю 1900, если такой режим установлен.
  - D. Поддерживается Telnet из переключателя 1900, если такой режим установлен.
2. Какая команда установит для интерфейса e0/10 переключателя 1900 полнодуплексный режим Ethernet?
  - A. full duplex on
  - B. duplex on
  - C. duplex full
  - D. full-duplex
  - E. set duplex on full
3. Какая команда установит интерфейс переключателя 1900 так, что буфер не будет переполняться по перегруженным линиям?
  - A. flow on
  - B. duplex flow control
  - C. duplex full-flow-control
  - D. full duplex-flow
4. Какая команда проверит дуплексный режим порта 26 переключателя 1900?
  - A. show port 26
  - B. show int 26
  - C. show int e0/26
  - D. show int f0/26
  - E. show int g0/26
  - F. show int h0/26

5. Что справедливо для лампочки статуса порта в переключателе?
  - A. Используется для показа возникновения петель в сети.
  - B. Идентифицирует сигналы RTS.
  - C. При подключении устройства к порту лампочка включается и остается в этом состоянии.
  - D. При подключении устройства к порту лампочка включается, а затем выключается.
6. Какая команда удалит файл startup-config в переключателе 1900?
  - A. erase startup-config
  - B. delete startup-config
  - C. delete nvram
  - D. delete startup
7. Какая команда позволит установить, что порт 3 переключателя 1900 соединен с сервером Finance Server?
  - A. int e0/3, description Finance Server
  - B. int e0/3, description Finance\_Server
  - C. set port name e0/3 Finance Server
  - D. set port name e0/3 Finance\_Server
8. Кабель какого типа соединяет два каскадных порта переключателей?
  - A. Прямой
  - B. Плоский
  - C. Перекрестный
  - D. Волоконно-оптический
9. Как установить пароль пользовательского режима в переключателе 1900?
  - A. usermode password todd
  - B. enable password todd
  - C. enable password level 1 todd
  - D. enable password level 15 todd
10. Какая команда установит пароль разрешенного режима в переключателе 1900?
  - A. 1900EN(config)#enablepassword level 1 todd
  - B. 1900EN(config)#enablepassword level 15 todd
  - C. 1900EN#set enable password todd
  - D. 1900EN(Config)#enablepassword todd
11. Какая команда покажет конфигурацию IP переключателя 1900?
  - A. sh ip config
  - B. ship
  - C. sh int config
  - D. sh int

12. Какая команда установит IP-адрес и шлюз по умолчанию в переключателе 1900 (укажите все правильные ответы)?
- A. ip address 172.16.10.16 255.255.255.0
  - B. ip default-gateway 172.16.10.1**
  - C. ip address 172.16.10.1 mask 255.255.255.0
  - D. default-gateway 172.16.10.10
13. Что справедливо для паролей в переключателе Catalyst 1900?
- A. Должно быть не менее восьми символов.**
  - B. Чувствительны к регистру.
  - C. Не могут быть короче четырех символов и длиннее восьми символов.
  - D. Не чувствительны к регистру.
14. Что справедливо для пароля разрешенного секрета?
- A. Чувствителен к регистру
  - B. Не используется в переключателе 1900**
  - C. Применяется вместо разрешенного пароля, когда установлены оба эти пароля
  - D. Не используется вместо разрешенного пароля, когда установлены оба эти пароля
15. Какая команда покажет постоянные MAC-адреса из фильтрующей таблицы?
- A. Todd1900EN#sh mac-filter-table
  - B. Todd1900EN#sh mac-address-table**
  - C. Todd1900EN(config)#sh mac-address-table
  - D. Todd1900EN#sh filter-address-table
16. Каковы три способа настройки переключателя 1900?
- A. VSM
  - B. VLSM**
  - C. Меню
  - D. CLI
  - E. CLIM
17. Какая команда установит имя переключателя?
- A. Switch name Cisco1900
  - B. Description 1900switch**
  - C. host name 1900
  - D. hostname 1900ethernet
18. Что из перечисленного является частью конфигурации по умолчанию в переключателе 1900?

- A. CDP: Допускается
  - B. IP-адрес: 192.168.10.2
  - C. Шлюз по умолчанию: 0.0.0.0
  - D. Режим коммутации: FragmentFree
  - E. Порт 10BaseT: Автосогласование дуплексного режима
  - F. Порт 100BaseT: Полудуплексный режим
  - G. Покрывающее дерево: Разрешено
  - H. Консольный пароль: Cisco
19. Какая команда покажет статистику порта 2 в переключателе?
- A. show int 2
  - B. show int eth 0/2
  - C. sh int e/2
  - D. show interfO/2
20. Какая команда покажет статистику порта 27?
- A. show int 27
  - B. show int eth 0/27
  - C. sh int f/27
  - D. sh inter f0/27
21. Какая команда разрешит связать с портом только один MAC-адрес?
- A. Todd1900EN(config-if)#port secure max-mac-count 1
  - B. Todd1900EN(config-if)#port max-mac-count secure 1
  - C. Todd1900EN(config)#mac-address-table restricted static 00A0.246E.0FA8 e0/2
  - D. Todd1900EN(config)#mac-address-table permanent 00A0.2448.60A5 e0/4
22. Какая часть команды служит для установки аппаратного адреса для порта e0/4 так, что разрешенным будет только MAC-адрес 00A0.2448.60A5?
- A. int e0/4 set MAC 00A0.2448.60A5
  - B. Todd1900EN(config)#mac-address-table restricted static 00A0.2448.60A5 e0/2
  - C. Todd1900EN(config)#mac-address-table permanent 00A0.2448.60A5 e0/4
  - D. Todd1900EN(config-if)#portsecure max-mac-count00A0.2448.60A5
23. Какая команда позволит только порту e0/5 переключателя 1900 взаимодействовать с аппаратным адресом 00A0.246E.0FA8?
- A. int e0/5 out 00A0.246E.0FA8
  - B. Todd1900EN(config)#mac-address-table permanent 00A0.246E.0FA8 e0/4

- C. Todd1900EN(config-if)#port secure max-mac-count  
OOA0.246E.OFA8
- D. Todd1900EN(config)#mac-address-table restricted  
static OOA0.246E.OFA8 eO/2 eO/5

## Ответы к упражнению

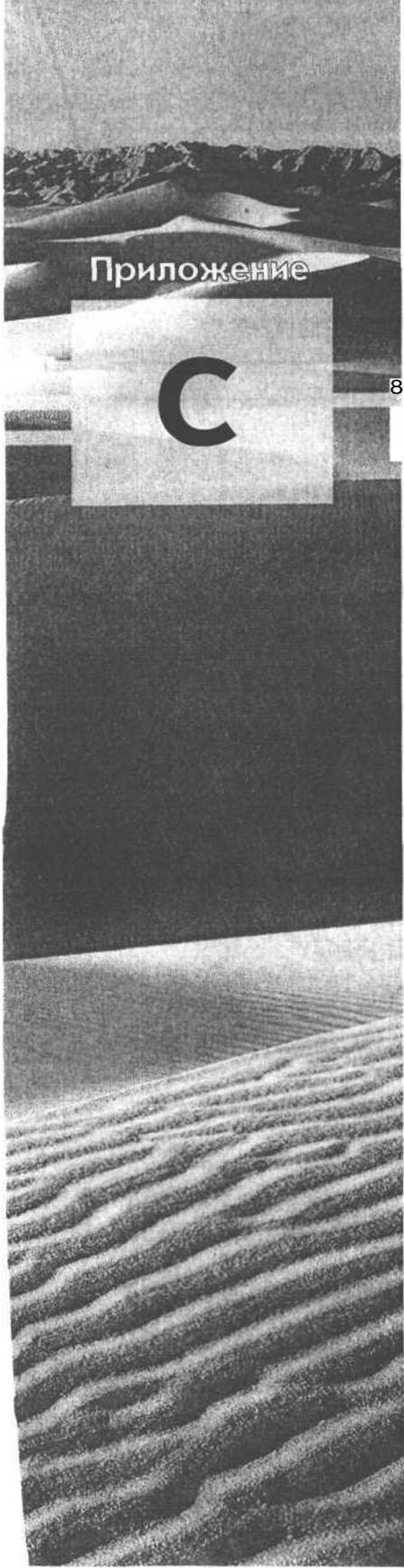
---

1. show running-config
2. sh ip
3. show mac-address-table
4. port secure max-mac-count 1
5. mac-address-table permanent 1234.4567.8912 eO/1
6. clear mac-address-table permanent 1234.4567.8912 eO/1
7. show int eO/5
8. **config t**  
**vlan 2 Purchasing**  
**vlan 3 Sales**  
**vlan 4 MIS**
9. **int eO/2**  
**vlan-membership static 3**  
**int eO/3**  
**vlan-membership static 3**  
**int eO/4**  
**vlan-membership static 2**  
**int eO/5**  
**vlan-membership static 2**  
**int eO/6**  
**vlan-membership static 4**  
**int eO/7**  
**vlan-membership static 4**
10. config t vtp client
11. config t vtp transparent
12. show vtp
13. int fO/27, trunk auto
14. show vlan
15. config t int eO/5, vlan-membership static 2

## Ответы на проверочные вопросы

1. D
2. C
3. C
4. D
5. C
6. C
7. B
8. C
9. C
10. B
11. B
12. A, B
13. C, D
14. C
15. B
16. A, C, D
17. D
18. A, C, D, G
19. B
20. D
21. A
22. C
23. D





Приложение

**C**

8

# Справочник команд Cisco

В этом приложении перечислены все команды, упомянутые в книге.

Команда	Описание	Глава
?	Вывод экрана справки	4
0.0.0.0 255.255.255.255	Заменитель, то же самое, что команда any	9
access-class	Применение стандартного списка доступа IP к линии VTY	9
access-list	Создание списка условий для фильтрации сети	9
any	Любой хост или любая сеть подобно 0.0.0.0 255.255.255.255	9
Backspace	Удаление одного символа	4
bandwidth	Установка полосы пропускания в последовательном интерфейсе	4
banner	Создание баннера для пользователя, входящего в систему маршрутизатора	4
cdp enable	Включение CDP в отдельный интерфейс	7
cdp holdtime	Изменение времени удержания пакетов CDP	7
cdp run	Включение протокола CDP в маршрутизаторе	7
cdp timer	Изменение таймера обновления CDP	7
clear counters	Очистка счетчиков статистики в интерфейсе	4
clear line	Очистка линии соединения по Telnet с маршрутизатором	7
clear mac-address-table	Очистка динамически созданной фильтрующей таблицы	Прилож. В
clock rate	Обеспечение тактовой частотой последовательного интерфейса DCE	4
configmemory	Копирование файла startup-config в running-config	4
config network	Копирование конфигурации из хоста TFTP в файл running-config	4
config terminal	Переход в режим глобального конфигурирования и изменение running-config	4
config-register	Загрузка маршрутизатора и изменение параметров конфигурационного регистра	7
copy flash tftp	Копирование файла из флэш-памяти на хост TFTP	7

Команда	Описание	Глава
copy run start	Краткая форма команды copy <i>running-config startup-config</i> . Запись конфигурации в NVRAM	4, 7
copy run tftp	Копирование файла <i>running-config</i> на хост TFTP	7
copy tftp flash	Копирование файла с хоста TFTP во флэш-память	7
copy tftp run	Копирование конфигурации из хоста TFTP в файл <i>running-config</i>	7
Ctrl+A	Перемещение курсора в начало строки	4
Ctrl+D	Удаление одного символа	4
Ctrl+E	Перемещение курсора в конец строки	4
Ctrl+F	Перемещение вперед на один символ	4
Ctrl+R	Повторный вывод строки	4
Ctrl+Shift+6, затем X	Возврат в исходный маршрутизатор во время подключения по Telnet к другим маршрутизаторам	7
Ctrl+U	Стирание строки	4
Ctrl+W	Стирание слова	4
Ctrl+Z	Завершение конфигурационного режима и возврат в EXEC	4
debug dialer	Показ процедур установки вызова и прерывания	10
debug frame-relay lmi	Показ обмена данными LMI между маршрутизатором и переключателем Frame Relay	10
debug ip igrp events	Итоговая информация о протоколе маршрутизации IGRP	5
debug ip igrp transactions	Показ сообщения с запросом соседнего маршрутизатора об обновлении или о широковещательной рассылке по всем соседним маршрутизаторам	5
debug ip rip	Отправка консольного сообщения с информацией о пакетах RIP, принятых и отправленных интерфейсом маршрутизатора	5
debug ipx	Показ информации RIP и SAP, прошедшей через маршрутизатор	8
debug isdn q921	Показ процессов уровня 2	10
debug isdn q931	Показ процессов уровня 3	10
delete nvram	Удаление содержимого NVRAM в переключателях серии 1900	7, прил. В
delete vtp	Удаление из переключателя конфигурации VTP	Прил. В
description	Установка описания интерфейса	4, прил. В
dialer idle-timeout number	Установка для линии BRI времени отмены, если не будет получен "интересный" трафик	10

Команда	Описание	Глава
dialer list number protocol protocol permit/deny	Указание "интересного" трафика для связи DDR	10
dialer load-threshold number inbound/outbound/either	Установка времени включения второго интерфейса BRI для линии ISDN	10
dialer map protocol address name hostname number	Используется вместо строки вызова для усиления защиты сети ISDN	10
dialer-string	Установка телефонного номера для вызова интерфейса BRI	10
disable	Возврат из привилегированного режима в пользовательский	4
disconnect	Разрыв соединения к удаленному маршрутизатору со стороны исходного маршрутизатора	7
duplex	Установка дуплексного режима в интерфейсе	Прил. В
enable	Переход в привилегированный режим	4
enable password	Установка нешифрованного разрешенного пароля	4
enable password Level 1	Установка пароля пользовательского режима	Прил. В
enable password Level 15	Установка пароля разрешенного режима	Прил. В
enable secret	Установка зашифрованного пароля разрешенного режима. При установке заменяет разрешенный пароль	4, Прил. В
encapsulation	Установка типа кадров в интерфейсе	8
encapsulation frame-relay	Установка инкапсуляции Frame Relay в последовательной линии	10
encapsulation frame-relay ietf	Установка типа инкапсуляции Internet Engineering Task Force (IETF) для связи маршрутизаторов Cisco с оборудованием других компаний	10
encapsulation hdlc	Восстановление инкапсуляции по умолчанию HDLC в последовательной линии	10
encapsulation isl 2	Установка маршрутизации ISL для сети VLAN 2	Прил. В
encapsulation ppp	Установка инкапсуляции PPP в последовательной линии	10
erase startup	Удаление файла startup-config	4
erase startup-config	Удаление содержимого NVRAM в маршрутизаторе	7
Esc+B	Переход назад на одно слово	4
Esc+F	Переход вперед на одно слово	4
exec-timeout	Установка тайм-аута в секундах и минутах для консольного подключения	4
exit	Разрыв подключения по Telnet к удаленному маршрутизатору	7

Команда	Описание	Глава
frame-relay interface-did	Настройка адреса цепи PVC в последовательном интерфейсе или подинтерфейсе	10
frame-relay lmi-type	Настройка типа LMI в последовательной линии	10
frame-relay map protocol address	Создание статического отображения в сети Frame Relay	10
Host	Указание адреса отдельного хоста	9
hostname	Установка имени маршрутизатора или переключателя	4, прил. В
int e0.10	Создание подинтерфейса	8
int f0/0.1	Создание подинтерфейса	Прил. В
interface	Переход в режим настройки интерфейса. Также используется в команде show	4
interface e0/5	Настройка интерфейса Ethernet 5	Прил. В
interface ethernet 0/1	Настройка интерфейса e0/1	Прил. В
interface f0/26	Настройка интерфейса FastEthernet 26	Прил. В
interface fastethernet 0/0	Переход в режим настройки порта FastEthernet. Также используется в команде show	4
interface fastethernet 0/0.1	Создание подинтерфейса	4
interface fastethernet 0/26	Настройка интерфейса f0/26	Прил. В
interface s0.16 multipoint	Создание многоточечного интерфейса в последовательной линии для сети Frame Relay	10
interface s0.16 point-to-point	Создание подинтерфейса "точка-точка" в последовательной линии для сети Frame Relay	10
interface serial 5	Переход в режим настройки интерфейса serial 5, а также в команде show	4
ip access-group	Применение к интерфейсу списка доступа IP	9
ip address	Установка IP-адреса интерфейса или переключателя	4, прил. В
ip classless	Команда глобального конфигурирования для установки в маршрутизаторе режима перенаправления пакетов в маршрутизатор по умолчанию, когда в таблице маршрутизации нет данных о сети назначения	5
ip default-gateway	Установка шлюза по умолчанию для переключателя	Прил. В
ip domain-lookup	Включение просмотра DNS (включен по умолчанию)	7
ip domain-name	Применение доменного имени во время просмотра DNS	7
ip host	Создание в маршрутизаторе таблицы хостов	7

Команда	Описание	Глава
ip name-server	Установка IP-адресов не более чем шести серверов DNS	7
ip route	Создание в маршрутизаторе статических путей и путей по умолчанию	5
ipx access-group	Применение к интерфейсу списка доступа IPX	9
ipx input-sap-filter	Применение к интерфейсу входного фильтра IPX SAP	9
ipx network	Присваивание интерфейсу номера сети IPX	8
ipx output-sap-filter	Применение к интерфейсу выходного фильтра IPX SAP	9
ipx ping	Программа Packet Internet Groper для тестирования прохождения пакетов IPX в объединенной сети	8
ipx routing	Включение маршрутизации IPX	8
isdn spid1	Установка номера для идентификации первого DSO в переключателе ISDN	10
isdn spid2	Установка номера для идентификации второго DSO в переключателе ISDN	10
isdn switch-type	Установка типа коммутации ISDN в маршрутизаторе. Может устанавливаться в глобальном режиме или на уровне интерфейсов	10
K	Используется во время запуска переключателя 1900 для перехода в режим CLI	Прил. В
line	Переход в конфигурационный режим для изменения или установки паролей пользовательского режима	4
line aux	Переход в режим настройки дополнительного интерфейса	4
line console 0	Переход в режим настройки консоли	4
line vty	Переход в режим настройки интерфейса VTY (Telnet)	4
logging synchronous	Отмена перезаписи командной строки консольными сообщениями	4
logout	Вход в консольный сеанс	4
mac-address-table permanent	Создание постоянной записи для MAC-адреса в фильтрующей базе данных	Прил. В
mac-address-table restricted static	Установка ограниченного адреса для фильтрующей базы данных MAC-адресов, чтобы разрешить интерфейсу взаимодействие только с указанным ограниченным адресом	Прил. В
media-type network	Установка в интерфейсе типа аппаратного носителя	4
network	Указание объявляемого протокола маршрутизации	5

Команда	Описание	Глава
no cdp enable	Выключение CDP в отдельном интерфейсе	7
no cdp run	Выключение CDP во всем маршрутизаторе	7
no inverse-arp	Выключение динамического протокола IARP в Frame Relay. Необходимо настроить статическое отображение	10
no ip domain-lookup	Выключение просмотра DNS	7
no ip host	Удаление имени из таблицы хостов	7
no IP route	Удаление статического пути или пути по умолчанию	5
no shutdown	Включение интерфейса	4
o/r 0x2142	Изменение загрузки в 2501 для отмены использования NVRAM	7
ping	Проверка подключения IP к удаленному устройству	4, 7, прил. В
port secure max-mac-count	Разрешение подключения и работы с интерфейсом только определенным устройствам	Прил. В
ppp authentication chap	Установка в PPP аутентификации CHAP	10
ppp authentication pap	Установка в PPP аутентификации PAP	10
router igrpas	Включение в маршрутизации IP IGRP	5
router rip	Переход в режим конфигурации RIP	4, 5
secondary	Добавление второй сети IPX в тот же самый физический интерфейс	8
Service password-encryption	Шифрование разрешенного пароля и пароля пользовательского режима	4
show access-list	Показ всех списков доступа маршрутизатора	9
show access-List 110	Показ только списка доступа 110	9
show cdp	Вывод значения таймера CDP и частоты для удержания	7
show cdp entry *	Подобна show cdp neighbor detail, но не действует в переключателях 1900	7
show cdp interface	Показ отдельных интерфейсов, где разрешен протокол CDP	7
show cdp neighbor	Показ непосредственно подключенных соседей и сведений о них	7
show cdp neighbor detail	Показ IP-адреса, номера версии IOS и типа, а также всех сведений из команды show cdp neighbor	7
show cdp traffic	Показ принятых и переданных пакетов CDP и всех ошибок	7
Show controllers 0	Показ статуса (DTE или DCE) интерфейса	4

Команда	Описание	Глава
showdialer	Показ промежутка времени для достижения строки набора, времени холостого хода во всех каналах В, длины вызова и имени маршрутизатора, к которому подключен интерфейс	10
showflash	Показ файлов из флэш-памяти	7
show frame-relay lmi	Установка типа LMI в последовательном интерфейсе	10
showframe-relaymap	Показ статического и динамического отображения сетевого уровня на цепи PVC	10
showframe-relay pvc	Показ настроенных в маршрутизаторе номеров PVC и DLCI	10
Show history	Показ последних 10-ти введенных команд (по умолчанию)	4
show hosts	Показ содержимого таблицы хостов	7
show int f0/26	Показ статистики интерфейса f0/26	Прил. В
show int e0/1	Показ статистики интерфейса e0/1	Прил. В
Show interface s0	Показ статистики интерфейса serial 0	4
show ip	Показ конфигурации IP в переключателе	Прил. В
show ip access-list	Показ только списков доступа IP	9
show ip interface	Показ интерфейсов, к которым применены списки доступа IP	9
show ip protocols	Показ протоколов маршрутизации и таймеров этих протоколов для каждого из настроенных в маршрутизаторе протоколов	5
show ip route	Вывод таблицы маршрутизации IP	5, 10
show ipx access-list	Показ списков доступа IPX, настроенных в маршрутизаторе	9
show ipx interface	Показ информации RIP и SAP, получаемой и принимаемой в определенном интерфейсе. Дополнительно выводится адрес IPX этого интерфейса	8, 9
show ipx route	Показ таблицы маршрутизации IPX	8
show ipx servers	Показ таблицы SAP в маршрутизаторе Cisco	8
show ipx traffic	Показ информации RIP и SAP, получаемой и отправляемой маршрутизатором Cisco	8
show isdn active	Показ количества вызовов и их исполнения	10
show isdn status	Показ корректных SPID и правильность их использования при подключении и взаимодействии с переключателем провайдера	10
show mac-address-table	Показ динамически созданной в переключателе фильтрующей таблицы	Прил. В

Команда	Описание	Глава
show protocols	Показ протоколов маршрутизации и сетевых адресов всех интерфейсов	5, 8
show run	Краткая форма команды show running-config. Показ текущей исполняемой конфигурации маршрутизатора	4, 7, прил. В
show sessions	Показ подключений по Telnet к удаленным устройствам	7
show start	Краткая форма команды show startup-config. Показ резервной конфигурации, хранящейся в NVRAM	4, 7
Show terminal	Показ размера файла журнала	4
show trunk A	Показ статуса магистрального порта 26	Прил. В
show trunk B	Показ статуса магистрального порта 27	Прил. В
show version	Предоставляет сведения о системе IOS переключателя, а также время его работы и базовый адрес Ethernet	4, 7, прил. В
showvlan	Показ всех сконфигурированных сетей VLAN	Прил. В
show vlan-membership	Показ всех портов, присвоенных сетям VLAN	Прил. В
show vtp	Показ конфигурации VTP переключателя	Прил. В
shutdown	Перевод интерфейса в режим административного выключения	4
Tab	Автозавершение ввода команды	4
telnet	Подключение, просмотр и запуск программ на удаленном устройстве	4, 7
Terminal history size	Изменение размера журнала (по умолчанию 10, максимально 256)	
trace	Тестирование подключения к удаленному устройству и показ пути к нему в объединенной сети	4, 7
traffic-share balanced	Перевод протокола маршрутизации IGRP в режим совместного использования линий обратно пропорционально их метрикам	5
traffic-share min	Перевод протокола маршрутизации IGRP в режим использования путей только с минимальной стоимостью	5
trunk auto	Установка порта в режиме автоопределения магистральной связи	Прил. В
trunk on	Установка в постоянный магистральный режим	Прил. В
username name password password	Создание имени пользователя и пароля для аутентификации в маршрутизаторе Cisco	10
variance	Управление балансировкой нагрузки между наилучшей и наихудшей из допустимых метрик	5

Команда	Описание	Глава
vlan 2 name Sales	Создание сети VLAN 2 с именем Sales	Прил. В
vlan-membership static 2	Статическое присваивание порта сети VLAN	Прил. В
vtp client	Установка переключателя в режим клиента VTP	Прил. В
vtp domain	Установка имени домена для конфигурации VTP	Прил. В
vtp password	Установка пароля для домена VTP	Прил. В
vtp pruning enable	Установка ограничения действия в переключателе	Прил. В
vtp server	Установка переключателя в режим сервера VTP	Прил. В



**A&B bit signaling** Процедура, используемая для передачи данных по линиям T1, при которой в каждом из 24-х подканалов T1 один бит из каждого шестого кадра отводится для передачи информации об управлении сигналами. Также называется "24-канальной схемой передачи сигналов".

**AAL (ATM Adaptation Layer)** Уровень адаптации ATM. Подуровень канального уровня, зависящий от предоставляемых услуг. AAL принимает данные от различных приложений и доставляет их на уровень ATM (ATM layer) в форме 48-байтовых сегментов полезной нагрузки ATM. Состоит из двух подуровней: подуровня сходимости (CS) и подуровня сегментации и повторной сборки (SAR). Уровни адаптации различаются в зависимости от используемого способа синхронизации источника и получателя, от применения постоянной (CBR) или переменной (VBR) скорости передачи двоичных данных, а также от того, является или нет режим передачи данных ориентированным на установление соединения. В настоящее время ИТУ-Т рекомендует четыре типа уровней адаптации ATM: AAL1, AAL2, AAL3/4, AAL5. *См. также AAL1, AAL2, AAL3/4, AAL5, CS, SAR, ATM и ATM layer.*

**AAL1** Уровень адаптации ATM 1. Один из четырех рекомендованных ИТУ-Т уровней адаптации ATM. Используется для служб, ориентированных на установление соединения, чувствительных к величине задержки и требующих постоянной скорости передачи двоичных данных, например для пересылки видеоданных без сжатия или другого изохронного трафика. *См. также AAL.*

**AAL2** Уровень адаптации ATM 2. Один из четырех рекомендованных ИТУ-Т уровней адаптации ATM. Используется для служб, ориентированных на установление соединения и поддерживающих передачу двоичных данных с переменной скоростью, например для пересылки некоторых изохронных видео- и аудиоданных. *См. также AAL.*

**AAL3/4** Уровень адаптации ATM 3/4. Один из четырех рекомендованных ИТУ-Т уровней адаптации ATM, объединяющий два первоначально отдельных уровня. Используется для служб, как ориентированных, так и не ориентированных на установление соединения, но в первую очередь — для передачи по сетям ATM пакетов SMDS. *См. также AAL.*

**AAL5** Уровень адаптации ATM 5. Один из четырех рекомендованных ИТУ-Т уровней адаптации ATM. Используется для служб, ориентированных на установление соединения, поддерживающих передачу двоичных данных с переменной скоростью, но в первую очередь — для пересылки данных классического протокола IP по сетям ATM и LANE. AAL5 поддерживает схему SEAL и является наименее сложным из всех рекомендуемых уровней адаптации. Характеризуется незначительным снижением пропускной способности и упрощенными требованиями к обработке данных, поэтому применяется там, где необходимо сохранять пропускную способность и осуществлять коррекцию ошибок. *См. также AAL и SEAL.*

**AARP (AppleTalk Address Resolution Protocol)** Протокол определения адреса AppleTalk. Протокол из стека протоколов AppleTalk, с помощью которого адрес канального уровня преобразуется в сетевой адрес.

**AARP probe packets** Пробные пакеты AARP. Передаются по протоколу AARP с целью определения, используется ли случайно выбранный идентификатор узла другим узлом в нерасширенной сети AppleTalk. Узел, пославший пакет, завладевает идентификатором, если выясняется, что последний свободен. Если идентификатор уже занят, узел выбирает другой идентификатор и вновь посылает пробный пакет. *См. также AARP.*

**ABM (Asynchronous Balanced Mode)** Асинхронный сбалансированный режим. Режим процедур (и протокола) HDLC для организации однорангового двухточечного взаимодействия двух станций, при котором передаче может начать любая станция.

**ABR (Area Border Router)** Граничный маршрутизатор области. Маршрутизатор, размещенный на границе одной или нескольких областей OSPF и связывающий эти области с магистральной сетью. Считается, что такие маршрутизаторы принадлежат как магистрали OSPF, так и связанным с нею областям. Поэтому их таблицы маршрутизации содержат информацию о топологии магистрали и областей.

**access layer** Уровень доступа. Один из трех уровней иерархической модели Cisco. Уровень доступа обеспечивает пользователям доступ к объединенной сети.

**access link** Канал доступа. Канал, используемый с коммутаторами и являющийся частью лишь одной виртуальной ЛВС (VLAN). Магистральные каналы переносят данные нескольких виртуальных ЛВС.

**access list** Список доступа. Список, сохраняемый маршрутизаторами и позволяющий управлять доступом к ним со стороны ряда служб (например, для предотвращения пересылки пакетов с определенным IP-адресом через конкретный интерфейс маршрутизатора).

**access method** Метод доступа. Способ получения сетевыми устройствами доступа к сети.

**access server** Сервер доступа. Также называется "сервер доступа к сети". Процесс коммуникации, соединяющий асинхронные устройства с ЛВС или глобальной сетью посредством сетевого и эмулирующего терминала ПО. Он обеспечивает синхронную или асинхронную маршрутизацию поддерживаемых протоколов.

**acknowledgment** Уведомление, посылаемое одним сетевым устройством другому для подтверждения некоторого события (например, приема сообщения). Иногда используется сокращение АСК. *Сравните с NAK.*

**ACR (Allowed Cell Rate)** Допустимая скорость передачи ячеек. Параметр, определенный Форумом АТМ для управления сетевым трафиком. Значения допустимой скорости передачи ячеек заключены в диапазоне

от MCR до PCR. Текущая величина допустимой скорости передачи ячеек динамически устанавливается механизмом управления перегрузкой сети. *См. также MCR и PCR.*

**active monitor** Активный монитор. Механизм управления сетью Token Ring. Узел сети с самым большим MAC-адресом в кольце становится активным монитором и выполняет управляющие функции: предотвращение петель и обеспечение сохранности маркеров.

**address learning** Запоминание адреса. Используется с прозрачными мостами, чтобы узнать все аппаратные адреса всех устройств объединенной сети. Затем коммутатор фильтрует сетевые данные на основе известных аппаратных MAC-адресов.

**address mapping** Преобразование адреса. Переводя сетевые адреса из одного формата в другой, этот прием позволяет взаимодействовать разным протоколам.

**address mask** Маска адреса. Битовая комбинация, с помощью которой можно выделить части адреса, относящиеся к сети, подсети или хосту. *См. также subnet mask.*

**address resolution** Определение (разрешение) адреса. В общем случае — метод установления отличий в схемах адресации компьютеров. Под определением адреса обычно понимают метод отображения адресов сетевого уровня (адресов уровня 3) в адреса канального уровня (в адреса уровня 2). *См. также address mapping.*

**adjacency** Смежность. Отношение, устанавливаемое между выбранными соседними маршрутизаторами и конечными узлами для обмена информацией о маршрутизации. Смежность устройств означает, что они используют общий сегмент сетевого носителя.

**administrative distance** Административное расстояние. Уровень доверия к источнику информации о маршрутизации. Административное расстояние часто выражается числом от 0 до 255. Чем больше значение расстояния, тем ниже уровень доверия.

**administrative weight** Административный вес. Значение, устанавливаемое администратором сети для указания привлекательности сетевого канала связи. Это один из четырех параметров канала, которыми обмениваются PTSP для проверки доступности сетевого ресурса ATM.

**ADSU (ATMDSU)** Модуль обслуживания данных (DSU) сети ATM. Оконечный адаптер, который используется для доступа к сети ATM через устройство, совместимое с высокоскоростным последовательным интерфейсом (HSSI). *См. также DSU.*

**advertising** Оповещение. Запускаемый маршрутизатором процесс, который через определенные интервалы времени рассылает обновленную информацию о маршрутизации или услугах. Рассылка необходима для того, чтобы другие маршрутизаторы сети могли скорректировать свои списки доступных маршрутизаторов.

**AEP (AppleTalk Echo Protocol)** Протокол обмена эхо-пакетами AppleTalk. Используется для проверки соединения между двумя узлами AppleTalk. Один узел посылает пакет другому пакету и получает его дубликат.

**AFI (Authority and Format Identifier)** Идентификатор полномочий и формата. Часть адреса ATM в формате NSAP, в которой указываются тип и формат части, отведенной под идентификатор исходного домена (**IDI**) в адресе ATM.

**AFP (AppleTalk Filing Protocol)** Файловый протокол AppleTalk. Протокол уровня представлений, используя который пользователи могут работать совместно с файлами данных и с прикладными программами, хранящимися на файловом сервере. Применяется комплектами протоколов **AppleShare** и **Mac OS File Sharing**.

**AIP (ATM Interface Processor)** Интерфейсный процессор ATM. Сетевой интерфейс маршрутизаторов Cisco серии 7000, разработанный для уменьшения числа "узких мест", которые снижают производительность в интерфейсе "абонент-сеть". Интерфейсный процессор ATM поддерживает уровни **AAL3/4** и **AAL5**. См. также **AAL3/4** и **AAL5**.

**algorithm** Алгоритм. Подробное правило или процесс решения некоторой задачи. В сетевых задачах алгоритмы обычно используются для построения наилучшего пути распространения трафика от заданного источника к известному получателю.

**alignment error** Ошибка выравнивания. Ошибка в сетях Ethernet, когда полученный кадр имеет лишние разряды, т.е. число не делится на 8. Ошибки выравнивания обычно происходят из-за повреждения кадра в результате коллизий.

**all-routes explorer packet** Пакет выявления всех маршрутов. Специальный пакет, который перемещается по всем возможным путям к заданному получателю в сети, содержащей мосты с маршрутизацией от источника. Иногда называется "пакетом обследования всех колец". См. также *explorer packet*, *local explorer packet* и *spanning explorer packet*.

**AM (Amplitude Modulation)** Амплитудная модуляция. Способ модуляции, при котором информация кодируется амплитудой сигнала несущей. Сравните с **FM** и **PAM**. См. также *modulation*.

**AMI (Alternate Mark Inversion)** Чередующаяся инверсия единиц. Тип линейного кода, применяемого в каналах T1 и E1. В каждой битовой ячейке нули представляются сигналом 01, а единицы — 11 или 00. Этот способ кодирования требует, чтобы устройство-источник поддерживало плотность единиц. Отдельно от потока данных плотность единиц не поддерживается. Иногда называется "двоичным кодированием с чередующейся инверсией единиц". Сравните с **B8ZS**. См. также *ones density*.

**amplitude** Амплитуда. Максимальная величина аналогового или цифрового сигнала.

**analog transmission** Передача аналоговых сигналов. Метод передачи сигналов (проводной или беспроводной), при котором информация кодируется некоторой комбинацией амплитуды, частоты и фазы сигнала.

**ANSI (American National Standards Institute)** Национальный институт стандартизации США. Это независимая организация, членами которой являются корпорации, правительственные учреждения и другие организации. Координирует работы в области стандартизации, совершенствует стандарты США и является представителем США в международных организациях по стандартизации. Помогает создавать международные и национальные стандарты, в том числе по коммуникациям и по работе в сети. ANSI — член IEC и ISO.

**anycast** Любая рассылка. В ATM — адрес, который может одновременно принадлежать нескольким конечным системам. Может быть использован для направления запроса в узел, предоставляющий конкретную услугу.

**AppleTalk** Набор коммуникационных протоколов, разработанных компанией Apple Computer. В настоящее время существуют две версии. Начальная — Phase I — поддерживает отдельную физическую сеть, которая может иметь только один сетевой номер и представляет собой одну зону. Более поздняя версия — Phase II — поддерживает объединение нескольких логических сетей в составе одной физической сети и допускает размещение этих сетей в нескольких зонах.

**Application layer** Уровень приложений. Седьмой уровень эталонной сетевой модели OSI, предоставляющий службы процедурам приложений (таким, как электронная почта и передача файлов), находящимся за пределами модели OSI. На нем выбирается и определяется доступность участников связи, а также необходимые для соединения ресурсы, координируют взаимодействующие приложения и согласовывают процедуры контроля целостности данных и восстановления после ошибок.

**ARA (AppleTalk Remote Access)** Протокол удаленного доступа AppleTalk. Дает возможность пользователям Macintosh осуществлять непосредственный доступ к информации и ресурсам удаленного сайта AppleTalk.

**area** Область. Логическое множество сетевых сегментов (например, сегментов CLNS, DECnet или OSPF) и подключенных к ним устройств. Области обычно соединяются друг с другом через маршрутизаторы, в результате формируется отдельная автономная система. См. также *autonomous system*.

**ARM (Asynchronous Response Mode)** Асинхронный режим ответа. Режим взаимодействия по протоколу HDLC между первичной и, по крайней мере, одной вторичной станциями, причем передачу может инициировать либо первичная, либо одна из вторичных станций.

**ARP (Address Resolution Protocol)** Протокол определения адреса. Протокол Интернета, применяемый для определения MAC-адреса по заданному IP-адресу. Описан в RFC 826. Сравните с RARP. См. также проху ARP.

**ASBR (Autonomous System Boundary Router)** Граничный маршрутизатор автономной системы. Располагается между автономной системой OSPF и сетью, в которой не поддерживается протокол OSPF. В граничном маршрутизаторе одновременно выполняются протокол OSPF и другой протокол маршрутизации, например RIP. Граничный маршрутизатор должен размещаться в нетупиковой области OSPF. *См. также ABR, non-stub area и OSPF.*

**ASCII (American Standard Code for Information Interchange)** Американский национальный стандартный код для обмена информацией. Представление символов 8-битовыми кодовыми комбинациями (7 бит кода и 1 бит контроля четности).

**ASICs (Application-Specific Integrated Circuits)** Специализированные интегральные схемы. Служат для фильтрации в коммутаторах второго уровня. Схема ASIC просматривает фильтрационную таблицу MAC-адресов и определяет, для какого порта предусмотрен аппаратный адрес назначения полученного аппаратного адреса. Кадру будет разрешено пересечь только этот участок. Если аппаратный адрес неизвестен, кадр рассылается всем портам.

**ASN.1 (Abstract Syntax Notation One)** Первая абстрактная синтаксическая нотация. Нотация OSI для описания типов данных без привязки к структуре конкретного компьютера и к способам представления данных. Определен стандартом ISO 8824. *См. также BER(2).*

**ASP (AppleTalk Session Protocol)** Протокол сеансового уровня AppleTalk. Взаимодействует с протоколом ATP. Используется для **установления**, поддержки и завершения соединения, а также для упорядочения запросов. *См. также ATP.*

**AST (Automatic Spanning Tree)** Автоматическое построение покрывающего дерева. Функция, поддерживающая автоматическое создание покрывающих деревьев в сетях, содержащих мосты с маршрутизацией от источника. Выполняется корректно, если между заданными сетевыми узлами существует хотя бы один путь для распространения кадров определения покрытия. Функция описана в стандарте IEEE 802.1. *См. также IEEE 802.1 и SRB.*

**asynchronous transmission** Асинхронная передача. Термин, описывающий передачу цифровых сигналов без **синхронизации**. Такие сигналы обладают различными частотами и фазами. Обычно при асинхронной передаче отдельные символы обрамляются управляющими битами (называемыми "стартовым" и "стоповым"), отмечающими начало и конец каждого символа. *Сравните с isochronous transmission, plesiochronous transmission и synchronous transmission.*

**ATCP (AppleTalk Control Protocol)** Управляющий протокол AppleTalk. Протокол установления и конфигурирования соединений AppleTalk в сетях PPP, как определено в RFC 1378. *См. также PPP.*

**ATDM (Asynchronous Time-Division Multiplexing)** Асинхронное мультиплексирование с разделением времени. Метод передачи информации, напоминающий обычное мультиплексирование с разделением времени. Отличие в том, что временные интервалы распределяются по мере необходимости, а не приписываются заранее определенным передатчикам. *Сравните с FDM, statistical multiplexing и TDM.*

**ATG (Address Translation Gateway)** Шлюз преобразования адреса. Программная функция Cisco для маршрутизации в сетях DECnet, с помощью которой маршрутизатор находит пути в различные независимые сети DECnet и производит определенное пользователем преобразование адресов для выбранных узлов между сетями.

**ATM (Asynchronous Transfer Mode)** Режим асинхронной передачи. Международный стандарт ретрансляции ячеек, согласно которому различные типы данных (например, аудио-, видео- или цифровые данные) передаются в ячейках фиксированной длины (53 байт). Применение фиксированной длины позволяет сосредоточить обработку ячеек на аппаратном уровне, что сокращает задержки передачи. Режим ATM разработан для реального использования высокой производительности носителей сетей E3, SONET и T3.

**ATM ARP server** Сервер ARP сети ATM. Устройство, обеспечивающее возможность определения адресов в логических подсетях IP при передаче данных протокола IP по сетям ATM.

**ATM endpoint** Конечная точка ATM. Точка сети ATM, в которой инициируется или завершается соединение ATM. Это рабочие станции и серверы, подключенные к сети ATM, коммутаторы и маршрутизаторы ATM.

**ATM Forum** Форум ATM. Международная организация, созданная в 1991 г. компаниями Cisco Systems, NET/ADAPTIVE, Northern Telecom и Sprint для разработки и распространения стандартизированных соглашений по реализации технологии ATM. Развивает официальные стандарты, созданные ANSI и ITU-T, и определяет соглашения по реализации до введения официальных стандартов.

**ATM layer** Уровень ATM. Подуровень канального уровня в сетях ATM, не зависящий от предоставляемых услуг. На уровне ATM к поступающим с уровня адаптации AAL 48-байтовым сегментам полезной нагрузки присоединяются 5-байтовые заголовки, в результате чего создаются стандартные ячейки ATM. Эти ячейки передаются на физический уровень для пересылки по физическому носителю. *См. также AAL.*

**ATMM (ATM management)** Управление ATM. Процесс, выполняемый на коммутаторе ATM для управления идентификаторами виртуальных каналов (VCI) и для повышения скорости передачи. *См. также ATM.*

**ATM user-user connection** Соединение между пользователями ATM. Создается на уровне ATM для обеспечения взаимодействия двух или нескольких пользователей-потребителей услуг ATM (например, для

взаимодействия процессов АТММ). Подобное взаимодействие может быть однонаправленным с использованием одного соединения виртуальных каналов (VCC) или двунаправленным с использованием двух соединений виртуальных каналов. См. также *ATM layer, АТММ*.

**АТР (AppleTalk Transaction Protocol)** Протокол транзакций AppleTalk. Протокол транспортного уровня, обеспечивающий выполнение транзакций между сокетами без потерь данных. Позволяет вести обмен между сокетами двух клиентов, один из которых посылает запрос другому на выполнение определенного задания и возврат результатов. АТР производит связывание запроса и ответа, чтобы гарантировать надежность обмена парами запрос-ответ.

**attenuation** Затухание. Уменьшение мощности сигнала.

**AURP (AppleTalk Update-Based Routing Protocol)** Протокол маршрутизации AppleTalk с рассылкой изменений. Метод инкапсуляции трафика AppleTalk в заголовок другого протокола, позволяющий соединить несколько разрозненных сетей AppleTalk через сеть другого типа (например, через сеть TCP/IP) и сформировать глобальную сеть AppleTalk. Подобное соединение называется "туннелем" AURP. Кроме инкапсуляции данных, протокол AURP поддерживает таблицы маршрутизации для всей глобальной сети AppleTalk за счет обмена информацией о маршрутизации между внешними маршрутизаторами. См. также *AURP tunnel u exterior router*.

**AURP tunnel** Туннель протокола AURP. Соединение, создаваемое в глобальной сети AURP и функционирующее как единый виртуальный канал передачи данных между сетями AppleTalk, физически разделенными сетью другого типа (например, сетью TCP/IP). См. также *AURP*.

**authority zone** Зона полномочий. Понятие, относящееся к системе именования доменов (DNS). Зона полномочий является частью дерева имен доменов, для именования доменов которой выбран уполномоченный сервер. См. также *DNS*.

**auto duplex** Параметр на устройствах первого и второго уровней, устанавливающий дуплекс коммутатора или порта концентратора автоматически.

**automatic call reconnect** Автоматическое восстановление связи (вызова). Свойство автоматического восстановления связи за счет обхода поврежденной линии связи.

**autonomous confederation** Автономная конфедерация. Группа самостоятельных систем, которые доверяют информации о достижимости и маршрутизации, распространяемой по их собственной сети, больше, чем подобной информации, получаемой от других автономных систем или конфедераций.

**autonomous switching** Автономная коммутация. Свойство маршрутизаторов Cisco, заключающееся в обеспечении более высокой скорости обработки пакетов за счет использования ciscoBus для независимой коммутации пакетов без прерывания работы процессора.

**autonomous system (AS)** Автономная система. Группа сетей с общим управлением и одинаковой технологией маршрутизации. Автономные системы подразделяются на области и должны иметь назначенный индивидуальный 16-битный номер организации IANA. См. также *area (область)*.

**autoreconfiguration** Автоматическая перенастройка. Процесс, выполняемый узлами, принадлежащими области неисправности в сетях Token Ring. Узлы автоматически производят диагностику, пытаются реконфигурировать сеть вокруг области неисправности.

**auxiliary port** Вспомогательный порт. Консольный порт на задней панели маршрутизаторов Cisco, позволяющий подключаться к маршрутизатору и производить настройку параметров консоли.

**B8ZS (Binary 8-Zero Substitution)** Двоичная 8-нулевая подстановка. Тип линейного кода, используемого в линиях E1 и T1, где вместо того, чтобы передавать по каналу связи восемь последовательных нулевых сигналов, производится подстановка специального кода. Этот код распознается на удаленном конце соединения. Метод B8ZS обеспечивает независимость плотности единиц от потока данных. Иногда называется "биполярной 8-нулевой подстановкой". Сравните с AMI. См. также *ones density*.

**backbone** Объединяющая магистраль. Часть сети, действующая как основной путь передачи трафика, исходящего из другой сети или направляемого в нее.

**back end** Прикладная часть. Узел или программное обеспечение, предоставляющее услуги интерфейсной части. См. *server*.

**bandwidth** Полоса пропускания. Разность между максимальным и минимальным значениями частоты, на которой можно передавать сигналы по сети. Этот термин используется также для описания номинальной пропускной способности сетевого носителя или протокола.

**baseband** Немодулированная передача в основной полосе частот. Характеристика сетевой технологии, допускающей передачу сигналов с помощью несущей одной частоты. Примером являются сети Ethernet. Также называется "узкополосной передачей". Противоположна broadband.

**Basic Management Setup** Установка с базовым управлением. Применяется на маршрутизаторах Cisco, находящихся в режиме настройки. Предоставляет возможности управления и настройки, достаточные только для того, чтобы привести маршрутизатор в рабочее состояние, чтобы кто-то еще мог посылать маршрутизатору сигналы Telnet и настраивать его.

**baud** Бод. То же самое, что и параметр битов в секунду (бит/с), если каждый сигнальный элемент представляет один бит. Это единица

скорости передачи сигналов, равная количеству отдельных сигнальных элементов, переданных в секунду.

**B channel** В-канал. Bearer channel (канал-носитель) — полнодуплексный канал на 64 Кбит/с в сети ISDN, передающий пользовательские данные. См. также *D channel (D-канал)*, *E channel (E-канал)*, *H channel (H-канал)*.

**beacon** Кадр аварийной сигнализации (маячок). Посылается устройством сети Token Ring или FDDI и указывает на наличие в кольце серьезной неисправности, например обрыва кабеля. Содержит адрес предполагаемой неисправной станции. См. также *failure domain*.

**BECN (Backward Explicit Congestion Notification)** Явное предупреждение о перегрузке. В сетях Frame Relay — установка в 1 соответствующего бита кадров, которые перемещаются в направлении, обратном пути передачи кадров, столкнувшихся с перегрузкой пути. Устройство DTE, принимающее кадры с установленным битом BECN, может послать запрос протоколом более высоких уровней на выполнение необходимых действий по управлению потоком данных. Сравните с *FECN*.

**BGP4 (BGP Version 4)** Протокол BGP версии 4. Четвертая версия самого распространенного в Интернете протокола междоменной маршрутизации. Поддерживает бесклассовую междоменную маршрутизацию (CIDR) и использует механизмы объединения маршрутов для сокращения таблиц маршрутизации. См. также *CIDR*.

**binary** Двоичная система счисления. Используются две цифры — 0 и 1.

**BIP (Bit Interleaved Parity)** Четность с чередованием битов. В ATM - метод выявления ошибок, вносимых в данные в канале связи. В дополнение к переданному блоку или кадру по каналу связи посылается контрольный бит или слово, анализ которого позволяет обнаруживать ошибки в полезной нагрузке и создавать необходимые информационные сообщения.

**BISDN (Broadband ISDN)** Широкополосная сеть ISDN. Коммуникационный стандарт ITU-T, разработанный для приложений, которым требуется большая полоса пропускания (например, приложения обработки видеоданных). В настоящее время в сетях BISDN используется технология ATM для передачи по линиям SONET, что позволяет пересылать данные со скоростью от 155 до 622 Мбит/с и более. Противоположна *N-ISDN*. См. также *BRI, ISDN и PRI*.

**bit-oriented protocol** Протокол побитовой передачи данных. Класс протоколов канального уровня для передачи кадров независимо от их содержимого. Эти протоколы обеспечивают полнодуплексную передачу и являются более эффективными и надежными по сравнению с протоколами побайтовой передачи данных. Сравните с *byte-oriented protocol*.

**Boot ROM** Загрузочное ПЗУ. В маршрутизаторах переводит их в режим самозагрузки. Режим самозагрузки, в свою очередь, загружает на устройстве операционную систему. ПЗУ может также содержать небольшую ОС Cisco IOS.

**border gateway** Граничный шлюз. Маршрутизатор, взаимодействующий с маршрутизаторами из других автономных систем.

**BPDU (Bridge Protocol Data Unit)** Протокольный блок данных моста. Пакеты приветствия протокола покрывающего дерева, рассылаемые мостами через выбранные интервалы времени в качестве оповещений об их присутствии в сети.

**BRI (Basic Rate Interface)** Интерфейс передачи данных с номинальной скоростью (интерфейс базового уровня). Интерфейс ISDN, состоящий из двух В-каналов и одного D-канала и позволяющий передавать видео-, аудио- и цифровые данные по соединениям с коммутацией каналов. Сравните с PRI. См. также *BISDN*.

**bridge** Мост. Устройство, соединяющее два сетевых сегмента с одинаковыми протоколами и пересылающее пакеты между этими сегментами. Мосты функционируют на канальном уровне (уровне 2) базовой модели OSI. Они фильтруют поступающие кадры или передают их через конкретный или через все интерфейсы по результатам анализа MAC-адреса кадра.

**broadband** Широкополосная передача. Характеризует системы, передающие мультиплексированные независимые сигналы по одному кабелю. В телекоммуникациях — это любой канал, имеющий полосу пропускания шире, чем звуковой канал (4 КГц). В локальных сетях — коаксиальный кабель, по которому передаются аналоговые сигналы. Противоположна *baseband*.

**broadcast** Широковещательная передача. Кадр или пакет с данными, передаваемый каждому узлу на локальном участке сети (по определению широковещательного домена). Широковещательные рассылки узнаются по широковещательному адресу, который является сетью назначения и адресом узла, где все биты включены. Другое название — "local broadcast" ("локальное широковещание"). Сравните с *directed broadcast*.

**broadcast domain** Домен широковещательной рассылки. Совокупность устройств, которые получают широковещательные кадры, переданные одним из устройств этой совокупности. Область широковещательной рассылки обычно ограничена маршрутизаторами, поскольку они не передают широковещательные кадры.

**broadcast storm** Широковещательный шторм. Нежелательное явление, при котором по всем сетевым сегментам одновременно рассылаются многочисленные широковещательные сообщения. Широковещательный шторм занимает существенную долю полосы пропускания сети и обычно приводит к тайм-аутам.

**buffer** Буфер. Область памяти, используемая для промежуточного хранения данных. При работе в объединенных сетях позволяет компенсировать различие скоростей разных сетевых устройств. Пакеты данных могут сохраняться в буфере до тех пор, пока более медленное устройство не приступит к их обработке. Иногда называется "буфером для хранения пакетов".

**bus topology** Шинная топология. Линейная архитектура локальной сети, в которой данные, передаваемые сетевыми станциями, распространяются по протяженному носителю и принимаются всеми другими станциями. *Сравните с ring topology и star topology.*

**bus** Шина. Любой физический путь, обычно провод или медный кабель, по которому с помощью цифрового сигнала могут посылаться данные от одной части компьютера к другой.

**BUS (broadcast and unknown servers)** Серверы широковещательных и неизвестных сообщений. В эмуляции ЛВС аппаратное или программное средство, отвечающее за преобразование всех широковещательных сообщений и пакетов с неизвестными (незарегистрированными) адресами в двухточечные виртуальные каналы, которые требуются для ATM. *См. также LANE, LEC, LECS и LES.*

**BX.25** Реализация X.25, выполненная компанией AT&T. *См. также X.25.*

**bypass mode** Режим обхода. Режим функционирования сетей FDDI и Token Ring после удаления из кольца некоторого интерфейса.

**bypass relay** Передача в обход. Разрешение на отключение конкретного интерфейса Token Ring и удаление его из кольца без нарушения работы сети.

**byte-oriented protocol** Протокол побайтовой передачи данных. Класс протоколов канального уровня, в которых для разграничения кадров используется определенный символ из пользовательского набора символов. Эти протоколы в значительной мере заменены протоколами побитовой передачи данных. *Сравните с bit-oriented protocol.*

**cable range** Кабельный диапазон. Диапазон сетевых номеров, используемых узлами расширенной сети AppleTalk. Значением кабельного диапазона может быть единственный сетевой номер или последовательность сетевых номеров. Адреса узлов назначаются в соответствии со значением кабельного диапазона.

**CAC (Connection Admission Control)** Управление разрешением соединения. Совокупность действий, предпринимаемых каждым коммутатором ATM во время установки соединения с целью определения, согласуется ли качество обслуживания (QoS) запроса на соединение с необходимостью гарантированного установления соединения. Также используется при маршрутизации запроса на соединение через сеть ATM.

**call admission control** Управление разрешением вызова. Механизм управления трафиком в сетях ATM, с помощью которого определяется, можно ли найти в сети путь с достаточной полосой пропускания для запрошенного соединения виртуальных каналов.

**call priority** Приоритет вызова. Назначается каждому передающему порту в системах с коммутацией каналов. Определяет порядок восстановления

вызовов, а также возможность (или невозможность) предоставления вызову зарезервированной полосы пропускания.

**call setup time** Время установки вызова. Время, необходимое для установления коммутируемого вызова между устройствами DTE.

**CBR (Constant Bit Rate)** Постоянная скорость передачи двоичных данных. Класс QoS, определенный Форумом ATM для сетей ATM. Применяется в соединениях, когда для обеспечения неискаженной доставки данных существенна точность синхронизации. *Сравните с ABR и VBR.*

**CD (Carrier Detect)** Обнаружение несущей. Сигнал, указывающий на активность интерфейса. Кроме того, сигнал, создаваемый модемом для указания, что соединение установлено.

**CDP (Cisco Discovery Protocol)** Протокол обнаружения устройств Cisco. Служит для сообщения соседнему устройству Cisco о типе аппаратного оборудования, версии программного обеспечения и активных интерфейсах, которые использует устройство Cisco. Основан на типе инкапсуляции SNAP и не маршрутизируется.

**CDVT (Cell Delay Variation Tolerance)** Устойчивость к изменениям задержки ячеек. Параметр, определенный Форумом ATM для управления трафиком ATM. При передаче данных с постоянной скоростью (CBR) определяет допустимый уровень дрожания при приеме ячеек с предельной скоростью (PCR). *См. также CBR и PCR.*

**cell** Ячейка. Основной блок данных при коммутации и мультиплексировании в сетях ATM. Каждая ячейка содержит идентификатор, определяющий поток данных, которому принадлежит ячейка. Состоит из 5-байтовой заголовка и 48-байтовой полезной нагрузки. *См. также cell relay.*

**cell payload scrambling** Кодирование полезной нагрузки ячейки. Метод, используемый в коммутаторах ATM для создания кадров в некоторых среднескоростных интерфейсах конечных устройств и в магистральных каналах.

**cell relay** Поячейковая передача. Технология, использующая небольшие пакеты фиксированного размера, которые называются ячейками. Фиксированная длина позволяет обрабатывать и коммутировать ячейки в аппаратных средствах с высокой скоростью. Благодаря этому, технология лежит в основе ATM и других высокоскоростных сетевых протоколов. *См. также cell.*

**Centrex** Служба местной телефонной компании, обеспечивающая локальную коммутацию, подобно тому, как это делает офисная АТС. Однако в Centrex отсутствуют средства локальной коммутации, и все соединения абонента возвращаются на центральный телефонный узел. *См. также CO.*

**CER (Cell Error Ratio)** Доля ячеек с ошибками. В ATM — отношение числа ячеек, содержащих ошибки, к общему числу ячеек, переданных за определенный промежуток времени.

**channelized E1** Сеть E1 с разделением каналов. Работающий на скорости 2.048 Мбит/с канал доступа, разделенный на 29 В-каналов и 1 D-канал. Поддерживает DDR, Frame Relay и X.25. *Сравните с channelized T1.*

**channelized T1** Сеть T1 с разделением каналов. Работающий на скорости 1.554 Мбит/с канал доступа, разделенный на 23 В-каналов и 1 D-канал, каждый на 64 Кбит/с, где отдельные каналы или группы каналов соединяются с разными точками назначения. Поддерживает DDR, Frame Relay и X.25. *Сравните с channelized E1.*

**CHAP (Challenge Handshake Authentication Protocol)** Протокол аутентификации по вызову с подтверждением. Средство обеспечения защиты линий с применением инкапсуляции данных протокола PPP для предотвращения несанкционированного доступа. Протокол CHAP не препятствует несанкционированному доступу, а лишь идентифицирует удаленный узел. Проверка наличия права доступа у пользователя осуществляется маршрутизатором или сервером доступа. *Сравните с PAP.*

**checksum** Проверка контрольной суммы. Способ проверки целостности передаваемых данных. Контрольная сумма является целым числом, получаемым после применения ряда арифметических операций к последовательности октетов данных. Вычисляется заново принимающей стороной и сравнивается со значением, переданным источником данных. *Сравните с CRC.*

**choke packet** Пакет с сообщением о перегрузке. Посылается передатчику, чтобы сообщить ему о возникновении перегрузки и необходимости уменьшения скорости передачи данных.

**CIDR (Classless Interdomain Routing)** Бесклассовая междоменная маршрутизация. Реализуемый протоколом BGP4 алгоритм маршрутизации, основанный на объединении маршрутов. Маршрутизаторы получают возможность группировать маршруты с целью сокращения объема информации о маршрутизации, пересылаемой маршрутизаторами ядра. При этом совокупность IP-сетей, по которым проходят сгруппированные маршруты, для остальных сетей выглядит как единый, очень большой объект. Для применения в CIDR IP-адреса и маски подсетей представляются в виде 4-октетного числа с разделительными точками, за которым следуют символ "/" (слэш) и двухразрядный номер, представляющий маску подсети. *См. также BGP4.*

**CIP (Channel Interface Processor)** Интерфейсный процессор канала. Интерфейс подключения к каналу в маршрутизаторах Cisco серии 7000. Используется для соединения большой ЭВМ с управляющим устройством, что позволяет обойтись без периферийного процессора (FEP) при подключении к каналу.

**CIR (Committed Information Rate)** Согласованная скорость передачи информации. Усредненная по небольшим интервалам времени скорость, с которой сеть Frame Relay согласна передавать информацию при

нормальных условиях функционирования. Измеряемая в бит/с, является одной из ключевых метрик согласованного тарифа.

**circuit switching** Коммутация каналов. Используется в таких коммуникационных сетях, как PPP и ISDN. Передает данные, но требует предварительной установки соединения, как при телефонном звонке.

**Cisco FRAD (Cisco Frame Relay Access Device)** Устройство доступа к сети Frame Relay компании Cisco. Продукт компании Cisco, который поддерживает службы SNA в сетях Frame Relay с помощью Cisco IOS и может быть модифицирован до многопротокольного маршрутизатора с полным набором функций. Cisco FRAD соединяет устройства сети SDLC с сетью Frame Relay, не требуя промежуточной локальной сети. Однако Cisco FRAD должен поддерживать подключенные локальные сети и может стыковать сеть SDLC с Ethernet и Token Ring. См. также FRAD.

**CiscoFusion** Название Cisco для архитектуры межсетевого обмена, в которой действует программное обеспечение Cisco IOS. Служит для объединения возможностей разнородных маршрутизаторов и коммутаторов.

**Cisco IOS software (Cisco Internetwork Operating System software)** Программное обеспечение межсетевого операционной системы Cisco. Системное программное обеспечение компании Cisco, обеспечивающее выполнение общих функций, расширяемость и безопасность для всех продуктов, создаваемых в рамках архитектуры CiscoFusion. Позволяет выполнять централизованную, интегрированную и автоматизированную установку и обслуживание объединенных сетей, гарантируя поддержку широкого набора протоколов, носителей, служб и платформ. См. также CiscoFusion.

**CiscoView** Прикладное программное обеспечение для управления устройствами с графическим пользовательским интерфейсом, позволяющее динамически управлять состоянием, собирать статистические данные и получать исчерпывающую информацию о конфигурации устройств Cisco, действующих в составе объединенной сети. Кроме вывода на экран изображений устройств Cisco, CiscoView имеет функции мониторинга устройств и основные средства поиска неисправностей и может быть объединено с некоторыми основными платформами управления сетью на основе протокола SNMP.

**Class A network** Сеть класса А. Компонент системы адресации протокола Интернета. Сети класса А имеют 16 бит для определения сетей и 16 бит для определения узлов в каждой сети.

**Class B network** Сеть класса В. Компонент системы адресации протокола Интернета. Сети класса В имеют 16 бит для определения сетей и всего 8 бит для определения узлов в каждой сети.

**Class C network** Сеть класса С. Компонент системы адресации протокола Интернета. Сети класса С имеют 24 бита для определения сетей и всего 8 бит для определения узлов в каждой сети.

**classical IP over ATM** Передача IP по сетям ATM. Спецификация для передачи данных протокола IP по сетям ATM с использованием всех достоинств сетей ATM. Описан в RFC 1577. Иногда обозначается как CIA.

**Classless routing** Бесклассовая маршрутизация. Маршрутизация, в которой сведения о маске подсети посылаются в обновлениях по маршрутизации. Бесклассовая маршрутизация поддерживает VLSM (маску подсети переменной длины) и суперсетевой обмен. Бесклассовую маршрутизацию поддерживают протоколы RIP версии 2, EIGRP и OSPF.

**CLI (Command Line Interface)** Интерфейс командной строки. Позволяет настраивать маршрутизаторы и коммутаторы Cisco с максимальной гибкостью.

**CLP (Cell Loss Priority)** Приоритет потери ячейки. Поле заголовка ячейки ATM, в котором определяется вероятность отбрасывания ячейки при перегрузке сети. Если бит CLP равен 0, ячейка относится к гарантированному трафику (insured traffic) и, скорее всего, не будет отброшена. Если бит CLP установлен в 1, ячейка относится к трафику, доставляемому по возможности (best-effort traffic), и может быть отброшена при перегрузке, чтобы освободить ресурсы для обработки гарантированного трафика.

**CLR (Cell Loss Ratio)** Коэффициент потери ячеек. В ATM — отношение числа отброшенных ячеек к числу успешно переданных ячеек. Величина коэффициента потери ячеек может быть задана как параметр качества обслуживания (QoS) при установлении соединения.

**CO (Central Office)** Центральный телефонный узел (офис). Центральный телефонный узел локальной телефонной компании, с которым соединяются все местные линии связи из заданной области и в котором размещается оборудование коммутации абонентских линий.

**collapsed backbone** Локализованная магистраль. Выступающая в роли единого устройства нераспределенная магистраль, связывающая все сетевые сегменты. Локализованной магистралью можно было бы назвать виртуальный сетевой сегмент, существующий внутри устройства, например концентратора, маршрутизатора или переключателя.

**collision** Конфликт. В сетях Ethernet — результат одновременного выполнения передачи данных двумя узлами. При столкновении в физическом носителе кадры, посланные разными устройствами, искажаются. См. также *collision domain*.

**collision domain** Область конфликтов. В сетях Ethernet — область, в которой распространяются кадры, вызывающие конфликты. Конфликты распространяются повторителями и концентраторами; переключатели локальной сети, мосты и маршрутизаторы ограничивают распространение конфликтов. См. также *collision*.

**composite metric** Составная метрика. Такие протоколы, как IGRP и EIGRP, используют несколько метрик для поиска оптимального пути к удаленной сети. И IGRP и EIGRP по умолчанию используют атрибуты полосы пропускания и задержки канала. Однако могут применяться и параметры максимальной единицы передачи, нагрузки и надежности канала.

**configuration register** Регистр конфигурации. В маршрутизаторах Cisco - задаваемое пользователем 16-битовое значение, определяющее функционирование маршрутизатора во время его инициализации. Содержимое регистра конфигурации может быть сохранено аппаратно или программно. При аппаратном сохранении значение каждого бита устанавливается с помощью переключателей. Для программного сохранения используются команды конфигурирования.

**congestion** Перегрузка. Объем трафика, превышающий возможности сети.

**congestion avoidance** Предотвращение перегрузки. Механизм, с помощью которого сеть ATM управляет трафиком, входящим в сеть, и минимизирует его задержку. Для более эффективного использования ресурсов низкоприоритетный трафик отбрасывается на границе (edge) сети, если при существующих условиях он не может быть доставлен.

**congestion collapse** Коллапс перегрузки. Условие, при котором повторная передача кадров в сети ATM приводит к тому, что к получателю доставляется либо небольшая часть трафика, либо трафик вообще не достигает получателя. Коллапс перегрузки часто возникает в сетях ATM с коммутаторами, не имеющими адекватных и эффективных механизмов буферизации с разумным отбрасыванием пакетов или механизмов снижения перегрузки за счет правильного выбора доступной скорости передачи двоичных данных (ABR).

**connection ID** Код соединения. Идентификаторы, которые даются каждому сеансу Telnet при подключении к маршрутизатору. Команда show sessions показывает соединения локального маршрутизатора с удаленным. Команда show users показывает коды соединений пользователей, подключившихся через Telnet к данному локальному маршрутизатору.

**connectionless** Без установления соединения. Термин, используемый для описания передачи данных без образования виртуального канала. *Сравните с connection-oriented. См. также virtual circuit.*

**connection-oriented** Ориентированный на установление соединения. Термин, используемый для описания передачи данных, требующей установления виртуального канала. *См. также connectionless и virtual circuit.*

**console port** Консольный порт. Как правило, порт RJ-45 на маршрутизаторе и коммутаторе Cisco, обеспечивающий функцию интерфейса командной строки.

**control direct VCC** Прямое соединение виртуальных каналов для управления. В ATM — двунаправленное соединение виртуальных каналов, установленное клиентом LANE с сервером LANE. Одно из трех управляющих соединений, определенных стандартом Phase 1 LANE. *Сравните с configuration direct VCC и control distribute VCC.*

**control distribute VCC** Распределенное соединение виртуальных каналов для управления. В ATM — однонаправленное соединение виртуальных каналов, установленное сервером LANE с клиентом LANE. Одно из трех управляющих соединений, определенных стандартом Phase 1 LANE. Обычно соединение виртуальных каналов является многоточечным (point-to-multipoint). *Сравните с configuration direct VCC и control direct VCC.*

**convergence** Сходимость. Скорость и способность группы устройств объединенной сети в рамках определенного протокола маршрутизации согласовывать свои базы топологических данных после изменения топологии объединенной сети.

**core layer (уровень ядра)** Верхний уровень в трехуровневой иерархической модели Cisco, который помогает проектировать, создавать и обслуживать иерархические сети Cisco. Уровень ядра быстро передает пакеты только устройствам уровня распределения. На этом уровне не должна происходить фильтрация пакетов.

**cost** Стоимость. Произвольное значение, обычно связанное с числом переходов, величиной полосы пропускания и другими характеристиками, назначаемое администратором сети путям через объединенную сеть и используемое затем для сравнения путей. Значения стоимости используются протоколами маршрутизации для выбора наиболее привлекательного пути к конкретному получателю: чем меньше стоимость, тем лучше путь. Иногда называется "стоимостью пути". См. также routing metric.

**count to infinity** Счет до бесконечности. Проблема, свойственная медленно сходящимся алгоритмам маршрутизации, в которых маршрутизаторы постоянно наращивают число переходов до конкретной сети. Обычно для предотвращения этой проблемы устанавливается предельное значение счетчика числа переходов.

**CPCS (Common Part Convergence Sublayer)** Подуровень сходимости унифицированных компонентов. Один из трех подуровней AAL, который является зависимым от службы. Подразделяется далее на подуровни CS и SAR. Уровень CPCS подготавливает данные к передаче по сети ATM, он формирует 48-байтовые ячейки, которые посылаются на уровень ATM. *См. также AAL и ATM layer.*

**CPE (Customer Premises Equipment)** Оборудование, устанавливаемое на территории абонента. Оконечное оборудование, например терминалы, телефоны или модемы, поставляемое телефонной компанией, устанавливаемое на сайтах абонентов и подключаемое к сети телефонной компании.

**crankback В АТМ** — метод отладки, применяемый, когда узел на выбранном маршруте не может принять запрос на установку соединения и запрос блокируется. Путь возвращается к промежуточному узлу, который затем применяет метод управления разрешением на соединение GCAC, чтобы попытаться найти альтернативный путь к месту назначения.

**CRC (Cyclic Redundancy Check)** Проверка при помощи циклически избыточного кода. Метод выявления ошибок, когда получатель кадра производит вычисление, деля содержание кадра простым двоичным делителем, и сравнивает остаток со значением, сохраненным в кадре посылающим узлом. *Сравните с: checksum (проверка контрольной суммы).*

**CSMA/CD (Carrier Sense Multiple Access with Collision Detect)** Множественный доступ с прослушиванием несущей и с обнаружением конфликтов. Механизм доступа к носителю, при котором устройства, готовые передавать данные, сначала проверяют наличие в канале сигнала несущей. Если в течение некоторого периода времени сигнал несущей отсутствует, устройство может приступить к передаче. Если два устройства начинают передачу одновременно, возникает конфликт, обнаруживаемый всеми вовлеченными в конфликт устройствами. Начало повторной передачи каждого из этих устройств задерживается на период случайной длительности.

**CSU (Channel Service Unit)** Устройство обслуживания канала. Цифровое интерфейсное устройство, соединяющее оборудование конечного пользователя с местной цифровой телефонной линией. Часто рассматривается как часть комбинации CSU/DSU. См. также DSU.

**CTD (Cell Transfer Delay)** Задержка передачи ячейки. В АТМ — время, прошедшее с момента отправки ячейки источником UNI до момента поступления ячейки получателю UNI по конкретному соединению. Задержка передачи ячейки между двумя точками складывается из полной задержки перемещения ячейки между узлами АТМ и полной задержки, связанной с обработкой ячейки в узле АТМ.

**cut-through frame switching** Коммутация кадров в ускоренном режиме. Метод коммутации кадров, пропускающий данные через коммутатор, так чтобы передняя часть выходила из маршрутизатора до того, как пакет закончит поступление в порт входа. Кадры считываются, обрабатываются и пересылаются устройствами, которые используют ускоренную коммутацию, как только подтверждается адрес назначения кадра и определяется исходящий порт.

**data direct VCC** Прямое соединение виртуальных каналов для передачи данных. В АТМ — двунаправленное двухточечное соединение виртуальных каналов, устанавливаемое между двумя клиентами LANE (LEC). Одно из трех соединений для передачи данных, определенных стандартом Phase 1 LANE. Не предоставляет никаких гарантий качества обслуживания, поэтому обычно используется для соединений с неопределенной (UBR) и доступной (ABR) скоростями передачи двоичных данных. *Сравните с control distribute VCC и control direct VCC.*

**data frame** Кадр данных. Инкапсуляция протокольного модуля данных на канальном уровне эталонной модели OSI. Инкапсулирует пакеты сетевого уровня и подготавливает данные к передаче по сетевому носителю.

**datagram** Датаграмма. Логически сгруппированная информация, посылаемая как блок данных сетевого уровня без предварительного установления виртуального канала. **IP-датаграммы** являются основными информационными блоками в Интернете. Для описания логических групп информации различных уровней базовой модели OSI и технологических циклов **используются** также термины "ячейка", "кадр", "сообщение", "пакет" и "сегмент",

**Data link control layer** Уровень управления каналом. Уровень 2-й архитектурной модели SNA, **отвечающий** за передачу информации по данному физическому каналу и несколько похожий на канальный уровень модели OSI.

**Data Link layer** Канальный уровень (уровень связи данных). Уровень 2 базовой модели OSI, обеспечивающий надежную передачу данных по физическому каналу. На этом уровне анализируются физические адреса, сетевая топология, устанавливается дисциплина передачи данных по каналу, выявляются ошибки, организуется упорядоченная доставка данных и производится управление потоком данных. Стандартом IEEE канальный уровень разделен на подуровень управления доступом к носителю (MAC) и подуровень управления логическим каналом (LLC). Примерно соответствует уровню управления каналом архитектуры SNA. *См. также Application layer, LLC, MAC, Network layer, Physical layer, Presentation layer, Session layer и Transport layer.*

**DCC (Data Country Code)** Код страны данных. Один из двух форматов адреса ATM, созданных Форумом ATM для применения в частных сетях. Заимствован из модели адресации подсетей, в которой отображение адресов сетевого уровня в адреса ATM производится на уровне ATM. *Сравните с ICD.*

**DCE (Data Communications Equipment (термин EIA) или Data Circuit-terminating Equipment (термин ITU-T))** Оборудование передачи данных (термин EIA) или оборудование терминирования цепей передачи данных (термин ITU-T). Сетевые устройства и соединения, подключаемые на стороне сети к интерфейсу "пользователь-сеть". Оборудование DCE обеспечивает физическую связь с сетью, передачу трафика и генерацию сигналов, синхронизирующих передачу данных между устройствами DCE и DTE. Примеры устройств DCE — модемы и сетевые интерфейсные платы. *Сравните с DTE.*

**D channel 1.** Bata channel. D-канал, канал данных. Полнодуплексный канал ISBN для передачи данных со скоростью 16 (BRI) или 64 Кбит/с (PRI). *Сравните с B channel, E channel и H channel.* 2. В SNA — устройство, соединяющее процессор и основное ОЗУ с периферийными устройствами.

**DDP (Datagram Delivery Protocol)** Протокол доставки датаграмм. Протокол сетевого уровня AppleTalk, ответственный за доставку датаграмм между сокетами в объединенной сети AppleTalk.

**DDR (Dial-on-Demand Routing)** Маршрутизация вызовов по запросу. Метод маршрутизации, при котором маршрутизатор может автоматически инициировать и закрывать сеанс коммутации каналов по запросу передающих станций. Подмена маршрутизатора выполняется так, чтобы конечные станции считали сеанс активным. Допускает маршрутизацию через сети ISDN или телефонные сети с использованием внешнего терминального адаптера ISDN или модема.

**DE (Discard Eligibility)** Доступность для отбрасывания. Указывает в сетях Frame Relay коммутатору, что кадр может быть отброшен, если коммутатор очень загружен. DE — это поле в кадре, которое задействуется передающими маршрутизаторами, если согласованная скорость передачи информации (CIR) превышена или установлена на 0.

**default route** Маршрут, выбранный по умолчанию. Запись таблицы маршрутизации, используемая для передачи кадров в тех случаях, когда следующая точка назначения не указана в таблице явно.

**delay** Задержка. Время, проходящее между инициацией отправителем транзакции и первым полученным ответом. Также время, необходимое для перемещения пакета по маршруту от его источника до назначения. См. также: *latency*.

**demarc** Разграничительная (демаркационная) точка. Точка соединения оборудования телефонной компании и оборудования, установленного на территории абонента (CPE).

**demodulation** Демодуляция. Процесс восстановления исходной формы модулированного сигнала. Модемы, осуществляющие демодуляцию аналогового сигнала, выделяют из него исходный (цифровой) сигнал. См. также *modulation*.

**demultiplexing** Демультимплексирование. Разделение на составные части совокупного входного потока, созданного путем мультиплексирования. См. также *multiplexing*.

**designated bridge** Назначенный мост. Мост, через который проходит путь передачи кадра из некоторого сегмента, имеющий минимальную стоимость.

**designated port** Назначенный порт. Применяется с протоколом STP для назначения пересылающих портов. Если в одной сети есть несколько каналов, STP отключает порт, чтобы предотвратить сетевые петли.

**designated router** Назначенный маршрутизатор. Маршрутизатор OSPF, создающий уведомления LSA для сети с множественным доступом и необходимый для выполнения других особых задач протокола OSPF. OSPF-сети с множественным доступом, поддерживающие минимум два

подключенных маршрутизатора, идентифицируют один маршрутизатор, который выбирается протоколом OSPF Hello. Это позволяет уменьшить количество необходимых смежных маршрутизаторов в сети с множественным доступом. Это, в свою очередь, сокращает количество трафика протокола маршрутизации и физический размер базы данных.

**destination address** **Адрес** получателя (назначения). Адрес сетевого устройства, принимающего данные.

**directed broadcast** Направленное широковещание. Кадр или пакет с данными, передаваемый определенной группе узлов на удаленном участке сети. Направленные широковещательные рассылки известны по широковещательному адресу, который представляет собой адрес подсети назначения, где задействованы все биты.

**discovery mode** Режим обнаружения. Процесс, во время которого интерфейс AppleTalk получает от функционирующего узла информацию о подключенной сети, а затем использует ее для самоконфигурирования. Также называется "динамическим конфигурированием".

**distance-vector routing algorithm** Алгоритм маршрутизации по вектору расстояния. Класс алгоритмов маршрутизации, в которых поиск дерева, покрывающего кратчайший путь, осуществляется итеративно по числу переходов на маршруте. Согласно алгоритму, после очередного обновления каждый маршрутизатор посылает всю свою таблицу маршрутизации, но только соседям. Эти алгоритмы могут приводить к заикливанию маршрутов, но по объему вычислений они проще, чем алгоритмы маршрутизации по состоянию канала. Другое название — "алгоритм Беллмана-Форда". См. также *link-state routing algorithm* и *SPF*.

**distribution layer** Уровень распределения. Средний уровень в трехуровневой иерархической модели Cisco, который помогает проектировать, устанавливать и обслуживать иерархические сети Cisco. Уровень распределения — это место соединения устройств уровня доступа. На этом уровне осуществляется маршрутизация.

**DLCI (Data-Link Connection Identifier)** Идентификатор соединения канала передачи данных. Идентифицирует виртуальные цепи в сети Frame Relay.

**DNS (Domain Name System)** Служба именованя доменов. Система, используемая в Интернете для преобразования имен сетевых узлов в их адреса.

**DSAP (Destination Service Access Point)** Точка доступа к услугам получателя. Точка доступа к услугам сетевого узла, указываемая в поле получателя пакета. Сравните с *SSAP*. См. также *SAP(1)*.

**DSR (Data Set Ready)** Сигнал готовности. Когда оборудование передачи данных включено и готово к работе, активизируется и эта интерфейсная цепь EIA/TIA-232.

**DSU (Data Service Unit)** Устройство обслуживания данных. Устройство передачи цифровых данных, которое настраивает физический интерфейс устройства DTE на тип линии передачи, например T1 или E1. Также отвечает за **синхронизацию** сигналов. Обычно рассматривается как часть комбинации DSU/CSU. *См. также CSU.*

**DTE (Data Terminal Equipment)** Оконечное оборудование обработки данных. Устройства DTE подключаются на стороне пользователя к интерфейсу между пользователем и сетью и выполняют функции источника и/или получателя. Устройство DTE соединяется с сетью передачи данных через устройство DCE (например, через модем) и обычно использует синхросигналы, создаваемые устройством DCE. К устройствам DTE относятся, например, компьютеры, трансляторы протоколов и мультиплексоры. *См. также DCE.*

**DTR (Data Terminal Ready)** Сигнал "устройство готово". Сигнал схемы EIA/TIA-232, сообщающий устройству DCE о том, что устройство DTE готово посылать или принимать данные.

**DUAL (Diffusing Update Algorithm)** Алгоритм диффузного обновления. Сходящийся алгоритм, используемый в расширенном протоколе IGRP для создания беспетлевых маршрутов на любом этапе их вычисления. Согласно алгоритму, маршрутизаторы, вовлеченные в изменение топологии, одновременно синхронизируют свои таблицы маршрутизации, а маршрутизаторы, которых эти изменения не касаются, в процессе изменения таблиц не участвуют. *См. также Enhanced IGRP.*

**DVMRP (Distance Vector Multicast Routing Protocol)** Протокол многоадресной маршрутизации по вектору расстояния. Протокол межсетевых шлюзов, основанный на протоколе RIP и реализующий обычную многоадресную схему рассылки в уплотненном режиме. Для обмена датаграммами о маршрутизации между соседями в протоколе DVMRP используется протокол IGMP. *См. также IGMP.*

- **DXI (Data Exchange Interface)** Интерфейс обмена данными. Спецификация Форума ATM, описанная в RFC 1482. Определяет, как сетевое устройство (например, маршрутизатор) может эффективно выполнять функции интерфейсного процессора в сети ATM, взаимодействуя со специальным устройством DSU, осуществляющим сегментирование и сборку пакетов.

**dynamic entries** Динамические записи. Используются в устройствах второго и третьего уровней для динамического создания таблицы аппаратных или логических адресов.

**dynamic routing** Динамическая маршрутизация. Процедура маршрутизации, при которой производится автоматическая настройка на изменение топологии сети или трафика. Также называется "адаптивной маршрутизацией".

**dynamic VLAN** Динамическая виртуальная ЛВС. Администратор создает запись на специальном сервере с аппаратными адресами всех устройств

объединенной сети. Затем сервер динамически назначает используемые виртуальные ЛВС.

**E1** Линия E1. Глобальная схема цифровой передачи данных со скоростью 2.048 Мбит/с, в основном применяемая в Европе. Линии E1 можно арендовать для частного использования.

**E.164** 1. Рекомендации ITU-T по нумерации международных телекоммуникаций, особенно в сетях ISDN, BISDN и SMDS. Эволюция стандартных телефонных номеров. 2. Название поля в адресе ATM, содержащего номера в формате E.164.

**E channel (Echo channel)** E-канал, эхо-канал. Коммутируемый канал управления в сетях ISDN, имеющий скорость передачи 64 Кбит/с. Определен в спецификации ISDN, созданной ITU-T в 1984 г., и исключен из спецификации 1988 г. *Сравните с B channel, D channel и H channel.*

**edge device** Устройство, обеспечивающее пересылку пакетов между традиционными интерфейсами (например Ethernet и Token Ring) и ATM-интерфейсами на основе информации канального и сетевого уровней. Граничное устройство не участвует в работе какого-либо протокола сетевого уровня — оно всего лишь использует протокол описания маршрутов, чтобы получить необходимые сведения для пересылки.

**EEPROM (Electrically Erasable Programmable Read-Only Memory)** Электрически стираемое программируемое ПЗУ. Микросхема памяти, содержимое которой может быть стерто под воздействием электрического сигнала, прилагаемого к определенному выводу микросхемы. *См. также EPROM, PROM.*

**EFCI (Explicit Forward Congestion Indication)** Индикация явного уведомления о перегрузке сети. В ATM — один из способов оповещения о перегрузке, выполняемый с доступной скоростью (ABR). Сетевой элемент, находящийся в состоянии приближающейся или наступившей перегрузки, может установить индикатор явного уведомления о перегрузке. Конечная система-получатель может реализовать протокол, с помощью которого адаптивно понизится скорость передачи ячеек по соединению, для которого выставлен индикатор. *См. также ABR.*

**EIGRP** *См.: Enhanced IGRP.*

**EIP (Ethernet Interface Processor)** Интерфейсный процессор Ethernet. Плата интерфейсного процессора в маршрутизаторе Cisco серии 7000. Интерфейсный процессор предоставляет высокоскоростной (10 Мбит/с) порт AUI, поддерживающий интерфейсы Ethernet Version 1 и Ethernet Version 2 или IEEE 802.3, и высокоскоростной путь передачи данных другим интерфейсным процессорам.

**ELAN (Emulated LAN)** Эмулируемая локальная сеть. Сеть ATM, в которой на основе модели клиент-сервер эмулируется локальная сеть Ethernet или Token Ring. Эмулируемые локальные сети содержат клиенты LANE

(LEC), серверы LANE (LES), серверы рассылки широковещательных и неизвестных сообщений (BUS) и серверы конфигурации LANE (LECS). В одной сети ATM могут существовать одновременно несколько эмулируемых локальных сетей. Эмулируемая локальная сеть определяется спецификацией LANE. См. также LANE, LEC, LECS и LES.

**ELAP (EtherTalk Link Access Protocol)** Протокол доступа к каналу EtherTalk. Используется в сети EtherTalk. ELAP построен на вершине стандартного канального уровня Ethernet.

**encapsulation** Инкапсуляция. Метод, используемый иерархическими протоколами, когда уровень добавляет к протокольной единице данных высшего уровня свою заголовочную информацию. Например, в Интернет-терминологии пакет содержит заголовок физического уровня, после которого идет заголовок сетевого уровня (IP), а за ним заголовок транспортного уровня (TCP), за которым следуют данные прикладного протокола.

**encryption** Шифрование. Преобразование информации в зашифрованную форму для защиты данных от нежелательного доступа. Каждая схема шифрования основана на хорошо проработанном алгоритме, на принимающей стороне выполняется обратное преобразование — дешифрование.

**Enhanced IGRP (Enhanced Interior Gateway Routing Protocol)** Усовершенствованная версия протокола IGRP, созданная компанией Cisco. Обладает ускоренной сходимостью и повышенной эффективностью, объединяет достоинства протоколов маршрутизации по состоянию канала и по вектору расстояния. *Сравните с IGRP. См. также IOP, OSPF и RIP.*

**enterprise network** Сеть предприятия. Большая разнородная сеть, соединяющая наиболее важные пункты предприятия или организации. Отличается от городской сети (MAN) тем, что является частной и обслуживается самим владельцем.

**EPROM (Erasable Programmable Read-Only Memory)** Программируемое ПЗУ. Микросхема ПЗУ, программируемого при изготовлении. При необходимости ее содержимое можно стереть или перепрограммировать. *Сравните с EEPROM и PROM.*

**ESF (Extended Superframe)** Расширенный суперкадр. Формат кадров, передаваемых по линиям T1: каждый суперкадр состоит из 24 кадров длиной по 193 бит. 193-й бит предназначен для синхронизации и других функций. *См. также SF.*

**Ethernet** Спецификация немодулированной ЛВС корпорации Xerox Corporation, продолженная совместными усилиями Xerox, Digital Equipment Corporation и Intel. Спецификация Ethernet похожа на стандарт IEEE серии 802.3 и, используя CSMA/CD, действует на разных кабелях со скоростью 10 Мбит/с. Другое название - DIX (Digital/Intel/Xerox) Ethernet. *См. также: 10BaseT, FastEthernet и IEEE.*

**EtherTalk** Продукт канального уровня, созданный компанией Apple Computer и предназначенный для соединения сетей AppleTalk и Ethernet.

**ETSI (European Telecommunication Standards Institute)** Европейский институт телекоммуникационных стандартов. Организация, созданная европейскими предприятиями почтовой, телефонной и телеграфной связи и странами ЕС для разработки телекоммуникационных стандартов.

**excess rate** Избыточная скорость. В АТМ — поступление трафика со скоростью, превышающей гарантированную скорость данного соединения. Избыточная скорость равна разности максимальной и гарантированной скоростей. Избыточный трафик доставляется по назначению, если имеются доступные ресурсы, и может быть отброшен в периоды перегрузки. Сравните с *maximum rate*.

**expansion** Процедура направления сжатых данных через алгоритм, восстанавливающая данные до их исходного размера.

**expedited delivery** Ускоренная доставка. Параметр, устанавливаемый протоколом некоторого уровня для указания протоколам других уровней (или протоколу того же уровня другого сетевого устройства) на необходимость повышения скорости обработки трафика.

**explorer packet** Пакет исследования. Пакет SNA, транслируемый исходным устройством Token Ring для поиска пути через мостовую сеть исходных маршрутов.

**extended IP access list** Расширенный список доступа IP. Список доступа IP, фильтрующий сеть по логическим адресам, полю протокола в заголовке сетевого уровня и даже полю порта в заголовке транспортного уровня.

**extended IPX access list** Расширенный список доступа IPX. Список доступа IPX, фильтрующий сеть по логическим адресам IPX, полю протокола в заголовке сетевого уровня или даже номеру сокета в заголовке транспортного уровня.

**Extended Setup** Расширенная настройка. В режиме настройки задает маршрутизатору большее количество параметров, чем в базовом режиме настройки. Разрешает многопротокольную поддержку и настройку интерфейса.

**failure domain** Область неисправности. Область сети Token Ring, содержащая неисправность, информация о которой распространяется в кадре аварийной сигнализации (beacon). Когда некоторая станция выявляет серьезную неисправность сети (например, обрыв кабеля), она посылает кадр аварийной сигнализации, в котором указываются станция, обнаружившая неисправность, ее ближайший активный предшественник (NAUN) и все, что находится между ними. Передача кадра аварийной сигнализации запускает процесс, называемый "автореконфигурированием". См. также *autoreconfiguration, beacon* и *NAUN*.

**fallback** Восстановление. Механизм, используемый в сетях АТМ, когда при выборе точного пути не удается построить доступный путь. Механизм восстановления пытается определить путь, смягчая некоторые атрибуты критерия выбора (например, задержку), чтобы найти путь, удовлетворяющий критерию с минимальным количеством атрибутов.

**Fast Ethernet** Быстрая Ethernet. Любая из спецификаций Ethernet со скоростью передачи 100 Мбит/с. Скорость передачи в Fast Ethernet в 10 раз выше, чем в Ethernet, при этом в Fast Ethernet сохранены принятые в Ethernet формат кадра, механизмы работы с **MAC-адресами** и максимальный пересылаемый блок данных (MTU). Это позволяет использовать в сетях Fast Ethernet приложения и средства управления, разработанные для сетей ЮBaseT. Основу спецификации Fast Ethernet составляет IEEE 802.3. *Сравните с Ethernet. См. также 100BaseFX, 100BaseT, 100BaseT4, 100BaseTX, 100BaseXu IEEE 802.3.*

**fast switching** Скоростная коммутация. Средство Cisco, с помощью которого кэш маршрутов используется для ускорения коммутации пакетов в маршрутизаторе. Противоположна process switching.

**FDM (Frequency-Division Multiplexing)** Мультиплексирование с разделением частот. Метод, позволяющий назначать одну линию данным разных каналов на основе частоты. *См. также ATDM, statistical multiplexing (статистическое уплотнение) и TDM.*

**FDDI (Fiber Distributed Data Interface)** Распределенный интерфейс пересылки данных по волоконно-оптическим каналам. Стандарт ЛВС, определенный спецификацией ANSI X3T9.5, который может работать на скоростях до 200 Мбит/с и использует доступ с передачей маркера оптоволоконного кабеля. Для обеспечения избыточности FDDI может использовать архитектуру сдвоенного кольца.

**FECN (Forward Explicit Congestion Notification)** Явное уведомление о перегрузке сети. Если в сетях Frame Relay первый бит FECN кадра равен 1, это указывает устройству DTE, принимающему кадр, на возникновение перегрузки в маршруте от источника к получателю. Устройство DTE, принимающее кадры с установленным битом FECN, может послать запрос протоколам более высоких уровней на выполнение необходимых действий по управлению потоком данных. *Сравните с BECN.*

**FEIP (Fast Ethernet Interface Processor)** Интерфейсный процессор Fast Ethernet. Интерфейсный процессор маршрутизаторов Cisco серии 7000. Поддерживает один или два порта 100BaseT со скоростью передачи 100 Мбит/с.

**firewall** Защитная система, брандмауер. Маршрутизатор или сервер доступа либо несколько таких устройств, выполняющих роль буфера между частной сетью и любыми общедоступными сетями. Для обеспечения защиты частной сети защитный маршрутизатор использует списки доступа и другие методы.

**Flash** Флэш. Электронно-стираемое программируемое постоянное запоминающее устройство; по умолчанию применяется для хранения в маршрутизаторе программного обеспечения Cisco IOS.

**flash memory** Флэш-память. Электрически стираемое программируемое ПЗУ. Разработано компанией Intel. Лицензией пользуются также другие производители полупроводниковых приборов. В флэш-памяти можно хранить образы программного обеспечения, программу начальной загрузки. При необходимости содержимое можно записать заново.

**flat network** Плоская сеть. Сеть, являющаяся одним большим коллизионным доменом и одним большим широковещательным доменом.

**flooding** Лавинная передача. Способ передачи трафика, применяемый мостами и переключателями: трафик, принятый через один интерфейс, посылается через все интерфейсы устройства, за исключением того, через который трафик был получен.

**flow control** Управление потоком данных. Методология, применяемая для предотвращения перегрузки принимающих устройств данными, поступающими от передающих устройств. При заполнении буферов принимающего устройства передающему устройству отправляется указание временно прекратить передачу, пока данные из буфера приема не будут обработаны и буфер не будет готов к работе.

**FRAD (Frame Relay Access Device)** Устройство подключения к сети Frame Relay. Любое сетевое устройство, обеспечивающее соединение локальной сети с глобальной сетью Frame Relay. См. также Cisco FRAD и FRAS.

**fragment** Фрагмент. Часть большого пакета, разбитого на более мелкие блоки. Появление фрагментов пакета не обязательно указывает на ошибку, это может быть сделано намеренно. См. также *fragmentation*.

**fragmentation** Фрагментирование. Процесс намеренного дробления пакета на части при посылке данных по промежуточной сетевой среде, которая не поддерживает большие размеры пакетов.

**FragmentFree** Тип коммутации ЛВС, считывающий раздел данных кадра, чтобы убедиться, что не было фрагментации. Иногда называется модификацией сквозного режима cut-through.

**frame** Кадр. Логически сгруппированная информация, посылаемая в виде блока данных канального уровня. Часто имеет заголовок и заключительную часть, окружающие пользовательские данные и используемые для синхронизации и контроля ошибок. Для описания логических групп информации разных уровней базовой модели OSI и различных технологических циклов также используются термины "ячейка", "датаграмма", "сообщение", "пакет" и "сегмент".

**Frame Relay** Протокол канального уровня с коммутацией, являющийся промышленным стандартом. Предназначен для управления несколькими виртуальными каналами, организованными между подключенными

устройствами, с помощью инкапсуляции трафика HDLC. Протокол Frame Relay эффективнее протокола X.25 и должен заменить его. *См. также X.25.*

**Frame Relay bridging** Мост Frame Relay. Метод создания моста, описанный в RFC 1490. Используется тот же алгоритм покрывающего дерева, что и в других функциях моста, но допускается инкапсуляция пакетов для передачи по сети Frame Relay.

**framing** Кадрирование. Инкапсуляция на канальном уровне модели OSI. Называется кадрированием, потому что пакет инкапсулируется и с заголовком, и с трейлером.

**FRAS (Frame Relay Access Support)** Поддержка доступа к Frame Relay. Свойство программного обеспечения Cisco IOS, позволяющее соединять через сеть Frame Relay устройства компании IBM, подключенные к сетям SDLC, Token Ring, Ethernet и Frame Relay, с другими устройствами IBM. *См. также FRAD.*

**frequency** Частота. Число циклов изменения сигнала переменного тока за единицу времени; измеряется в герцах.

**FSIP (Fast Serial Interface Processor)** Быстрый последовательный интерфейсный процессор. Используется по умолчанию в маршрутизаторах Cisco серии 7000. Поддерживает 4 или 8 высокоскоростных последовательных портов.

**FTP (File Transfer Protocol)** Протокол передачи файлов. Протокол уровня приложений из стека протоколов TCP/IP, используемый для передачи файлов между сетевыми узлами. Определен в RFC 959.

**full duplex** Полнодуплексная связь. Возможность одновременной передачи данных обеими взаимодействующими станциями. *Сравните с half duplex и simplex.*

**full mesh** Полная сеть. Термин, описывающий сеть с ячеистой топологией, в которой каждый сетевой узел связан с каждым из оставшихся узлов либо физическим, либо виртуальным каналом. Полная сеть имеет существенную избыточность, но поскольку ее реализация требует серьезных финансовых затрат, она обычно применяется в качестве объединяющей магистрали. *См. также: partial mesh.*

**GNS (Get Nearest Server)** Найти ближайший сервер. Пакет запроса, посылаемый клиентом по сети IPX для обнаружения ближайшего активного сервера конкретного типа. Клиент сети IPX рассылает запрос GNS, требуя ответа либо от сервера из этого же сегмента, либо от маршрутизатора, которому известно, где в объединенной сети может быть размещен нужный сервер. GNS является частью протокола оповещения об услугах (Service Advertisement Protocol, SAP) сети IPX. *См. также IPX и SAP.*

**GRE (Generic Routing Encapsulation)** Общая инкапсуляция при маршрутизации. Туннельный протокол, созданный Cisco и позволяющий

инкапсулировать пакеты разнообразных протоколов в IP-пакеты, создавая виртуальный двухточечный канал от маршрутизаторов Cisco к удаленным точкам через объединенную сеть IP. Подключая многопротокольные подсети к однопротокольной объединяющей магистрали, IP-туннель, использующий GRE, позволяет расширять сеть за пределы магистрали.

**guard band** Защитная полоса. Неиспользуемая полоса частот между двумя коммуникационными каналами, обеспечивающая разделение каналов во избежание взаимных наводок.

**half duplex** Полудуплексный. Возможность передавать данные в каждый момент времени только в одном направлении между станцией-источником и станцией-получателем. Примером полудуплексного протокола является протокол BSC. *См. также full duplex.*

**handshake** Квитирование. Последовательность сообщений, которыми обмениваются два или несколько сетевых устройств для обеспечения синхронизации передачи.

**H channel (High-speed channel)** H-канал, высокоскоростной канал. Полнодуплексный канал ISDN для передачи данных со скоростью 384 Кбит/с. *См. также B channel, D channel и E channel.*

**HDLC (High-Level Data Link Control)** Высокоуровневый протокол управления каналом передачи данных. Созданный ISO протокол канального уровня для синхронной побитовой передачи данных. Основанный на протоколе SDLC, протокол HDLC определяет инкапсуляцию данных для передачи по синхронной последовательной линии с использованием символов кадра и контрольных сумм. *См. также SDLC.*

**helper address** Вспомогательный адрес. Настраивается на интерфейс, через который был получен предназначенный ему широковещательный пакет.

**hierarchical addressing** Иерархическая адресация. Какой-либо план адресации, задействующий логическую цепь команд для определения расположения. IP-адреса состоят из иерархии сетевых номеров, номеров подсети и номеров узлов, чтобы направлять пакеты по соответствующему назначению.

**HIP (HSSI Interface Processor)** Интерфейсный процессор HSSI. Интерфейсный процессор маршрутизаторов Cisco серии 7000. Имеет один порт HSSI для поддержки соединений с сетями ATM, SMDS, Frame Relay или с частными линиями, обладающими скоростью передачи линий T3 и E3.

**holddown** Удержание. Состояние маршрута, при котором маршрутизаторы не передают и не принимают оповещений о нем в течение некоторого времени (период удержания). Используется для удаления неверной информации о маршруте на всех маршрутизаторах сети. Маршрут обычно переводится в состояние удержания при отказе какой-либо связи, входящей в состав маршрута.

**hop** Переход (участок). Термин, описывающий перемещение пакета между двумя сетевыми узлами, например между двумя маршрутизаторами. *См. также hop count.*

**hop count** Счет переходов (участков). Метрика маршрута, используемая для измерения расстояния между источником и получателем. Протокол RIP использует число переходов в качестве единственной метрики. *См. также hop и RIP.*

**host address** Адрес узла. Логический адрес, задаваемый на устройстве администратором или сервером. Логически идентифицирует устройство в объединенной сети.

**HSCI (High-Speed Communication Interface)** Высокоскоростной коммуникационный интерфейс. Созданный Cisco однопортовый интерфейс, обеспечивающий возможность полнодуплексного синхронного последовательного взаимодействия со скоростью до 52 Мбит/с.

**HSRP (Hot Standby Router Protocol)** Протокол маршрутизатора горячего резерва. Обеспечивает высокую готовность сети и прозрачность изменений сетевой топологии. Создает группу маршрутизаторов горячего резерва с лидирующим маршрутизатором, который обслуживает все пакеты, посылаемые по адресу группы горячего резерва. Лидирующий маршрутизатор осуществляет мониторинг остальных маршрутизаторов группы; при его отказе один из резервных маршрутизаторов принимает на себя функции лидера и адрес группы горячего резерва.

**HSSI (High-Speed Serial Interface)** Высокоскоростной последовательный интерфейс. Сетевой стандарт для высокоскоростных (до 52 Мбит/с) последовательных соединений через глобальную сеть.

**hubs** Концентраторы. Устройства физического уровня, которые фактически являются всего лишь портовыми повторителями. Когда на порт поступает электронный цифровой сигнал, этот сигнал усиливается или регенерируется и пересылается всем участкам, кроме того, из которого был получен.

**ICD (International Code Designator)** Указатель международного кода. Один из двух форматов адреса АТМ, созданных Форумом АТМ для применения в частных сетях. Заимствован из модели адресации подсетей, в которой отображение адресов сетевого уровня в адреса АТМ производится на уровне АТМ. *См. также DCC.*

**ICMP (Internet Control Message Protocol)** Протокол управляющих сообщений Интернета. Протокол Интернета сетевого уровня, создающий отчеты об ошибках и предоставляющий другую информацию, относящуюся к обработке IP-пакетов. Описан в RFC 792.

**IEEE (Institute of Electrical and Electronics Engineers)** Институт инженеров по электротехнике и электронике. Профессиональная организация, одним из направлений деятельности которой является разработка

коммуникационных и сетевых стандартов. Стандарты IEEE для локальных сетей в настоящее время являются самыми распространенными.

**IEEE 802.1** Спецификация комитета IEEE, которая определяет мостовую группу. Спецификацией для STP (протокол Spanning Tree Protocol) является IEEE 802.1d. Протокол STP использует алгоритм связующего дерева SPA для поиска и предотвращения сетевых петель в сетях с мостами. Спецификация для транкирования виртуальных ЛВС — IEEE 802.1q.

**IEEE 802.3** Спецификация комитета IEEE, которая определяет группу Ethernet, точнее первоначальный стандарт 10 Мбит/с. Ethernet — это протокол ЛВС, определяющий физический уровень и подуровень MAC сетевого доступа. Спецификация IEEE 802.3 использует метод CSMA/CD (множественный доступ с контролем несущей и обнаружением конфликтов), чтобы обеспечить доступ для многих устройств одной сети. Fast-Ethernet определен как стандарт 802.3и, и Gigabit Ethernet определен как стандарт 802.3q. *См. также CSMA/CD.*

**IEEE 802.5** Спецификация комитета IEEE, определяющая доступ к среде Token Ring.

**IGMP (Internet Group Management Protocol)** Протокол Интернета управления группой. Используется IP-хостами для передачи смежному маршрутизатору, поддерживающему многоадресные рассылки, отчета о своем членстве в группе. В отчет включаются данные о многоадресной рассылке.

**IGP (Interior Gateway Protocol)** Протокол внутреннего шлюза. Протокол Интернета, используемый для обмена информацией о маршрутизации внутри автономной системы. Подобными протоколами являются, например IGRP, OSPF и RIP.

**ILMI (Interim Local Management Interface)** Интегрированный или промежуточный локальный интерфейс управления. Созданная Форумом ATM спецификация, предназначенная для внедрения средств сетевого управления в интерфейс пользователь-сеть ATM. Ячейки интегрированного локального интерфейса управления обеспечивают автоматическую конфигурацию между системами ATM. В эмуляции ЛВС ILMI может предоставлять достаточно информации для того, чтобы конечная станция ATM могла найти сервер LECS. Кроме того, ILMI предоставляет конечной станции префиксные данные точки доступа к сетевой службе ATM.

**in-band management** Внутриполосное управление. Внутриполосным называется управление сетевым устройством через сеть. Примером может служить использование протокола Simple Network Management Protocol (SNMP — протокол простого управления сетью) или Telnet непосредственно через локальную ЛВС. *Сравните с out-of-band management (внеполосное управление).*

**insured burst** Гарантированный монопольный пакет. В сети ATM — наибольший монопольный пакет данных, который может временно существовать в постоянном виртуальном канале (PVC). В соответствии с

функцией охраны трафика он не будет помечен для отбрасывания при перегрузке в сети. Величина гарантированного монопольного пакета измеряется в байтах или ячейках.

**interarea routing** Маршрутизация через несколько областей. Термин, используемый для описания процедуры маршрутизации через несколько логических областей. *Сравните с infra-area routing. См. также area.*

**interface processor** Интерфейсный процессор. Любой процессорный модуль, используемый в маршрутизаторах Cisco серии 7000. См. AIP, SIP, EIP, FEIP, HIP, MIP и TRIP.

**Internet** Интернет. Глобальная "сеть сетей", популярность которой стремительно выросла за последние несколько лет. Изначально задуманный как средство совместных научных исследований, Интернет стал средством обмена и распространения самой разнообразной информации. Требование Интернета к взаимодействию несопоставимых компьютерных платформ и технологий привело к разработке унифицированных протоколов и стандартов, которые тоже широко распространились в корпоративных ЛВС. *См. также TCP/IP и MBONE.*

**internet** Сокращение слова "internetwork". Не путать с Интернетом. См. *internetwork.*

**Internet protocol** Протокол Интернета. Любой протокол, входящий в состав стека протоколов TCP/IP. См. TCP/IP.

**internetwork** Объединенная сеть. Совокупность сетей, объединенных маршрутизаторами и другими устройствами и функционирующих как единая сеть. Иногда называется internet. Не путать с Интернетом.

**internetworking** Общее название отрасли промышленности, возникшей для практического решения проблемы объединения сетей. Этот же термин может относиться к продукции, процедурам и технологиям, предназначенным для тех же целей.

**intra-area routing** Маршрутизация **внутри** области. Термин, используемый для описания процедуры маршрутизации внутри логической области. *Сравните с interarea routing.*

**Inverse ARP (Inverse Address Resolution Protocol)** Протокол обратного разрешения адресов. Прием создания в сети динамических сопоставлений, позволяющий устройству, например маршрутизатору, обнаруживать логический сетевой адрес и сопоставлять его с постоянной виртуальной цепью (PVC). Обычно применяется в сети Frame Relay, чтобы определить адрес TCP/IP удаленного узла, отправив локальному идентификатору DLCI запрос обратного разрешения адреса.

**IP (Internet Protocol)** Межсетевой протокол. Протокол сетевого уровня стека TCP/IP, предлагающий межсетевое обслуживание без установления соединения. Протокол IP предоставляет средства адресации и обеспечения безопасности, а также спецификации типа обслуживания, фрагментации и сборки. Описан в RFC 791.

**IP address** IP-адрес. 32-битовый адрес, присваиваемый хостам, которые выполняют TCP/IP. IP-адрес принадлежит одному из пяти классов (А, В, С, D или Е) и представляется четырьмя числами (соответствующими четырем октетам), разделенными точками. Каждый адрес состоит из номера сети, необязательного номера подсети и номера хоста. Номера сети и подсети используются для маршрутизации, а номер хоста служит для адресации отдельного хоста внутри сети или подсети. Маска подсети применяется для извлечения из IP-адреса информации о сети и подсети. Бесклассовая междоменная маршрутизация (CIDR) предлагает новый способ представления IP-адресов и масок подсетей. IP-адрес также называют "адресом Интернета". *См. также CIDR, IPu subnet mask.*

**IPCP (IP Control Program)** Управляющий протокол IP. Протокол установления и конфигурирования соединений IP в сетях PPP. *См. также IP и PPP.*

**IP multicast** Многоадресная IP-рассылка. Метод маршрутизации, позволяющий распространять IP-трафик от одного источника к нескольким получателям или от нескольких источников к нескольким получателям. Вместо того чтобы посылать каждому получателю по одному пакету, группе получателей, идентифицируемой единым многоадресным IP-адресом, отправляется один пакет.

**IPX (Internetwork Packet Exchange)** Протокол межсетевого обмена пакетами. Протокол сетевого уровня (уровня 3) NetWare, используемый для передачи данных между сервером и рабочими станциями. Протокол IPX напоминает протоколы IP и XNS.

**IPXCP (IPX Control Program)** Протокол управления сетью IPX. Протокол, с помощью которого устанавливаются и конфигурируются соединения IPX в сети PPP. *См. также IPX и PPP.*

**IPXWAN** Протокол для новых каналов WAN (глобальной сети), позволяющий предоставлять и согласовывать параметры линии на канале с IPX. Когда канал создан и параметры согласованы двумя прямыми каналами, начинается обычная передача IPX.

**ISDN (Integrated Services Digital Network)** Цифровая сеть с комплексными услугами. Предложенный телефонными компаниями коммуникационный протокол, позволяющий передавать по телефонным сетям данные, речь и другие виды трафика. *См. также B1SDN, BRI и PRI.*

**ISL routing (ISL-маршрутизация)** Маршрутизация Inter-Switch Link является собственным методом Cisco тегирования кадров в коммутируемой объединенной сети. Тегирование кадров — это способ определения принадлежности кадра к виртуальной ЛВС во время его прохождения через коммутируемую объединенную сеть.

**isochronous transmission** Изохронная передача. Асинхронная передача данных по синхронным линиям связи. Для пересылки изохронных сигналов требуется постоянная скорость передачи двоичных сигналов и надежный транспорт. *Сравните с asynchronous transmission и synchronous transmission.*

**ITU-T (International Telecommunication Union Telecommunication Standardization Sector)** Сектор по стандартизации электросвязи ИТУ. Международная организация, разрабатывающая стандарты в области телекоммуникационных технологий.

**LAN (Local Area Network)** Локальная сеть. Высокоскоростная сеть передачи данных с низким уровнем возникновения ошибок, размещаемая в относительно небольшой географической области (диаметром до нескольких тысяч метров). Локальные сети объединяют рабочие станции, периферийные устройства, терминалы и другие устройства, находящиеся в некоторой ограниченной области, например в одном здании. Стандартами локальной сети определены кабельная система и способы передачи сигналов на физическом и канальном уровнях базовой модели OSI. Широко применяемыми технологиями локальных сетей являются Ethernet, FDDI и Token Ring. *Сравните с MAN.*

**LANE (LAN Emulation)** Эмуляция локальной сети. Технология, позволяющая использовать сеть ATM в качестве магистрали локальной сети. Для этого сеть ATM должна поддерживать многоадресную и широковещательную рассылку, отображение MAC-адресов в ATM-адреса и наоборот, управление коммутируемыми виртуальными каналами и нужный формат пакетов. Эмуляция локальной сети определяет также эмулируемые сети Ethernet и Token Ring. *См. также ELAN.*

**LAN switch** Переключатель локальной сети. Высокоскоростной переключатель, пересылающий пакеты между сегментами канального уровня. Большинство переключателей локальной сети передает трафик, используя MAC-адреса. Подобные переключатели иногда называют "коммутаторами кадров" и часто классифицируют в соответствии с используемыми в них методами передачи трафика: методом сквозной коммутации пакетов или методом коммутации пакетов с промежуточным хранением. Многоуровневые переключатели составляют подмножество интеллектуальных переключателей. *См. также multilayer switch, store and forward packet switching.*

**LAPB (Link Access Procedure, Balanced)** Бит-ориентированный протокол канального уровня, составляющий часть стека X.25 и происходящий от протокола SDLC. *См. также SDLC и X.25.*

**LAPD (Link Access Procedure on the D channel)** Процедура доступа к D-каналу. Протокол канального уровня ISDN для D-канала. Создан на основе протокола LAPB для удовлетворения требований к передаче сигналов при доступе к ISDN. Описан в рекомендациях ИТУ-T Q.920 и Q.921.

**latency** Задержка. 1. Промежуток времени между запросом устройства на доступ к сети и предоставлением ему разрешения на передачу данных. 2. Промежуток времени между моментом получения кадра устройством и моментом отправки кадра получателю через соответствующий порт.

**Layer 3 switch** Коммутатор третьего уровня. *См. также multilayer switch (многоуровневый коммутатор).*

**layered architecture** Уровневая архитектура. Стандартный способ создания приложений для работы в сети. Уровневая архитектура позволяет разработчику приложений вносить изменения только на одном уровне, а не во всей программе.

**LCP (Link Control Protocol)** Протокол управления каналом. Протокол, с помощью которого устанавливается, настраивается и закрывается соединение канального уровня, используемое протоколом PPP. *См. также PPP.*

**leaky bucket** Ведро для утечки. В АТМ — метафорическое название общего алгоритма определения скорости передачи ячеек (**GCRA**), который используется для проверки скорости потока ячеек, поступающего от пользователя или из сети. "Дырка в ведре" определяет установившуюся скорость, при которой ячейки еще могут восприниматься, а "глубина ведра" — устойчивость к лавинам ячеек определенной длительности.

**learning bridge** Мост с обучением. Запоминает **MAC-адреса** для сокращения сетевого трафика. Мосты с обучением поддерживают базу данных, содержащую **MAC-адреса** и перечень интерфейсов, связанных с каждым адресом.

**LE\_ARP (LAN Emulation Address Resolution Protocol)** Протокол определения адреса для LANE. Протокол определения АТМ-адреса, соответствующего заданному **MAC-адресу**.

**LEC (LAN Emulation Client)** Клиент LANE. Объект в конечной системе, выполняющий передачу данных, определение адреса и другие функции управления для отдельной конечной системы (**ES**) в отдельной эмулируемой локальной сети (**ELAN**). Клиент LANE предоставляет взаимодействующему с ним объекту более высокого уровня стандартный интерфейс со службами локальной сети. Каждый клиент LANE идентифицируется уникальным АТМ-адресом и связан с одним или несколькими **MAC-адресами**, достижимыми по этому АТМ-адресу. *См. также ELAN и LES.*

**LECS (LAN Emulation Configuration Server)** Сервер конфигурации LANE. Объект, приписывающий клиентов LANE конкретным эмулируемым локальным сетям (**ELAN**), связывая их непосредственно с сервером LANE (**LES**) соответствующей эмулируемой сети. В административном домене должен существовать один сервер конфигурации LANE, обслуживающий все эмулируемые локальные сети, находящиеся внутри этого домена. *См. также ELAN.*

**LES (LAN Emulation Server)** Сервер эмуляции ЛВС. Центральный компонент эмуляции ЛВС, предоставляющий начальные конфигурационные сведения для каждого соединяющегося клиента эмуляции ЛВС. Сервер LES обычно располагается на интегрированном в АТМ маршрутизаторе либо на коммутаторе. В функции сервера эмуляции ЛВС входит настройка и поддержка клиентов эмуляции ЛВС, регистрация для них адресов, хранение базы данных и предоставление ответов по адресам АТМ, а также сопряжение с эмулированной ЛВС. *См. также ELAN, LEC и LECS.*

**link-state routing algorithm** Алгоритм маршрутизации по состоянию канала. Согласно этому алгоритму, маршрутизатор рассылает по широковещательному или многоадресному адресу во все узлы объединенной сети информацию о стоимости путей к каждому из своих соседей. Объективно оценивает топологию сети. Не склонен к заикливанию маршрутов. Однако требуются более сложные вычисления и более мощный трафик (по сравнению с подобными характеристиками алгоритмов маршрутизации по вектору расстояния). См. также *distance vector routing algorithm*.

**LLAP (LocalTalk Link Access Protocol)** Протокол доступа к каналу LocalTalk. Протокол канального уровня, управляющий доставкой данных между узлами в среде LocalTalk. Управляет доступом к шине, предоставляет механизм адресации узлов, управляет передачей и приемом данных, обеспечивает проверку длины пакета и целостности данных.

**LLC (Logical Link Control)** Управление логическим каналом. Верхний из двух подуровней канального уровня, определенных IEEE. На этом подуровне осуществляется обнаружение ошибок, управление потоком данных, создание кадров и адресация для подуровня MAC. Наиболее распространенным протоколом подуровня LLC является протокол IEEE 802.2 в вариантах с установлением и без установления соединения. См. также *Data Link layer* и *MAC*.

**LMI (Local Management Interface)** Улучшенная версия первоначальной спецификации Frame Relay. Функции включают механизм поддержания работоспособности, глобальную адресацию и механизм состояния.

**LNNI (LAN Emulation Network-to-Network Interface)** Межсетевой интерфейс эмуляции ЛВС. В спецификации LANE фазы 2 — интерфейс, поддерживающий связь с серверными компонентами одной эмулированной ЛВС.

**local explorer packet** Локальный пакет-анализатор. В SRB-сети Token Ring — пакет, создаваемый оконечной системой для поиска узла, соединенного с локальным кольцом. Если локальный узел не найден, оконечная система создает одно из двух — связывающий пакет-анализатор или пакет-анализатор всех маршрутов.

**local loop** Местная абонентская линия (отвод). Телефонная линия, идущая с территории абонента к центральному телефонному узлу.

**LocalTalk** Собственный протокол компании Apple Computer, который действует на канальном и физическом уровнях базовой модели OSI. LocalTalk использует метод доступа CSMA/CD и позволяет передавать данные со скоростью 230.4 Кбит/с.

**LSA (Link-State Advertisement)** Оповещение о состоянии канала. Широковещательный пакет, используемый протоколами маршрутизации по состоянию канала и содержащий информацию о соседях и стоимости путей. Оповещения учитываются принимающими их маршрутизаторами для обновления таблиц маршрутизации. Иногда называется "пакетом состояния канала" (*LSP*).

**LUNI (LAN Emulation User-to-Network Interface)** Интерфейс "пользователь-сеть" LANE. Стандарт Форума ATM для LANE в сети ATM. LUNI определяет интерфейс между клиентом LANE (LEC) и сервером LANE (LES). *См. также LES и LECS.*

**MAC (Media Access Control)** Управление доступом к носителю. Нижний из двух подуровней канального уровня, определенных IEEE. На подуровне MAC осуществляется доступ к совместно используемому носителю на основе передачи маркера или соперничества. *См. также Data Link layer и LLC.*

**MAC address** MAC-адрес. Стандартизированный адрес канального уровня, присваиваемый каждому порту или устройству, подключенному к локальной сети. Другие сетевые устройства используют MAC-адреса для определения местоположения в сети нужных портов и для создания и обновления таблиц маршрутизации и структур данных. MAC-адрес имеет длину 6 байт и находится под контролем IEEE. Другие названия — "аппаратный адрес", "адрес уровня MAC", "физический адрес".

**MacIP** Протокол сетевого уровня, инкапсулирующий пакеты IP в пакеты протокола DDP для передачи по сети AppleTalk. Также выполняет функции прокси ARP.

**MAN (Metropolitan-Area Network)** Городская сеть. Размещается в пределах одного города. По своим размерам больше локальной сети, но меньше глобальной сети. *См. также LAN.*

**Manchester encoding** Кодирование Манчестер. Используемый в IEEE 802.3 и сетях Ethernet метод кодирования цифрового сигнала, при котором для синхронизации сигналов используется **внутрибитовое** изменение полярности, а двоичная единица представляется положительным уровнем в начальной части сигнала.

**maximum burst** Максимальный монополюсный пакет. Определяет максимальную длину монополюсного пакета данных, которая временно допустима для постоянного виртуального канала (PVC) ATM. Данные не будут отброшены на ребре сети в соответствии с функцией охраны трафика, даже при превышении максимальной скорости передачи. Подобная величина трафика может существовать лишь на ограниченном интервале времени; в среднем, источник трафика должен передавать данные без превышения максимальной скорости. Значение максимального монополюсного пакета измеряется в байтах или ячейках. *Сравните с insured burst. См. также maximum rate.*

**maximum rate** Максимальная скорость передачи данных, возможная в данном виртуальном канале; равна сумме гарантированного и негарантированного трафика, поступающего из источника. Негарантированные данные могут быть отброшены при перегрузке в сети. Максимальная скорость, которая не может превышать скорость, свойственную носителю, отражает наивысшую пропускную способность виртуального канала. Измеряется в битах или ячейках в секунду. *Сравните с excess rate и insured rate. См. также maximum burst.*

**MBS (Maximum Burst Size)** Максимальный размер пакета. В сигнализирующем сообщении ATM эта метрика, выражающаяся в количестве ячеек, передает степень устойчивости к пиковым пакетам.

**MBONE (Multicast Backbone)** Объединяющая магистраль с многоадресными рассылками. Магистраль Интернета. Поддерживающая многоадресная виртуальная сеть, которая составлена из локальных сетей с поддержкой многоадресных рассылок и из соединяющих их двухточечных туннелей.

**MCDV (Maximum Cell Delay Variation)** Максимальное изменение задержки ячеек. В сетях ATM — максимальное значение CDV для двухточечного соединения вдоль канала связи для Определенного класса трафика. Одна из четырех метрик канала связи, обмен которыми производится с помощью пакетов состояния топологии PTSP при определении доступных ресурсов сети ATM. Для каждого класса трафика существует только одно значение MCDV.

**MCLR (Maximum Cell Loss Ratio)** Максимальный коэффициент потери ячеек. В сети ATM — максимальное значение отношения числа ячеек, потерянных в канале связи или узле, к полному числу ячеек, доставленных по каналу связи или в узел. Одна из четырех метрик канала связи, обмен которыми производится с помощью пакетов состояния топологии PTSP при определении доступных ресурсов сети ATM. Применяется только к ячейкам из трафика, передаваемого с постоянной (CBR) или переменной (VBR) скоростью, если бит CLP ячеек равен 0. *См. также CBR, CLP и VBR.*

**MCR (Minimum Cell Rate)** Минимальная скорость передачи ячеек. Параметр, определенный Форумом ATM, для управления трафиком в сети ATM. Действителен только для соединений с доступной скоростью передачи двоичных данных (ABR) и определяет минимальную величину ABR. *См. также ACR и PCR*

**MCTD (Maximum Cell Transfer Delay)** Максимальная скорость передачи ячеек. В ATM — сумма MCDV и компонента фиксированной задержки, вносимой каналом связи или узлом. Одна из четырех метрик канала связи, обмен которыми производится с помощью пакетов состояния топологии PTSP при определении доступных ресурсов сети ATM. Для каждого класса трафика существует только одно значение MCTD. *См. также MCDV.*

**MIB (Management Information Base)** База сетевой управляющей информации, используемая и поддерживаемая с помощью протокола управления сетью (например, SNMP или CMIP). Значения объектов MIB могут изменяться или извлекаться с помощью команд SNMP или CMIP через графический пользовательский интерфейс системы управления сетью. Объекты MIB организованы в виде деревообразной структуры, имеющей общественные (стандартные) и частные (для внутреннего использования) ветви.

**MIP (Multichannel Interface Processor)** Интерфейсный процессор MultiChannel. Интерфейсный процессор маршрутизаторов Cisco серии 7000. Обеспечивает возможность использования одного или двух соединений с мультиплексированными линиями T1 или E1 через последовательный кабель, подключенный к CSU. Каждый из двух контроллеров MIP поддерживает до 24-х канальных групп в T1 или до 30-ти канальных групп в E1, причем каждая канальная группа воспринимается системой как последовательный интерфейс с возможностью отдельного конфигурирования.

**mips (Millions of instructions per second)** Миллион команд в секунду. Единица измерения скорости процессора.

**MLP (Multilink PPP)** Многоканальный протокол PPP. Метод расщепления, объединения и упорядочения **датаграмм** для передачи по нескольким логическим каналам данных.

**MMP (Multichassis Multilink PPP)** Расширение протокола MLP на несколько маршрутизаторов и серверов доступа. MMP позволяет нескольким маршрутизаторам и серверам доступа функционировать как единый пул устройств с единым сетевым адресом и номером доступа ISDN. Корректно производит фрагментирование и сборку пакетов, когда соединение пользователя расщепляет их между двумя устройствами физического доступа.

**modem (modulator-demodulator)** Модулятор-демодулятор, модем. Устройство для преобразования цифровых сигналов в аналоговые и наоборот, благодаря чему можно передать цифровую информацию по аналоговым линиям связи, например по обычным голосовым телефонным линиям. Для этого цифровой сигнал на передающей станции преобразуется в аналоговый, а на принимающей выполняется обратное преобразование. *См. также modulation и demodulation.*

**modem eliminator** Заменитель (эмулятор) модема. Устройство, позволяющее соединить два устройства DTE без помощи модема.

**modulation** Модуляция. Преобразование характеристик электрических сигналов для кодирования информации. Возможные виды модуляции: амплитудная (AM), частотная (FM) и импульсно-амплитудная (PAM). *См. также AM.*

**MOSPF (Multicast OSPF)** Многоадресный протокол OSPF. Это расширение одноадресного протокола OSPF, **задействующее** в домене маршрутизацию многоадресной рассылки IP. *См. также OSPF.*

**MPOA (Multiprotocol over ATM)** Многопротокольность поверх ATM. Попытка Форума ATM создать стандарт для передачи данных существующих и будущих протоколов сетевого уровня (IP, IPv6, AppleTalk, IPX) по сети ATM с непосредственным подключением хостов, маршрутизаторов и многопротокольных переключателей локальной сети.

**MTU (Maximum Transmission Unit)** Максимальный передаваемый блок. Максимальный размер пакета (в байтах), который может обработать конкретный интерфейс.

**multicast** В широком смысле слова — любая связь между одним отправителем и несколькими получателями. В отличие от ширококвещательных сообщений, посылаемых всем адресам сети, многоадресные сообщения отправляются определенной подгруппе сетевых адресов. Она имеет адрес группы, который указывается в поле назначения пакета. *См. также broadcast (широковещание), directed broadcast (направленное ширококвещание).*

**multicast address** Адрес многоадресной рассылки. Единый адрес, относящийся к группе сетевых устройств. Синоним — group address. *Сравните с broadcast address и unicast address. См. также multicast.*

**multicast send VCC** VCC с многоадресной рассылкой. В сетях ATM - двунаправленное двухточечное соединение виртуальных каналов (VCC), установленное клиентом LANE (LEC) с сервером BUS. Одно из трех соединений, определенных в Phase 1 LANE. *См. также control distribute VCC и control direct VCC.*

**multilayer switch** Многоуровневый переключатель. Крайне специализированный высокоскоростной аппаратный вид маршрутизатора ЛВС. Фильтрует и пересылает пакеты на основе их MAC-адресов второго уровня и сетевых адресов третьего. Есть даже возможность считывания четвертого уровня. Иногда называется коммутатором третьего уровня. *См. также LAN switch (коммутатор ЛВС).*

**multiplexing** Мультиплексирование. Способ одновременной передачи нескольких логических сигналов по одному физическому каналу. *Сравните с demultiplexing.*

**NAK (Negative Acknowledgment)** Отрицательное подтверждение. Ответ, посылаемый принимающим устройством устройству-источнику, чтобы сообщить о наличии ошибок в полученной информации. *Сравните с acknowledgment.*

**NAT (Network Address Translation)** Трансляция сетевого адреса. Механизм, применение которого позволяет сократить число глобально уникальных IP-адресов. Организации, не обладающие глобально уникальными адресами, могут подключаться к Интернету, используя NAT для трансляции своих адресов внутрь пространства глобально маршрутизируемых адресов. Иногда называется "транслятором сетевого адреса".

**NBP (Name Binding Protocol)** Протокол связывания имен. Протокол транспортного уровня AppleTalk, транслирующий символьную строку имени в адрес DDP соответствующего клиента сокета. Позволяет протоколам AppleTalk распознавать зоны, определенные пользователем, и имена устройств за счет создания и поддержки трансляционных таблиц, отображающих имена в соответствующие адреса сокетов.

**neighboring routers** Соседние маршрутизаторы. В OSPF — два маршрутизатора, подключенные к одной сети. В сетях с множественным доступом обнаружение соседних маршрутизаторов производится динамически с помощью протокола Hello, входящего в состав OSPF.

**NetBEUI (NetBIOS Extended User Interface)** Расширенный интерфейс NetBIOS. Улучшенная версия протокола NetBIOS, используемая в нескольких операционных системах, включая LAN Manager, Windows NT, LAN Server и Windows for Workgroups, и реализующая протокол LLC2 модели OSI. NetBEUI формализует транспортный кадр, не типизированный в NetBIOS, и добавляет новые функции. См. также *OSI*.

**NetBIOS (Network Basic Input/Output System)** Сетевая базовая система ввода-вывода. Интерфейс прикладных программ, используемый приложениями в локальной сети IBM для запроса услуг сетевых процессов нижнего уровня. К таким услугам можно отнести открытие и закрытие сеанса и передачу информации.

**NetView** Созданная компанией IBM архитектура управления сетью и связанные с ней приложения. NetView является приложением VTAM, используемым для управления большими ЭВМ в сетях SNA.

**NetWare** Популярная сетевая операционная система, созданная компанией Novell. Обеспечивает прозрачный доступ к удаленным файлам и предоставляет множество других услуг, распределенных по сети.

**network address** Сетевой адрес. Используется с логическими сетевыми адресами для идентификации участка сети в объединенной сети. Логические адреса имеют иерархическую организацию и состоят из, по меньшей мере, двух частей — сетей и узла. Например, в иерархическом адресе 172.16.10.5 значение 172.16 — это сеть, а 10.5 — адрес узла.

**Network layer** Сетевой уровень. Уровень 3 базовой модели OSI. Отвечает за установление соединения и выбор пути между двумя конечными системами. Именно на этом уровне осуществляется маршрутизация. Сетевой уровень примерно соответствует уровню управления путями модели SNA. См. также *Application layer, Data Link layer, Physical layer, Presentation layer, Session layer* и *Transport layer*.

**NFS (Network File System)** Сетевая файловая система. Один из протоколов в широко распространенном наборе протоколов Sun Microsystems, обеспечивающий удаленный доступ к файлам через сеть. Название часто относится ко всему набору протоколов Sun, куда также входят RPC, XDR и другие протоколы.

**NHRP (Next Hop Resolution Protocol)** Протокол определения следующей точки попадания. Используется маршрутизаторами для динамического определения MAC-адресов других маршрутизаторов и хостов, соединенных с сетью NBMA. С этими системами можно связаться напрямую без промежуточных переходов, что повышает производительность сетей ATM, Frame Relay, SMDS и X.25.

**NHS (Next Hop Server)** Сервер следующего перехода. Определяется протоколом **NHRP**. Поддерживает таблицы для определения точки следующего попадания. Эти таблицы содержат IP-адреса и ATM-адреса для связанных узлов и узлов, достижимых через маршрутизаторы, которые обслуживаются сервером следующего перехода.

**NIC (Network Interface Card)** Сетевая интерфейсная плата (сетевой адаптер). Печатная плата, обеспечивающая возможность сетевого взаимодействия с компьютером.

**NLSP (NetWare Link Services Protocol)** Протокол обслуживания канала NetWare. Протокол маршрутизации по состоянию канала, в основе которого лежит протокол **IS-IS**.

**NMP (Network Management Processor)** Процессор управления сетью. Процессорный модуль переключателя Catalyst 5000, используемый для управления переключателем и его мониторинга.

**node address** Адрес узла. Служит для идентификации определенного устройства в объединенной сети. Это может быть впаянный в сетевой адаптер аппаратный адрес или логический сетевой адрес, который назначает узлу администратор или сервер.

**nondesignated port** Неназначенный порт. Протокол связующего дерева приказывает порту на коммутаторе второго уровня прекратить передачу и создание сетевых петель. Кадры могут посылать только назначенные порты.

**non-stub area** Нетупиковая область. Насыщенная ресурсами область **OSPF**, по которой проходят маршрут по умолчанию, статические маршруты, внутренние маршруты области, маршруты, проложенные между областями, и внешние маршруты. Нетупиковые области являются единственными областями **OSPF**, в которых могут существовать конфигурируемые виртуальные связи и размещаться граничные маршрутизаторы автономных систем (**ASBR**). Сравните с *stub area*. См. также *ASBR* и *OSPF*.

**NRZ (Nonreturn to Zero)** Кодирование без возврата к нулю. В течение всего интервала передачи бита сигналы поддерживают постоянный уровень без изменения полярности (без возврата к нулевому уровню). Сравните с *NRZI*.

**NRZI (Nonreturn to Zero Inverted)** Кодирование без возврата к нулю с инвертированием. В течение всего интервала передачи бита сигналы поддерживают постоянный уровень без изменения полярности (без возврата к нулевому уровню), но интерпретируют двоичную единицу сменой уровня сигнала в начале интервала передачи бита, а нуль — отсутствием смены уровня. Сравните с *NRZ*.

**NT1 (Network termination 1)** Сетевое оконечное устройство 1. Назначение **ISDN** устройствам, которые понимают стандарты **ISDN**.

**NT2 (Network termination 2)** Сетевое оконечное устройство 2. Назначение ISDN устройствам, которые не понимают стандарты ISDN. Чтобы можно было использовать NT2, нужен терминальный адаптер (TA).

**NVRAM (Non-volatile RAM)** Энергонезависимое ОЗУ. Устройство памяти, сохраняющее содержимое при отключении питания.

**OC (Optical Carrier)** Оптический носитель. Ряд физических протоколов, обозначаемых как OC-1, OC-2, OC-3 и т.д. для оптических передач сигнала SONET. Сигнальные уровни OC помещают кадры STS на многорежимную оптоволоконную линию с разной скоростью, где самой низкой является 51.84 Мбит/с (OC-1). Каждый последующий протокол работает на скорости, кратной 51.84. *См. также SONET.*

**octet** Октада. Восьмеричная система исчисления, которая служит для идентификации раздела точечно-десятичного IP-адреса. Другое название — байт.

**100BaseT** Основанная на стандарте IEEE 802.3u спецификация узкополосной передачи FastEthernet на 100 Мбит/с, использующая неэкранированный кабель. 100BaseT посылает каналные импульсы (содержащие больше данных, чем в спецификации 10BaseT) по сети при отсутствии трафика. *См. также: 10BaseT, FastEthernet и IEEE 802.3.*

**100BaseTX** Основанная на стандарте IEEE 802.3u спецификация узкополосной передачи FastEthernet на 100 Мбит/с, использующая две неэкранированные или экранированные витые пары. Первая пара кабеля получает данные, вторая — посылает. Для обеспечения правильной синхронизации сигналов участок 100BaseTX не должен быть длиннее 100 метров.

**ones density** Плотность единиц. Метод синхронизации сигналов, называемый еще импульсной плотностью. Устройство CSU/DSU извлекает информацию о синхронизации из проходящих через него данных. Чтобы этот механизм действовал, данные должны кодироваться так, чтобы они содержали, по меньшей мере, одну двоичную единицу на каждые восемь передаваемых битов. *См. также CSU и DSU.*

**OSI (Open Systems Interconnection)** Взаимодействие открытых систем. Международная программа по стандартизации, созданная ISO и ITU-T для развития стандартов сетевой передачи данных, облегчающих решение проблемы совместимости оборудования разных производителей.

**OSI reference model** Базовая модель OSI. Модель сетевой архитектуры, предложенная ISO и ITU-T. Состоит из семи уровней, каждый из которых определяет конкретные функции (например, адресацию, управление потоком данных, контроль ошибок, инкапсуляцию и надежную передачу сообщений). Нижний уровень (физический) близок к технологии передачи сигналов по физическому носителю. Два нижних уровня реализуются программно-аппаратным способом, а следующие пять уровней имеют только программную реализацию. Высший уровень (уровень приложений)

наиболее близок к пользователю. Базовая модель OSI позволяет разобраться в функциональных особенностях работы сетей. Некоторые аспекты этой модели напоминают архитектуру SNA. См. *Application layer, Data Link layer, Network layer, Physical layer, Presentation layer, Session layer u Transport layer*.

**OSPF (Open Shortest Path First)** "Сначала открывать кратчайший путь". Протокол канального уровня для иерархической маршрутизации, относящийся к классу протоколов внутреннего шлюза (ЮР) и предложенный сообществом Интернет в качестве развития протокола RIP. Особенности OSPF: маршрутизация по критерию наименьшей стоимости пути, многовариантность и сбалансированность сетевой нагрузки. OSPF базируется на ранней версии протокола IS-IS. См. также *Enhanced IGRP, IGP u IP*.

**OUI (Organizational Unique Identifier)** Организационно уникальный код. Назначается Институтом ШЕЕ предприятию, которое производит сетевые адаптеры. Затем предприятие закладывает этот код в каждую производимую плату. Код OUI равен 3 байтам (24 битам). Производитель добавляет к этому 3-битный код, чтобы уникальным образом идентифицировать узел в объединенной сети. Общая длина адреса равняется 48 бит (6 байт) и называется аппаратным адресом или MAC-адресом.

**out-of-band management** Внеполосное управление. Управление за пределом физических каналов сети. Например, использование консольного соединения, не сопряженного напрямую через локальную ЛВС или глобальную сеть или наборный модем. Сравнить с *in-band management (внутриполосное управление)*.

**out-of-band signaling** Управление по внешнему каналу. Передача на частотах или по каналам, находящимся вне частотного диапазона или совокупности каналов, обычно используемых для передачи данных. Управление по внешнему каналу применяется для сообщений об ошибках в ситуациях, когда нельзя воспользоваться внутренними каналами сети вследствие проблем, возникших в работе сети. Противоположно *in-band signaling*.

**packet** Пакет. В передачах данных — основная логическая единица передаваемой информации. Пакет состоит из определенного количества байтов данных, упакованных или инкапсулированных в заголовках и/или трейлерах, содержащих сведения о происхождении пакета, его назначении и т.д. Различные протоколы, участвующие в отправке передачи, добавляют свои уровни заголовочных сведений, которые затем интерпретируются соответствующими протоколами принимающих устройств.

**packet switch** Коммутатор пакетов. Физическое устройство, с помощью которого канал связи может иметь общий доступ к нескольким соединениям; его функции включают поиск оптимального маршрута передачи пакетов.

**packet switching** Коммутация пакетов. Сетевая технология, основанная на передаче данных пакетами. Членение непрерывного потока данных на небольшие модули — пакеты — позволяет нескольким устройствам сети совместно использовать один канал связи одновременно, но требует точной маршрутной информации.

**PAP (Password Authentication Protocol)** Протокол аутентификации по паролю. Протокол, с помощью которого равноправные партнеры, использующие протокол PPP, опознают друг друга. Чтобы установить соединение с локальным маршрутизатором, удаленный маршрутизатор должен послать запрос аутентификации. В отличие от протокола CHAP, протокол PAP пересылает пароль и имя хоста или пользователя в открытом (незашифрованном) виде. PAP не препятствует несанкционированному доступу, а лишь идентифицирует удаленный узел. Проверка наличия права доступа у пользователя осуществляется маршрутизатором или сервером доступа. Протокол PAP поддерживается только на линиях PPP. *Сравните с CHAP.*

**parity checking** Проверка четности. Метод проверки ошибок в передачах данных. Дополнительный бит (бит четности) добавляется к каждому символу или слову данных, чтобы сумма битов была нечетным числом (в проверке на нечетность) или четным числом (проверка на четность).

**partial mesh** Частичная сеть. Термин, описывающий сеть с ячеистой топологией, в которой часть сетевых узлов составляет полную сеть, а оставшиеся узлы имеют связи лишь с одним или двумя сетевыми узлами. Частичная сеть не имеет той избыточности, которая присуща полной сети, однако она дешевле. Топология частичной сети используется обычно в периферийных сетях, которые связываются с объединяющей магистралью, являющейся полной сетью. *См. также full mesh.*

**PCR (Peak Cell Rate)** Пиковая скорость ячеек. Согласно определению Форума АТМ, параметр, определяющий в ячейках в секунду максимальную скорость, с которой может передавать источник.

**PDN (Public Data Network)** Общественная сеть передачи данных. Управление сетью осуществляется либо правительством (в Европе), либо частным концерном. Предназначается для организации взаимодействия между компьютерными системами различных владельцев, обычно платно. Использование общественной сети дает возможность небольшим организациям создать глобальную сеть, не приобретая всего необходимого оборудования для передачи сигналов на большие расстояния.

**PGP (Pretty Good Privacy)** Распространенное приложение шифрования с помощью открытого и закрытого ключей, обеспечивающее защищенную передачу файлов и сообщений.

**Physical layer** Физический уровень. Уровень 1 базовой модели OSI. Определяет электрические, механические, процедурные и функциональные спецификации для активизации, поддержки и деактивизации физического канала между конечными системами. Соответствует уровню физического управления архитектуры SNA. *См. также Application layer, Data Link layer, Network layer, Presentation layer, Session layer и Transport layer.*

**ping (packet internet groper)** Основанный на платформе Unix инструмент диагностики, состоящий из сообщения, посылаемого для проверки доступности определенного устройства сети IP. Сокращенная форма (из

которой произошло "полное название") отражает подразумеваемое метафорическое представление гидролокатора подводной лодки (Слово "ping" по-английски означает еще звуковой или ультразвуковой импульс гидролокатора. *Прим. пер.*). Как оператор гидролокатора посылает сигнал и ожидает его отраженное эхо (импульс) от погруженного в воду объекта, так пользователь сети может послать сигнал ping другому узлу сети, чтобы узнать, будет ли ответ.

**plesiochronous** Плейзохронный. Почти синхронный с тем исключением, что тактирование происходит из внешнего источника, а не внедрено в сигнал, как в синхронных передачах.

**PLP (Packet Level Protocol)** Протокол пакетного уровня. Протокол сетевого уровня из стека протоколов

**X.25.** Иногда называется X.25 Level 3 или X.25 Protocol. *См. также X.25.*

**PNNI (Private Network-Network Interface)** Частный интерфейс сеть-сеть. Спецификация Форума ATM для предложения данных топологии, используемых при вычислении путей по сети между коммутаторами и группами коммутаторов. Спецификация основывается на хорошо известных процедурах маршрутизации состояния каналов и позволяет производить автоматическую настройку в сетях, система адресации которых определяется топологией.

**point-to-multipoint connection** Соединение "точка-несколько точек" (один-ко-многим). Один из двух фундаментальных способов соединения. В ATM многоточечное соединение является однонаправленным, причем одно конечное устройство-источник (корневой узел) соединяется с несколькими конечными узлами-получателями (листьями). *Сравните с point-to-point connection.*

**point-to-point connection** Соединение "точка-точка". Один из двух фундаментальных способов соединения. В ATM двухточечное соединение может быть однонаправленным или двунаправленным соединением между двумя конечными системами ATM. *Сравните с point-to-multipoint connection.*

**poison reverse updates** Обновления типа "опасный реверс". Вместо исключения из обновляющей информации о маршрутах сведений о недостижимой сети или подсети, в сообщении об обновлении вносится явное указание на недостижимость сети. Рассылка обновлений типа "опасный реверс" предотвращает появление больших циклов в маршрутах.

**polling** Опрос (голосование). Метод доступа, при котором основное сетевое устройство выясняет в принятом порядке, имеет ли вторичное устройство данные для передачи. При этом каждому вторичному устройству сообщается о предоставлении права на передачу.

**POP 1. Point of presence.** Точка присутствия. В системе оперативной поддержки (OSS) — физическая точка, где пересекаются оборудование, установленное провайдером дальней связи, и оборудование местной

телефонной компании. 2. Post Office Protocol. Протокол почтового офиса. Используется клиентом приложения электронной почты для получения почты от почтового сервера.

**port security** Безопасность портов. Применяется с коммутаторами второго уровня для обеспечения безопасности. Редко используется в производстве, потому что сложна в управлении. Позволяет только определенным кадрам пересекать назначенные администратором участки.

**PDU (Protocol Data Unit)** Единица данных протокола. Название процессов на каждом уровне модели OSI. Модули PDU на транспортном уровне называются сегментами, на сетевом — пакетами, или датаграммами, на канальном уровне — кадрами. Физический уровень использует биты.

**PPP (Point-to-Point Protocol)** Протокол сквозного соединения. Наиболее распространенный протокол для удаленного доступа к Интернету, пришедший на замену более раннему протоколу SLIP. Его характеристики включают адресное уведомление, проверку подлинности через протокол CHAP или PAP, поддержку нескольких протоколов и наблюдение за связью. PPP имеет два уровня: протокол управления каналом Link Control Protocol (LCP) устанавливает, настраивает и проверяет канал; затем какая-либо из различных программ управления сетью Network Control Program (NCP) передает трафик для определенного набора протоколов, например, IPX. См. также CHAP, PAP, и SLIP.

**Presentation layer** Уровень представлений. Уровень 6 базовой модели OSI. Гарантирует, что данные, переданные с уровня приложений одной системы, будут читаемы на уровне приложений другой системы. Работает со структурами данных, используемых программами, и поэтому согласует синтаксис передаваемых данных для уровня приложений. Примерно соответствует уровню представительных служб модели SNA. См. также *Application layer, Data Link layer, Network layer, Physical layer, Session layer u Transport layer*.

**PRI (Primary Rate Interface)** Интерфейс передачи данных с основной скоростью. Интерфейс сети для доступа к носителю с основной скоростью. Доступ с основной скоростью осуществляется по одному D-каналу (64 Кбит/с) и 23-м (T1) или 30-ти (E1) B-каналам для передачи речи или данных. См. также ISDN.

**priority queuing** Очередь приоритетов. Свойство процесса маршрутизации: кадры в выходной очереди интерфейса получают приоритеты в соответствии с различными характеристиками, например, в зависимости от длины пакета или типа интерфейса.

**process switching** Переключение процессов. Когда пакет поступает в маршрутизатор для пересылки, он копируется в буфер процессов маршрутизатора, и маршрутизатор просматривает адрес третьего уровня. С помощью таблицы маршрутов выходной интерфейс ассоциируется с адресом назначения. Процессор пересылает пакет с новой добавленной информацией на выходной интерфейс, в то время как маршрутизатор

инициирует кэш быстрой коммутации. Последующие пакеты, направляющиеся к тому же адресу назначения, следуют по тому же пути, что и первый пакет.

**PROM (Programmable Read-Only Memory)** Программируемое ПЗУ. Может быть запрограммировано с помощью специального оборудования лишь однократно. *Сравните с EPROM.*

**propagation delay** Задержка распространения. Время, необходимое для переноса данных по сети от источника к получателю.

**protocol** Протокол. Формальное описание набора правил и соглашений, управляющих процессом обмена данными между сетевыми устройствами.

**protocol stack** Стек протоколов. Группа связанных между собой протоколов.

**PSE (Packet Switch Exchange)** Узел коммутации пакетов. Термин X.25, обозначающий коммутатор.

**PSN (Packet-Switched Network)** Сеть с коммутацией пакетов. Сеть, в которой при передаче данных используется технология коммутации пакетов. Иногда называется "сетью передачи данных с коммутацией пакетов" (PSDN). *См. packet switching.*

**PSTN (Public Switched Telephone Network)** Телефонная коммутируемая сеть общего пользования. Общий термин, описывающий различные телефонные сети и услуги. Иногда называется "обычной аналоговой телефонной сетью" (POTS).

**PVC (Permanent Virtual Circuit)** Постоянная виртуальная цепь. Устанавливается на длительное время. Постоянные виртуальные цепи сохраняют полосу пропускания, связанную с установлением соединения, и закрывают соединение, если некоторые цепи должны существовать все время. В терминологии АТМ называется "постоянным виртуальным соединением". *Сравните с SVC. См. также virtual circuit.*

**PVP (Permanent Virtual Path)** Постоянный виртуальный путь. Содержит постоянные виртуальные каналы. *См. также PVC.*

**PVP tunneling (Permanent Virtual Path tunneling)** Туннель PVP. Метод связи двух частных сетей АТМ через общедоступную сеть с использованием виртуального пути. Общедоступная сеть является прозрачной магистралью, объединяющей всю совокупность виртуальных каналов в виртуальный путь между двумя частными сетями.

**QoS (Quality of Service)** Качество обслуживания. Мера производительности передающей системы, отражающая качество передачи и доступность сервиса.

**queue** Очередь. В широком смысле слова, любой упорядоченно организованный ряд объектов, готовый к обслуживанию, например очередь людей перед входом в кинотеатр. В маршрутизации — задолженность по

обработке пакетов данных, ожидающих в очереди своей передачи через интерфейс маршрутизатора.

**R reference point** Контрольная точка R. В сетях ISDN — идентифицирует соединение между ISDN-устройством NT1 и устройством S/T. Устройство S/T преобразовывает 4-кабельную сеть в стандартную 2-кабельную сеть ISDN.

**RAM (Random-Access Memory)** Устройство памяти с произвольным доступом, ОЗУ. Энергозависимая память, содержимое которой может быть считано или записано микропроцессором.

**RARP (Reverse Address Resolution Protocol)** Протокол обратного определения (разрешения) адреса. Протокол из набора TCP/IP, позволяющий определять IP-адрес, соответствующий MAC-адресу. См. также AIP.

**rate queue** Скорость очереди. Величина, связанная с одним или несколькими виртуальными каналами. Определяет скорость, с которой отдельный виртуальный канал может передать данные в конечную точку. Каждая скорость очереди представляет часть полной полосы пропускания, доступной в канале ATM. Объединенная полоса пропускания всех сконфигурированных скоростей очереди не должна превышать полную доступную полосу пропускания.

**RCP (Remote Copy Protocol)** Протокол удаленного копирования. Позволяет пользователям обмениваться файлами (с помощью копирования) с файловой системой удаленного хоста или сервера. Использует протокол TCP для обеспечения надежной доставки данных.

**redistribution** Перераспределение. Допустимость распространения информации о маршрутизации, полученной с помощью одного протокола, в сообщениях об обновлении, формируемых другим протоколом маршрутизации. Иногда называется "перераспределением маршрута".

**redundancy** Избыточность. В объединенных сетях дубликат соединений, устройств или служб, который может использоваться как резерв на случай сбоя основных соединений, устройств или служб.

**reload** Перезагрузка. Событие, при котором происходит повторная начальная загрузка маршрутизатора Cisco, или команда, вызывающая начальную загрузку маршрутизатора.

**RIF (Routing Information Field)** Поле информации маршрутизации. В объединении с помощью мостов по маршруту источника — поле заголовка, которое определяет направление пути кадра или метки. Если бит индикатора маршрутной информации (RI) не установлен, поле RIF считывается от источника к назначению (слева направо). Если бит RI установлен, поле RIF считывается от назначения к источнику, т.е. справа налево. Это поле определяется как часть заголовка кадра Token Ring для кадров с направлением от источника, который содержит данные о пути.

**ring** Кольцо. Соединение нескольких станций в логическую кольцевую структуру. Информация последовательно передается между активными станциями. Token Ring, FDDI и CDDI — сети с кольцевой топологией.

**ring topology** Кольцевая топология. Сетевая топология, состоящая из последовательности повторителей, соединенных друг с другом однонаправленным каналом передачи так, что образуется единое замкнутое кольцо. Каждая сетевая станция соединяется с сетью через повторитель. Представляя собой логическое кольцо, кольцевая топология в большинстве случаев организуется как смешенная — звездообразная и кольцевая — физическая структура. *Сравните с bus topology и star topology.*

**RIP (Routing Information Protocol)** Протокол информации о маршрутизации. Протокол внутреннего шлюза (IGP), поставляемый вместе с системой UNIX BSD. Наиболее распространенный протокол внутреннего шлюза в Интернете. В качестве метрики при маршрутизации в RIP используется число переходов между маршрутизаторами. *См. также Enhanced IGRP, hop count, IGP и OSPF.*

**RJ connector (Registered Jack connector)** Стандартный разъем. Соединитель с регистрованным гнездом используется с витой парой для соединения медного провода с сетевыми адаптерами, коммутаторами и концентраторами.

**ROM (Read-Only Memory)** ПЗУ. Энергонезависимая память, содержимое которой микропроцессор может только прочитать; изменить содержимое ПЗУ невозможно.

**root bridge** Корневой мост. Применяется с протоколом связующего дерева для предотвращения сетевых петель. Выбирается по наименьшему коду моста. Код моста определяется по предпочтению (32 768 по умолчанию на всех мостах и коммутаторах) и основному аппаратному адресу устройства. Корневой мост определяет, какие из интерфейсов соседних устройств второго уровня становятся назначенными или неназначенными портами.

**routed protocol** Маршрутизируемый протокол. Направляемые протоколы (например, IP и IPX) применяются для пересылки пользовательских данных через объединенную сеть. В отличие от них, направляющие протоколы (например, RIP, IGRP и OSPF) служат для обновления таблиц маршрутизации между маршрутизаторами.

**route poisoning** "Отравление маршрута". Используется различными протоколами маршрутизации дистанционного вектора, чтобы преодолеть большие петли маршрутизации и предоставить ясную информацию в случае, когда сеть или подсеть недоступна (вместо того чтобы просто предполагать, что сеть недоступна, не включая данные сведения в обновления). Обычно для этого устанавливается число маршрутов, превышающее максимально значение на один. *См. также: poison reverse updates (обновления "отравленного обратного пути").*

**route summarization** Маршрутное резюмирование. Объединение маршрутов. В OSPF, EIGRP и IS-IS — объединение известных адресов в один общий маршрут, информация о котором передается граничным маршрутизатором автономной системы в другие области.

**router** Маршрутизатор. Устройство сетевого уровня, использующее одну или несколько метрик для определения оптимального пути, по которому будет передан сетевой трафик. Маршрутизаторы перемещают пакеты из одной сети в другую в соответствии с информацией сетевого уровня. Иногда называется "шлюзом" (хотя это значение термина "шлюз" постепенно выходит из употребления).

**routing** Маршрутизация. Поиск пути к хосту получателя. Маршрутизация в больших сетях является сложной задачей, поскольку существует множество потенциальных промежуточных точек, которые пакет мог бы пройти, прежде чем достигнуть хоста получателя.

**routing domain** Область маршрутизации. Группа конечных и промежуточных систем, функционирующих по общим административным правилам. Внутри каждой области маршрутизации существует одна или несколько областей, каждая из которых однозначно описывается адресом области.

**routing metric** Метрика маршрута. Метод, с помощью которого алгоритм маршрутизации определяет, что один маршрут лучше другого. Соответствующая информация хранится в таблицах маршрутизации. Метрика включает в себя размер полосы пропускания, стоимость взаимодействия, задержки, число переходов, программу начальной загрузки, максимальный размер блока на маршруте, стоимость пути, надежность. *См. также cost.*

**routing protocol** Протокол маршрутизации. Выполняет маршрутизацию с помощью конкретного алгоритма маршрутизации. Примерами протоколов маршрутизации являются IGRP, OSPF и RIP.

**routing table** Таблица маршрутизации. Таблицы, хранящиеся в маршрутизаторах или в других устройствах объединенной сети и содержащие описания маршрутов в конкретные точки сети, а в некоторых случаях и метрики, связанные с маршрутами.

**RP (Route Processor)** Процессор маршрута. Процессорный модуль в маршрутизаторах Cisco серии 7000, который содержит процессор, системное программное обеспечение и большинство компонентов памяти, используемых внутри маршрутизатора. Иногда называется "супервизорным процессором".

**RSP (Route/Switch Processor)** Процессорный модуль в маршрутизаторах Cisco серии 7500, который объединяет функции протоколов RP и SP. *См. также RP и SP.*

**RTS (Request To Send)** Запрос на передачу. Управляющий сигнал интерфейса EIA/TIA-232, с помощью которого запрашивается передача данных по коммуникационному каналу.

**S reference point** Контрольная точка S. Контрольная точка ISDN, работающая с контрольной точкой T над преобразованием 4-кабельной сети ISDN в 2-кабельную сеть ISDN, необходимую для связи с коммутаторами ISDN у поставщика услуг.

**sampling rate** Частота дискретизации. Частота, с которой производится выборка сигналов с конкретной амплитудой.

**SAP** 1. Service Access Point. Точка доступа к услугам. Поле, определенное спецификацией ШЕЕ 802.2 и являющееся частью описания адреса. Таким образом, адрес получателя и поле DSAP задают получателя пакета. Это же применимо и к SSAP. См. также DSAP и SSAP. 2. Service Advertisement Protocol. Протокол оповещения об услугах. Протокол IPX для информирования сетевых клиентов через маршрутизаторы и серверы о доступных сетевых ресурсах и услугах. См. также IPX.

**SCR (Sustainable Cell Rate)** Поддерживаемая скорость передачи ячеек. Параметр, определенный Форумом ATM для управления трафиком в сетях ATM. Для соединений с переменной скоростью передачи двоичных данных (VBR) SCR определяет усредненную по времени скорость передачи ячеек.

**SDLC (Synchronous Data Link Control)** Управление синхронным каналом передачи данных. Коммуникационный протокол канального уровня SNA. Полнодуплексный протокол побитовой передачи данных по последовательной линии, породивший многочисленные подобные протоколы, в том числе HDLC и LAPB. См. также HDLC и LAPB.

**seed router** Ведущий маршрутизатор. Маршрутизатор в сети AppleTalk, сетевой номер или диапазон кабеля которого встроен в описатель порта. Ведущий маршрутизатор определяет сетевой номер или диапазон кабеля для других маршрутизаторов того же сетевого сегмента и отвечает на запросы о конфигурировании ведомых (nonseed) маршрутизаторов, находящихся в его сети, позволяя им подтверждать или модифицировать свою конфигурацию. Каждая сеть AppleTalk должна иметь хотя бы один ведущий маршрутизатор.

**server** Сервер. Узел или программа, предоставляющая услуги клиенту (client).

**set-based** На основе команды set. Маршрутизаторы и коммутаторы на основе команды set используют эту команду для настройки. Cisco прекращает использование команд через set и применяет интерфейс командной строки (CLI) на всех новых устройствах.

**Session layer** Сеансовый уровень. Уровень 5 базовой модели OSI. На этом уровне устанавливаются, поддерживаются и завершаются сеансы между

приложениями, а также производится управление обменом данными между объектами уровня представлений. Соответствует уровню управления потоком данных архитектуры SNA. См. также *Application layer, Data Link layer, Network layer, Physical layer, Presentation layer* и *Transport layer*.

**setup mode** Режим установки. Режим, в который переходит маршрутизатор, если не обнаружено никаких настроек в энергонезависимом ОЗУ при загрузке маршрутизатора. Позволяет администратору производить пошаговую настройку маршрутизатора. Не так надежен и гибок, как интерфейс командной строки.

**SF (Super Frame)** Суперкадр. Обычный формат кадров, передаваемых по линиям T1. Суперкадр состоит из 12 кадров, каждый длиной 193 бит, из которых 193-й бит предназначен для проверки ошибок и других функций. Суперкадры вытесняются расширенными суперкадрами, хотя по-прежнему широко распространены. Другое название — "кадр D4". См. также *ESF*.

**signaling packet** Сигнальный пакет. Создается устройством, подключенным к сети ATM и желающим установить соединение с другим подобным устройством. Сигнальный пакет содержит ATM-адрес NSAP соответствующей конечной точке ATM, а также параметры класса обслуживания (QoS), необходимые для соединения. Если конечная точка может поддерживать желательный класс обслуживания, она отвечает, возвращая принятое сообщение, и соединение открывается. См. также *QoS*.

**silicon switching** Кремниевая коммутация. Основана на применении механизма SSE. Допускает обработку пакетов независимо от процессора кремниевого коммутатора (SSP). Обеспечивает высокоскоростную коммутацию пакетов по выделенным линиям. См. также *SSE*.

**simplex** Симплексная передача. Способность к передаче сигналов между источником и приемником только в одном направлении. Широковещательное телевидение является примером системы с симплексной передачей.

**sliding window** Раздвижное окно. Метод управления передачей, используемый протоколом TCP и рядом протоколов канального уровня. Буфер помещается между принимающим приложением и потоком сетевых данных. "Окно", доступное для приема данных, равно размеру буфера минус количество уже находящихся там данных. Окно увеличивается в размере по мере того, как приложение считывает из него данные, и уменьшается по мере того, как посылаются новые данные. Получатель посылает передающему устройству уведомления о текущем размере окна и может прекратить прием данных, пока окно не увеличится и не превысит определенный порог.

**SLIP (Serial Line Internet Protocol)** Межсетевой протокол для последовательной линии. Стандартный протокол для двухточечных последовательных соединений, использующий разновидность набора протоколов TCP/IP. Предшественник протокола PPP. См. также *PPP*.

**SMDS (Switched Multimegabit Data Service)** Служба коммутируемой многомегабитовой передачи данных. Технология высокоскоростной передачи датаграмм по глобальной сети с коммутацией пакетов, реализуемая телефонными компаниями.

**SMTP (Simple Mail Transfer Protocol)** Простой протокол передачи почты. Протокол Интернета, предназначенный для поддержки электронной почты.

**SNA (Systems Network Architecture)** Системная сетевая архитектура. Сложная многофункциональная сетевая архитектура, похожая на эталонную модель OSI, но с несколькими отличиями; создана компанией IBM в 1970-х гг. и, по существу, состоит из семи уровней.

**SNAP (Subnetwork Access Protocol)** Протокол доступа к подсети. Протокол Интернета, определяющий взаимодействие сетевого объекта подсети и сетевого объекта конечной системы. Описывает стандартный способ инкапсуляции датаграмм IP и сообщений ARP для передачи по сети IEEE. Объект SNAP конечной системы использует службы подсети и выполняет три ключевые функции: передачу данных, управление соединением и выбор класса обслуживания (QoS).

**socket** Сокет. 1. Программная структура, функционирующая как конечная точка коммуникаций внутри сетевого устройства. 2. Адресуемый объект внутри узла, соединенного с сетью AppleTalk. Сокетами владеют программные процессы, называемые "клиентами сокетов". Сокеты AppleTalk делятся на две группы: статически назначаемые сокет (SAS), резервируемые для клиентов (например, для базовых протоколов AppleTalk), и динамически назначаемые сокет (DAS), присваиваемые динамически протоколом DDP по запросу клиента узла. Концепция сокета AppleTalk напоминает порт TCP/IP.

**SONET (Synchronous Optical Network)** Синхронная оптическая сеть. Стандарт ANSI для синхронной передачи по оптоволоконной среде, разработанный в Bell Labs. Он определяет базовую скорость сигнала 51,84 Мбит/с и набор кратных значений этой скорости, известных как уровни оптического носителя, вплоть до 2,5 Гбит/с.

**SP (Switch Processor)** Процессор переключателя. Процессорный модуль маршрутизаторов Cisco серии 7000, действующий как администратор всех процессов в шине CxBus. Иногда называется "контроллером cisco-Bus".

**span** Участок, интервал. Полнодуплексная цифровая линия передачи, соединяющая два объекта.

**SPAN (Switched Port Analyzer)** Анализатор коммутируемого порта. Особенность коммутатора Catalyst 5000, позволяющая свободно действовать в коммутируемой среде Ethernet благодаря ее возможности наблюдения имеющихся сетевых анализаторов. На одном коммутируемом участке SPAN отражает трафик в предопределенный порт SPAN в то время, как

сетевой анализатор, подключенный к порту SPAN, наблюдает за данными из любого другого коммутируемого порта Catalyst.

**spanning explorer packet** Пакет исследования покрывающего дерева. Следует по статически конфигурируемому покрывающему дереву при поиске путей в сети SRB. Другие названия — "пакет исследования ограниченного маршрута" и "пакет исследования отдельного маршрута". См. также *all-routes explorerpacket*, *explorerpacket* и *local explorerpacket*.

**spanning tree** Покрывающее дерево. Подраздел сетевой топологии, в котором не существует петель. Когда мосты соединяются в петлю, мост или коммутатор не может идентифицировать кадр, который был переправлен перед этим, — т.е. отсутствует механизм удаления кадра, многократно проходящего через интерфейс. Из-за этого мосты постоянно их пересылают, потребляя полосу пропускания и увеличивая издержки сети. Связующие деревья обрезают сеть, чтобы для кадра оставался только один путь. См. также *Spanning Tree Protocol* и *spanning tree algorithm*.

**spanning-tree algorithm (STA)** Алгоритм покрывающего дерева. Применяется в протоколе покрывающего дерева для создания покрывающего дерева. Иногда используется сокращение STA. См. также *spanning tree* и *Spanning-Tree Protocol*.

**Spanning-Tree Protocol (STP)** Протокол покрывающего дерева. Протокол моста, в котором используется алгоритм покрывающего дерева. Позволяет мосту с обучением динамически обходить циклы в топологии сети и создавать покрывающее дерево. Для выявления циклов мосты обмениваются друг с другом протокольными блоками данных моста, а затем исключают циклы, закрывая интерфейсы с выбранными мостами. Все это относится и к стандарту IEEE 802.1 (*Spanning-Tree Protocol*), и к более ранней версии этого протокола, созданной компанией DEC и ставшей основой стандарта. Версия IEEE поддерживает области мостов и допускает построение покрывающего дерева в расширенной локальной сети. Кроме того, эта версия предпочтительнее версии DEC. Иногда используется сокращение STP. См. также *BPDU*, *learning bridge*, *MAC address*, *spanning tree* и *spanning-tree algorithm*.

**SPF (Shortest Path First algorithm)** Алгоритм "сначала кратчайший путь". Кратчайший путь по покрывающему дереву определяется итеративным наращиванием длины пути. Обычно используется в алгоритмах маршрутизации по состоянию канала. Иногда называется "алгоритмом Дейкстры". См. также *link-state routing algorithm*.

**SPID (Service Profile Identifier)** Код профиля обслуживания. Номер, назначаемый поставщиками услуг или местными телефонными компаниями, а также администраторами порту BRI. Коды SPID используются для определения абонентских услуг устройства, подключенного по ISDN. Устройства ISDN применяют их при доступе к коммутатору телефонной компании, который отводит канал поставщику услуг.

**split horizon** "Расщепленный горизонт". Помогает предотвратить петли маршрутизации. Разновидность правила маршрутизации дистанционного вектора, когда создается препятствие, чтобы сведения о маршруте не покидали интерфейс маршрутизатора, через который они были получены.

**spoofing** Имитация соединений. 1. Схема, используемая маршрутизаторами для того, чтобы заставить хост воспринимать интерфейс так, будто он работает и поддерживает сеанс. Маршрутизатор имитирует ответы на сообщения о поддержке соединения, посылаемые хостом, чтобы убедить хост в том, что сеанс продолжается. Имитация соединений полезна при маршрутизации в такой среде, как DDR (при отсутствии трафика в таких средах связь коммутируемого канала разрушается), для сохранения права на взимание платы за предоставленный канал связи. *См. также DDR.* 2. Некорректное требование пакета с адресом, владельцем которого пакет не мог быть послан. Имитация соединения разработана для усложнения работы механизмов обеспечения безопасности сети, например фильтров и списков доступа.

**spooler** Программа буферизации. Приложение, управляющее запросами или заданиями, посылаемыми ему для выполнения. Обрабатывает запросы в порядке их поступления. Примером является программа буферизации принтера.

**SPX (Sequenced Packet Exchange)** Последовательный обмен пакетами. Надежный протокол с установлением соединения, дополняющий службу обработки датаграмм протоколов сетевого уровня.

**SQE (Signal Quality Error)** Ошибка качества сигнала. Посылка, отправляемая приемопередатчиком обратно контроллеру, чтобы он определил, работоспособна ли схема выявления конфликтов.

**SRB (Source-Route Bridging)** Мост с маршрутизацией от источника. Метод внедрения моста, принадлежащий компании IBM и широко используемый в сетях Token Ring. В сети с мостами с маршрутизацией от источника весь маршрут от источника до получателя определяется заранее, до отправки данных получателю. *Сравните с transparent bridging.*

**SRT (Source-Route Transparent bridging)** Выполнение функций моста с маршрутизацией от источника. Предложенная компанией IBM схема внедрения моста, в которой объединяются две самые распространенные стратегии — организация мостов с маршрутизацией от источника и прозрачных мостов. Для удовлетворения потребностей всех конечных узлов (EN) эта схема совмещает в одном устройстве обе технологии. *Сравните с SR/TLB.*

**SR/TLB (Source-Route Translational Bridging)** Транслирующий мост с маршрутизацией от источника. Способ внедрения моста, при котором станции с маршрутизацией от источника могут взаимодействовать со станциями, выполняющими функции транслирующего моста, через промежуточный мост, преобразующий форматы между протоколами двух мостов. *Сравните с SRT.*

**SSAP (Source Service Access Point)** Точка доступа к услугам источника. Точка доступа к услугам сетевого узла, указываемая в поле источника пакета. См. также *DSAP* и *SAP*.

**SSE (Silicon Switching Engine)** Механизм кремниевой коммутации. Механизм маршрутизации и коммутации: заголовок канального или сетевого уровня поступившего пакета сравнивается с содержимым кэша кремниевой коммутации с целью определения типа выполняемой операции (маршрутизация или функция моста). Затем пакет передается через соответствующий интерфейс. Механизм кремниевой коммутации реализован аппаратно в процессоре кремниевого коммутатора (SSP) маршрутизатора Cisco серии 7000. Поэтому коммутация может выполняться независимо от функционирования системного процессора, что существенно ускоряет маршрутизацию по сравнению с ее программной реализацией.

**standard IP access list** Стандартный список доступа IP. Список доступа IP, который использует для фильтрации сообщений сети только исходящие IP-адреса.

**standard IPX access list** Стандартный список доступа IPX. Список доступа IPX, который использует для фильтрации сообщений сети только исходящие и конечные IPX-адреса.

**star topology** Звездообразная топология. Топология локальной сети, в которой конечные точки соединяются с центральным переключателем двухточечными связями. В сетях с звездообразно-кольцевой топологией для соединений используются не двухточечные связи, а однонаправленные. Сравните с *bus topology* и *ring topology*.

**startup range** Диапазон для начальной загрузки. Диапазон значений (от 65280 до 65534), из которого узел сети AppleTalk выбирает сетевой номер для собственного инициализируемого адреса, если нет других сохраненных номеров.

**state transitions** Переходы состояний. Система цифровой сигнализации, которая считывает состояние цифрового сигнала в середине битовой ячейки. Если это 5 вольт, ячейка интерпретируется как 1. Если состояние цифрового сигнала — 0 вольт, битовая ячейка интерпретируется как 0.

**static route** Статический маршрут. Маршрут с явно указанными промежуточными точками. Вносится в таблицу маршрутизации. Статические маршруты предшествуют маршрутам, найденным с помощью протоколов динамической маршрутизации.

**static VLANs** Статические виртуальные ЛВС. Статические виртуальные ЛВС настраиваются вручную для каждого порта. Этот метод обычно используется в производственных сетях.

**statistical multiplexing** Статистическое мультиплексирование. Метод, с помощью которого информация, полученная по нескольким логическим каналам, может быть передана по одному физическому каналу. При

статистическом мультиплексировании динамически распределяется полоса пропускания только входных каналов, что оптимизирует использование доступной полосы пропускания и позволяет установить связь для большего числа устройств по сравнению с другими способами мультиплексирования. Также называется "статистическим мультиплексированием с разделением времени".

**STM-1 (Synchronous Transport Module level 1)** Синхронный транспортный модуль уровня 1. Один из форматов SDH, определяющий структуру кадра для линий передачи ячеек ATM со скоростью 155.52 Мбит/с.

**store and forward packet switching** Коммутация пакетов с промежуточным хранением. Метод коммутации пакетов, при котором кадры полностью обрабатываются перед дальнейшей передачей через соответствующий порт. Обработка включает в себя вычисление циклического избыточного кода и проверку адреса получателя. Кроме того, кадры временно сохраняются до появления ресурсов (например, свободной линии), достаточных для передачи сообщения.

**STP 1. Shielded Twisted-Pair.** Экранированный кабель "витая пара". Двухпарный проводной носитель, используемый в различных сетевых реализациях. Имеет экранирующий слой, уменьшающий влияние электромагнитных помех. Сравните с UTP. 2. См. *Spanning-TreeProtocol*.

**stub area** Тупиковая область. Область OSPF, по которой проходят маршруты, выбранный по умолчанию, внутренние маршруты области и маршруты между областями, но нет маршрутов во внешние сети. Виртуальные каналы нельзя конфигурировать для прохождения через тупиковую область; тупиковые области не должны содержать граничные маршрутизаторы автономной системы (ASBR). См. также *non-stub area, ASBR и OSPF*.

**stub network** Тупиковая сеть. Сеть, соединенная только с маршрутизатором.

**STUN (Serial Tunnel)** Последовательный туннель. Свойство маршрутизатора, позволяющее соединить два SDLC- или HDLC-совместимых устройства не прямой последовательной линией, а через произвольную многопротокольную топологию (с использованием маршрутизаторов Cisco).

**subarea** Подобласть. Часть сети SNA, содержащая узел подобласти и любые линии подключения и периферийные узлы.

**subarea node** Узел подобласти. Коммуникационный контроллер SNA или хост, обрабатывающий полные сетевые адреса.

**subchannel** Субканал. В широкополосных системах — создание отдельных коммуникационных каналов за счет разделения по частотам исходной полосы пропускания.

**subinterface** Субинтерфейс. Виртуальный интерфейс, назначенный на один физический интерфейс.

**subnet** Подсеть. См.: *subnetwork*.

**subnet address** Адрес подсети. Часть IP-адреса, выделяемая с помощью маски подсети. См. также *IP address, subnet mask u subnetwork*.

**subnet mask** Маска подсети. 32-битовая маска адреса, используемая в протоколе IP для указания битов IP-адреса, которые описывают адрес подсети. Иногда называется просто маской. См. также *address mask u IP address*.

**subnetwork** Подсеть. 1. Для сетей IP — сеть, совместно с другими использующая некоторый адрес подсети. Подсети произвольно выделяются администратором из исходной сети с целью создания многоуровневой иерархической маршрутизируемой структуры и исключения сложной адресации подключенных сетей. См. также *IP address, subnet address u subnet mask*. 2. Для сетей OSI — совокупность конечных и промежуточных систем, управляемых из одного административного домена и использующих единый протокол доступа к сети.

**SVC (Switched Virtual Circuit)** Коммутируемая виртуальная цепь. Динамически устанавливается по запросу и закрывается после завершения передачи данных. Такие цепи используются, когда передача данных носит спорадический (нерегулярный) характер. В терминологии АТМ называется "коммутируемым виртуальным соединением". Сравните с *PVC*.

**switch** Переключатель. 1. Сетевое устройство, осуществляющее фильтрацию, распространение и создание лавин кадров по результатам анализа адреса получателя. Функционирует на канальном уровне модели OSI. 2. Обобщенный термин, относящийся к электронным или механическим устройствам, которые устанавливают при необходимости соединения и разрывают их после завершения сеанса.

**switch fabric** Термин, обозначающий коммутируемый сетевой комплекс с многочисленными коммутаторами.

**switched LAN** Локальная сеть, в составе которой имеются переключатели локальной сети (LAN switch). См. также *LAN switch*.

**synchronous transmission** Синхронная передача. Термин, описывающий передачу сигналов с синхронизацией. Такие сигналы имеют одинаковую частоту, причем отдельные символы обрамляются управляющими битами (стартовым и стоповым), отмечающими начало и конец передаваемого символа. См. также *asynchronous transmission u isochronous transmission*.

**T reference point** Контрольная точка Т. Используется с контрольной точкой S для изменения 4-проводной сети ISDN в 2-проводную сеть ISDN.

**T1** Цифровая глобальная сеть, которая использует 24 цифровых сигнала DSO по 64 Кб каждый для создания полосы на 1.536 Мбит/с минус издержки тактирования, что составляет 1.544 Мбит/с доступной полосы пропускания.

**T3** Цифровая глобальная сеть, обеспечивающая полосу 44,763 Мбит/с.

**tag switching** Коммутация идентификаторов. Высокопроизводительная технология передачи пакетов, объединяющая маршрутизацию сетевого уровня и коммутацию канального уровня и обеспечивающая расширяемую высокоскоростную коммутацию в ядре сети. Основана на идее обмена метками: пакеты или ячейки получают короткие метки фиксированной длины, по содержимому которых переключатели определяют, куда следует передавать данные.

**tagged traffic** Помеченный (маркированный) трафик. Ячейки АТМ, в которых приоритета отбрасывания ячейки (CLP) установлен в 1. Если в сети возникает перегрузка, помеченный трафик может быть отброшен для обеспечения гарантированной доставки высокоприоритетного трафика. Иногда называется "трафиком, подходящим для отбрасывания". См. также *CLP*.

**TCP (Transmission Control Protocol)** Протокол управления передачей. Протокол транспортного уровня, ориентированный на установление соединения. Обеспечивает надежную полнодуплексную передачу данных. Часть набора протоколов TCP/IP.

**TCP/IP (Transmission Control Protocol/Internet Protocol)** Протокол управления передачей/межсетевой протокол. Название набора протоколов, созданных в Министерстве обороны США в 1970-х гг. для применения в объединенных сетях мирового масштаба. TCP и IP являются наиболее известными протоколами этого набора. См. также *IP* и *TCP*.

**TDM (Time-Division Multiplexing)** Временное мультиплексирование (уплотнение). Метод разделения полосы пропускания одного носителя между несколькими информационными потоками, основанный на предварительном задании временных интервалов для каждого потока. Полоса пропускания распределяется между каналами независимо от того, будут ли по каналу передаваться данные. См. также *ATDM*, *FDM* и *multiplexing*.

**TE (Terminal Equipment)** Терминальное оборудование. Любое периферийное устройство, совместимое с ISDN и подключенное к сети, например телефон и компьютер. TE1 — это устройства, готовые к ISDN-связи и понимающие способы передачи сигналов ISDN. TE2 — это устройства, неготовые к ISDN-связи и не понимающие способы передачи сигналов ISDN. С устройством TE2 должен использоваться терминальный адаптер.

**TE1** Терминальным оборудованием типа 1 называются устройства с четырехпроводным интерфейсом витой пары. Большинство современных устройств ISDN относятся именно к этому типу.

**TE2** Устройства, которые называют терминальным оборудованием типа 2, не понимают методов передачи сигналов ISDN, поэтому для преобразования передач сигналов должен применяться терминальный адаптер.

**telco (telephone company)** Телефонная компания.

**Telnet** Стандартный протокол эмуляции терминала из стека протоколов TCP/IP. Используется для соединения с удаленным терминалом, предоставляет пользователям возможность зарегистрироваться на удаленной системе и применять ее ресурсы так, будто они находятся в локальной системе. Telnet описан в RFC 854.

**10BaseT** 10BaseT составляет часть первоначального стандарта IEEE 802.3. Это спецификация Ethernet узкополосной, немодулированной передачи 10 Мбит/с с двумя витыми парами категории 3, 4 или 5: одна пара для отправки данных, вторая — для приема. 10BaseT ограничен расстоянием примерно 100 метров на участок. См. также *Ethernet* и *IEEE 802.3*.

**terminal adapter** Адаптер терминала. Устройство, используемое для стыковки соединений ISDN BRI с существующими интерфейсами (например, с EIA/TIA-232). Таким устройством является модем ISDN.

**terminal emulation** Эмуляция терминала. Сетевое приложение, создающее на удаленном хосте впечатление, будто компьютер, выполняющий некоторую программу, является непосредственно подключенным терминалом.

**TFTP** По существу, этот протокол — уменьшенная версия FTP, которая может быть его альтернативой, если вы точно знаете, что ищете и где это искать. TFTP не содержит такого многообразия функций, как FTP. В частности, у него нет обзора каталога; он не может делать ничего, кроме отправки и приема файлов.

**thicknet** Сеть с использованием толстого коаксиального кабеля. Другое название — 10Base5. Система шин из толстого кабеля, использующая Ethernet на расстоянии до 500 метров.

**thinnet** Сеть с тонким коаксиальным кабелем. Другое название — 10Base2. Система шин из тонкого коаксиального кабеля, реализующая доступ к среде Ethernet на расстоянии до 185 метров.

**token** Маркер. Кадр, содержащий управляющую информацию. Сетевое устройство, обладающее маркером, имеет право передавать данные по сети. См. также *token passing*.

**token bus** Маркерная шина. Архитектура локальной сети, для доступа к которой используется передача маркера. Основа стандарта IEEE 802.4 для локальных сетей. См. также *IEEE*.

**token passing** Передача маркера. Метод доступа к носителю, при котором сетевые устройства регулярно получают доступ к физическому носителю, если они обладают небольшим кадром, называемым "маркером". Противоположна circuit switching и contention. См. также *token*.

**Token Ring** Локальная сеть с передачей маркера, созданная и поддерживаемая компанией IBM. Имеет кольцеобразную топологию и передает данные со скоростью 4 или 16 Мбит/с. Сходна со стандартом IEEE 802.5. См. также *ring topology* и *token passing*.

**toll network** Междугородная сеть. Глобальная сеть, использующая коммутируемую телефонную сеть общего пользования (PSTN) для отправки пакетов.

**trace** Команда IP для отслеживания пути, который проходит пакет по объединенной сети.

**transparent bridging** Выполнение функций прозрачного моста. Схема организации моста, часто используемая в сетях Ethernet и IEEE 802.3: мосты пересылают кадры данных в соседний сетевой сегмент в соответствии с таблицами, связывающими конечные узлы и порты моста. Происхождение термина объясняется тем, что передача данных через мост производится прозрачно (незаметно) для конечных сетевых узлов. *Сравните с SRB.*

**Transport layer** Транспортный уровень. Уровень 4 базовой модели OSI, обеспечивающий надежное сетевое взаимодействие конечных узлов. На транспортном уровне устанавливаются, поддерживаются и закрываются виртуальные соединения, обнаруживаются и корректируются ошибки транспортировки и производится управление потоком информации. Соответствует уровню управления передачей модели SNA. *См. также Application layer, Data Link layer, Network layer, Physical layer, Presentation layer и Session layer.*

**TRIP (Token Ring Interface Processor)** Интерфейсный процессор Token Ring. Высокоскоростной интерфейсный процессор маршрутизаторов Cisco серии 7000. Предоставляет два или четыре порта Token Ring для подключения кабеля Token Ring или IEEE 802.5, причем скорость передачи (4 или 16 Мбит/с) для каждого порта устанавливается независимо.

**trunk link** Магистральный канал. Канал между коммутаторами и от некоторых серверов к коммутаторам. Магистральные каналы переносят данные о нескольких виртуальных ЛВС. Каналы доступа служат для связи узловых устройств с коммутатором и пересылают только данные виртуальной ЛВС, участником которой является устройство.

**TTL (Time To Live)** Время жизни. Поле IP-заголовка, содержимое которого указывает, сколько времени пакет считается действительным.

**tunneling** Туннелирование. Предоставление услуг, необходимых для реализации любой стандартной двухточечной схемы инкапсуляции. *См. также encapsulation.*

**TUD (Trunk Up-Down)** Протокол Trunk Up-Down — протокол ATM для наблюдения транков. Если транк пропускает определенное количество проверочных сообщений, посылаемых коммутаторами ATM для проверки качества магистральной линии, протокол TUD объявляет магистраль закрытой. Если транк меняет поведение и снова входит в строй, TUD признает, что транк работает и возвращает его к службе.

**U refer nce point** Контрольная точка U. Контрольная точка между устройством TE1 и сетью ISDN. Контрольная точка U понимает методы сигнализации ISDN и использует 2-проводное соединение.

**UDP (User Datagram Protocol)** Протокол пользовательских датаграмм. Протокол транспортного уровня без установления соединения из стека протоколов TCP/IP. Простой протокол обмена датаграммами без подтверждений и без гарантированной доставки, обработка ошибок и выполнение повторной передачи возлагается на другие протоколы. Протокол UDP определен в RFC 768.

**unnumbered frames** Ненумерованные кадры. Кадры HDLC, используемые для различных целей управления, включая открытие и закрытие канала и спецификацию режима.

**UTP (Unshielded Twisted-Pair)** Неэкранированная витая пара. Медный провод, используемый в небольших и средних сетях для соединения узловых устройств с концентраторами и коммутаторами. Соединяет также коммутатор с коммутатором или концентратор с концентратором.

**VBR (Variable Bit Rate)** Переменная скорость передачи двоичных данных. Класс QoS, определенный Форумом ATM для сетей ATM. Подразделяется на класс передачи в реальном времени (RT) и класс передачи без учета времени (NRT). При передаче в реальном времени относится к соединениям с фиксированным интервалом следования данных. При передаче без учета времени применяется в соединениях без подобного ограничения, которые, однако, требуют гарантированного качества обслуживания.

**VCC (Virtual Channel Connection)** Соединение виртуальных каналов. Представляет собой логический канал, составленный из связей виртуальных каналов (VCL) и организованный для передачи данных между двумя конечными точками сети ATM.

**VIP** 1. Versatile Interface Processor. Интерфейсная плата, используемая в маршрутизаторах Cisco серий 7000 и 7500. Выполняет Cisco IOS и обеспечивает многоуровневую коммутацию. Наиболее свежая версия VIP — VIP2. 2. Virtual IP. Функция, позволяющая создавать логически разделенные коммутируемые рабочие группы IP между портами переключателя Catalyst серии 5000, на котором выполняется программное обеспечение Virtual Networking Services.

**virtual circuit** Виртуальная цепь. Логический канал, созданный для обеспечения надежного взаимодействия двух сетевых устройств. Определяется парой VPI/VCI и может быть либо постоянным (PVC), либо коммутируемым (SVC). Виртуальные цепи используются в сетях Frame Relay, X.25 и ATM. См. также PVC и SVC.

**virtual ring** Виртуальное кольцо. Объект сети, содержащий мосты с маршрутизацией от источника (SRB).

**VLAN (Virtual LAN)** Виртуальная локальная сеть. Группа устройств из одной или нескольких локальных сетей, конфигурируемых (с помощью управляющего программного обеспечения) так, чтобы они могли взаимодействовать как устройства, подключенные к одному элементу.

**VLSM (Variable-Length Subnet Mask)** Маска подсети переменной длины. Для выделения в одной и той же сети различных подсетей можно определить различные маски подсетей. Маска подсети переменной длины позволяет оптимизировать использование доступного пространства адресов.

**VTP (VLAN Trunk Protocol)** Протокол VLAN Trunk Protocol; служит для обновления сведений коммутаторов в структуре коммутаторов о виртуальных ЛВС, заданных на сервере VTP. Устройствами VTP могут быть сервер VTP, клиент VTP или прозрачное устройство. Серверы обновляют клиентов. Прозрачные устройства — это только локальные устройства, они не **обмениваются** данными с клиентами VTP. Устройства VTP посылают данные виртуальной ЛВС только по магистральным каналам.

**WAN (Wide-Area Network)** Глобальная вычислительная сеть. Обозначение, используемое для связи нескольких ЛВС по сети DCE (оборудование для пересылки данных). Как **правило**, WAN является арендованной линией или удаленным соединением по сети PSTN. В качестве примеров протоколов WAN можно привести Frame Relay, PPP, ISDN и HDLC.

**wildcard** Подстановочные знаки. Применяются при настройке списков доступа, суперсетей и OSPF. Подстановочные знаки — это обозначения для определения диапазона подсетей.

**windowing** Обработка методом окна. Метод управления потоком данных, используемый протоколом TCP на транспортном уровне модели OSI.

**WinSock (Windows Socket Interface)** Программный интерфейс, позволяющий использовать широкое множество приложений для взаимодействия с Интернетом. Реализован как динамически подключаемая библиотека (DLL) с некоторыми программами поддержки (например, программой дозвона, инициирующей установление **соединения**).

**workgroup switching** Коммутация рабочих групп. Метод коммутации, обеспечивающий организацию высокоскоростного прозрачного моста между сетями Ethernet и высокоскоростного транслирующего моста между Ethernet и FDDI или CDDI.

**X.25** Стандарт ИТУ-Т, определяющий, как соединения между устройствами DTE и DCE поддерживаются при доступе к удаленному терминалу и при коммуникациях компьютеров в общедоступных сетях передачи данных (PDN). X.25 определяет протокол канального уровня LAPB и протокол сетевого уровня PLP. Frame Relay вытесняет стандарт X.25.

**ZIP (Zone Information Protocol)** Протокол информации о зоне. Протокол сеансового уровня AppleTalk, отображающий сетевые номера на имена

зон. Используется протоколом NBP с целью определения, какой сети принадлежит узел из конкретной зоны. См. также *ZIP storm* и *zone*.

**ZIP storm** ZIP-шторм. Широковещательный шторм, возникающий, когда маршрутизатор AppleTalk распространяет маршрут, для которого в текущий момент времени нет соответствующего имени зоны. Маршрут затем распространяется к следующим маршрутизаторам, и возникает ZIP-шторм. См. также *ZIP*.

**zone** Зона. В сетях AppleTalk — логическая группа сетевых устройств. См. также *ZIP*.



# CCNA

## Cisco Certified Network Associate

### Учебное руководство

Эта книга облегчит и сделает максимально эффективной подготовку к новому сертификационному экзамену Cisco Certified Network Associate (640-507). Написанное экспертами по объединенным сетям учебное руководство включает в себя:

- Предварительную оценочную контрольную работу, определяющую уровень вашей подготовки к экзамену
- Полное описание процедур конфигурации маршрутизаторов Cisco с учетом экзаменационных вопросов
- Письменные и практические лабораторные работы для закрепления материала
- 200 обзорных вопросов, требующих понимания материала

#### Подробный анализ всех экзаменационных заданий:

- Использование команд Cisco IOS
- Использование протоколов маршрутизации RIP и IGRP
- Конфигурация интерфейсов локального управления сети Frame Relay, таблиц отображения адресов и подинтерфейсов
- Наблюдение на маршрутизаторе за функционированием сети Frame Relay
- Конфигурация и службы региональных сетей
- IP-маршрутизация и динамическая IP-маршрутизация
- IP-адресация и выделение подсетей
- Сегментирование локальных сетей с помощью мостов, переключателей и маршрутизаторов
- Работа с TCP/IP
- Сохранение и восстановление Cisco IOS и конфигурации маршрутизатора
- Алгоритм покрывающего дерева
- Создание и реализация списков доступа

#### Об авторе

**Тодд Леммл** специалист CCNP, MCT, MCSE, CNI и MCNE. Президент компании GlobalNet Training Solutions, Inc. ([www.Lammle.com](http://www.Lammle.com)) и ведущий специалист компании RouterSim, LLC. Имеет более чем 18-летний опыт работы по диагностике, установке и настройке глобальных и локальных сетей.

Подготовка к экзамену  
с обзором вопросов  
и лабораторных  
упражнений  
по всем разделам  
экзамена

Десятки примеров  
конфигурации  
маршрутизаторов

Обучение  
конфигурированию  
многопротокольных  
маршрутизаторов Cisco

Последняя версия  
экзамена **CCNA 2.0**



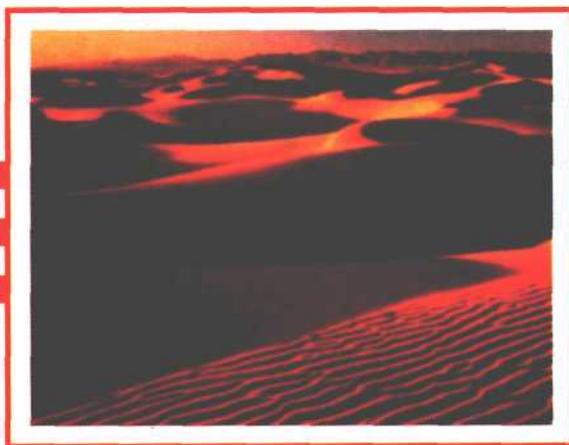
Издательство  
"ЛОРИ"  
[www.lory-press.ru](http://www.lory-press.ru)

# CCNA

Бестселлер  
#1

# Cisco Certified Network Associate

Учебное руководство



Экзамен  
640-507

Второе издание

**Тодд Леммл**

Свыше **100 000** пользователей  
выбрали это учебное руководство

**O**  
SYBEX

Издательство "Лори"